The Security of Accounting Information Systems
A Cross-Sector Study of UK companies

By

Nancy Ibrahim Riad

A Thesis Submitted in Fulfilment of the Requirements for the Degree of Doctor of Philosophy at Cardiff University

Accounting and Finance Section

Cardiff Business School

2009

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

DECLARATION

This work has not previously been accepted in substance for any degree and is not concurrently submitted in candidature for any degree.

Signed ....nancy..... (candidate)

Date ...2.12.2009.....

STATEMENT 1

This thesis is being submitted in partial fulfillment of the requirements for the degree of ..... (insert MCh, Md, MPhil, PhD etc, as appropriate)

Signed .....nancy..... (candidate)

Date ...2.12.2009....

STATEMENT 2

This thesis is the result of my own independent work/investigation, except where otherwise stated. Other sources are acknowledged by footnotes giving explicit references.

Signed .....nancy..... (candidate)

Date ...2.12.2009.....

STATEMENT 3

I hereby give consent for my thesis, if accepted, to be available for photocopying and for inter-library loan, and for the title and summary to be made available to outside organisations.

Signed .....nancy..... (candidate)

Date ...2.12.2009....

Abstract

The issue of information systems (IS) security has received considerable attention from both academics and professionals. Information systems security has become a major part of core business processes in companies of all sizes and types, and it has become more vital than ever for companies to have an organised, efficient, and proactive security approach to their IS. Despite this importance, a number of significant gaps exist in the academic literature. Most of the previous studies have dealt with IS security or information security in general, without particular attention to accounting information systems (AIS) security. Security research is fragmented, and most previous studies lack an overall and comprehensive view of AIS security issues. Each study has tended to deal with a particular security dimension. In addition, much research on IS security has been overwhelmingly focused on the technical aspects with limited consideration given to non-technical issues such as security policy, training and awareness, risk assessment or security budget.

In an attempt to fill these gaps, the current study presents an integrated view of AIS security in UK companies by addressing both the technical and non-technical aspects of security. The current study aims to investigate the AIS security level among UK companies in different industry sectors by investigating the sources and types of AIS security threats, the different types of controls implemented to prevent or reduce security threats, and the existence of a management framework for AIS security within UK companies in different sectors. To achieve the research objectives, the current study employed quantitative and qualitative approaches using a postal questionnaire and semi-structured interviews. The first stage involved sending a postal questionnaire to the IT managers of 800 UK listed companies in different industry sectors. A total of 104 responses were received, of which 65 responses were usable for statistical analysis. The second stage involved conducting nine interviews with IT managers of UK companies.

The results indicated that some activities and practices forming the AIS security management framework are well known and undertaken by the majority of UK companies regardless of the industry sector for example AIS security policy, security risk assessment, security incident handling procedures, and a business continuity plan. However, security training and awareness program, security budget, and the British Standard for Information Security (BS 7799) are the most neglected security practices in the majority of companies. The results also showed that UK companies suffer from different types of security incidents; however, many incidents go unreported because of the fear of negative publicity and the majority prefer to maintain their brand and to deal with these incidents internally.

The results also revealed that employees are now the most common source of AIS security threats facing UK companies. In addition, the results suggested frequent occurrence of some types of security threats, for instance, employees' errors such as unintentional destruction of data by employees, spamming and malware attacks, and employees' sharing of passwords. Moreover, the majority of companies are paying more attention to software, hardware, input, and output security controls. However, more effort must be devoted to organisational and personnel controls.

Dedication

To the memory of my father and to my mother, my husband and my brother

Acknowledgements

I would like to begin by thanking God for guiding me during the whole period of this study and for helping me in completing my research.

Second, I am very grateful to my supervisors, Professor Roy Chandler and Professor Maurice Pendlebury for accepting the supervision, and for their invaluable guidance, support and encouragement during the whole supervision period, and for always being there when I need them.

I would also like to express my thanks to all members of staff of the Accounting and Finance Section at Cardiff Business School, especially Professor John Doyle for helping and advising me on some statistical problems, and Professors Mahmoud Ezzamel, Mike Peel, and Jason Xiao, and Dr Mark Clatworthy for their invaluable comments and suggestions on the questionnaire. Many thanks also to the PhD secretaries, Elsie Philips and Laine Clayton for their continuous help and support during the whole period of the research.

I am also grateful to the IT managers of the UK listed companies, who spared me a part of their valuable time to complete the questionnaire, especially those who were involved in the interviews. Without their help, I would not have been able to complete this research.

Many thanks also to all my friends for their help, assistance and encouragement during the period of the study.

My deepest thanks to my family, especially my dear father who sadly passed away during my first year of study, my dearest mother, and my brother who have provided me with all the love, support and encouragement in all my life, not only during the period of my study. Finally, especial thanks to my dearest husband Nabil for his ongoing love, patience and kindness. Without his wonderful support and encouragement, I would not have been able to complete this study.

Table of Contents

Chapter 3: Methodology

Chapter 4: Analysis of questionnaire results

Chapter 5: Analysis of interview results

Chapter 6: Summary and conclusion

List of Tables

Chapter 3: Methodology

Chapter 4: Analysis of questionnaire results

Chapter 5: Analysis of interview results

Chapter 6: Summary and conclusion

List of Figures

Chapter 1: Introduction

Chapter 2: Literature review

Chapter 3: Methodology

Chapter 5: Analysis of interview results

Chapter 1
Introduction

1.1 Introduction

Security has become a pervasive concern for all organisations today and continues to rise in importance. Companies now are more dependent upon their information systems (IS) and particularly their accounting information systems (AIS) than ever before. However, due to the higher levels of interconnectivity among AIS both within and among companies, these companies face a growing risk of their systems being compromised. There is also extensive evidence to suggest that IS security threats are now growing in number, variety and most importantly, the severity of their impact (Collette and Gentile 2006). Such threats cost organisations millions of pounds annually, in addition to the loss of customers, profitability, loss of data, loss of reputation and even bankruptcy (Mitchell *et al.* 1999).

Companies have recognised the problems and are trying to take positive steps to defend their IS and to increase the security controls (Romney and Steinbart 2003). However, information security is not doing nearly enough to keep up with the rapid changes in the business environment. The gap continues to widen between the growing threats and what is actually done to address these threats, and action is still required to close this gap by applying sound information security practices (Ernst & Young 2005).

Consequently, the current study investigates the sources and types of AIS security threats, the different types of security controls implemented to prevent or reduce these threats and the existence of an AIS security management framework among UK companies in different industry sectors, in an attempt to highlight the common threats facing each particular sector as a first step for companies to implement the appropriate security controls.

The remainder of this chapter provides an outline of the current study. Section 1.2 briefly discusses the background of the research. Section 1.3 examines the importance of the research, while Section 1.4 presents the objectives, questions, and hypotheses

of the research. The research methodology is briefly introduced in Section 1.5. Section 1.6 outlines the structure of the thesis, and the final section concludes the chapter.

1.2 Background of the research

The security issue has received considerable attention from both academics and professionals. IS security has become a part of core business processes in companies of all sizes and types, and it has become more vital than ever for companies to have an organised, efficient, and proactive security approach to their IS (Booker 2006). In the UK, the priority given to security remains high across all sizes of companies. According to the BERR[1] Information Security Breaches Survey (BERR 2008), four fifths of respondents believe that information security is a high or very high priority for their senior management. In addition, the American Institute of Certified Public Accountants' 19th Top Technology Initiatives Survey (AICPA 2008) stated that, for six consecutive years, the survey identified information security as the country's number one technology concern.

Moreover, the increasing dependence on and the greater complexity of IS have brought companies different types of security threats (Chang and Yeh 2006). In addition, the literature identifies different classifications of security threats including passive/active (Mitchell *et al.* 1999), internal/external (Rainer *et al.* 1991), human/non-human (Loch *et al.* 1992), intentional/non-intentional (Qureshi and Siegel 1997), physical/logical (Abu-Musa 2003), and IT-related/non-IT-related security threats (Chang and Yeh 2006).

Security surveys also indicated that the number of security breaches occurring within companies continues to rise. The 2006 DTI Information Security Breaches Survey (DTI 2006) stated that 62 percent of UK companies had had a security incident in the last year and, on average, every UK company now suffers several security incidents a day. Consequently, the cost to UK companies is significant. The 2006 Technology, Media & Telecommunications Security Survey (DTT 2006b, p.3) confirms this fact

[1] The Department for Business, Enterprise and Regulatory Reform (BERR) is a UK government department, which was created on 28 June 2007 on the disbanding of the Department of Trade and Industry (DTI). The BERR covers the same areas covered previously by the DTI e.g. Company Law, Trade, Business Growth, Economic Development, etc.

and indicated, "Security incidents are in the news every day and the overall risks are growing". In addition, more than half of the companies surveyed said that their systems had been breached over the last 12 months. Even worse, both the magnitude and complexity of the attacks are increasing. Despite the fact that the BERR Information Security Breaches Survey (BERR 2008) revealed that fewer companies had security incidents in the last year than two years before, the average seriousness of incidents increased.

Whitman (2003) argued that knowing the enemy that confronts information security is a vital component in shaping an information security defence posture. Accountants, as well as users, managers, and designers of IS should be knowledgeable about security threats and appropriate control techniques in order to protect their own systems (Beard and Wen 2007).

A review of the literature reveals that there is a great concern from academics and practitioners regarding security threats facing different companies. They have investigated the different types of threats, the seriousness of threats and the frequency of occurrence of each threat in an attempt to assist companies to identify and employ the relevant security controls to prevent or reduce such threats.

Consequently, the need to understand and employ adequate information security controls has become an issue no company can ignore. Chang and Yeh (2006) indicated that a lack of robust information security protection raises the information security threat level of companies. Every company, regardless of its size and type, must prepare itself for all possible security threats. However, there is no one security solution that is suitable for all companies (Tsohou *et al.* 2006). Security controls are increasingly complex and must be tailored to the business (Jones 2003). In addition, due to resource constraints, companies cannot implement unlimited controls to protect their systems. Instead, they should try to understand the major threats and implement effective controls accordingly (Lin 2006).

The literature reveals a great concern regarding the IS security controls that companies implement to prevent or reduce security threats facing them. In addition, different classifications were assigned to these security controls. For example,

security controls can be classified, among others, according to purpose into preventive, detective, and corrective controls (Bagranoff *et al.* 2005; Flowerday and Von Solms 2005; Lin 2006; Romney and Steinbart 2003). Controls can also be classified according to their association with data processing stages into input, processing, storing, and output security controls (Abu-Musa 2004b; Bagranoff *et al.* 2005). In addition, Gerber and Von Solms (2001) classified information security controls according to the evolution of the computing eras into physical, technical, and operational controls.

However, despite the progress made by companies in protecting their IS and the sensitive information stored in them, they often focus on the technical controls and neglect the non-technical issues of information security such as security policy, training and awareness, and standards. There is a wide agreement in the literature that these two dimensions - technical and non-technical - have to work together to create a secure environment. Chang and Yeh (2006) indicated that effective information security should address both IT and non-IT related issues instead of simply considering IT systems. More recently, Kritzinger and Smith (2008) stated that the technical and non-technical issues of information security should be balanced to ensure that the technical issues do not overshadow the non-technical issues so that the human side of information security is adequately addressed when developing a common body of knowledge for information security suited to industry.

It is, therefore, necessary for companies to go beyond technical considerations and to adopt a structured process for managing their IS security. Eloff and Von Solms (2000) argued that IS security management is a stream of management activities that aims to protect the IS and create a framework within which such systems operate as expected by the company. Pironti (2005) indicated that by introducing a structured approach to information security, a company could increase its security posture and reduce the security costs. It can also gain advantage in its efforts to ensure compliance to security standards and regulations. Consequently, an IS security management framework must exist not only to protect IS but also to ensure the continuity of the company (Karyda *et al.* 2005).

However, the literature review reveals that there are various approaches to dealing with the IS security management issue. Some studies discussed security management in general, for example, Vermeulen and Von Solms (2002), while the majority of the other studies focused only on one of its activities such as security policy, security training and awareness, incident handling, business continuity, risk assessment, security budget, or security standards.

Furthermore, there is a high degree of agreement that companies in different industry sectors tend to give a different role to IS (Jarvenpaa and Ives 1990) and therefore have different security requirements (Chang and Yeh 2006; Kankanhalli *et al.* 2003; Straub 1986). Consequently, a company's approach to security depends on its industry sector.

Based on the above, the current study aims to present an integrated view of the AIS security in UK companies by covering both technical and non-technical aspects of security, and to investigate the different sources and types of AIS security threats and the types of security controls implemented to prevent or reduce security threats among companies in different industry sectors in the UK. In addition, the current study aims to investigate the existence of a management framework for AIS security within UK companies, including AIS security policy, security training and awareness program, risk assessment, incident response, disaster recovery, and business continuity plan, security budget, security standards and certification, and AIS security effectiveness.

1.3 Importance of the research

While the importance of IS security is being increasingly recognised, a number of significant gaps exist in the academic literature. It can be recognised that most of the previous studies have dealt with IS security or information security in general, without particular attention to AIS security.

In addition, a review of the literature underlines the fact that security research is fragmented and no comprehensive framework exists. Cannoy *et al.* (2006) stated that most previous security studies included diagrams, charts and tables; however, none of them included major constructs and their relationships, only proposing a model for a specific topic or clarifying a technical system, and many of the frameworks proposed

are extremely specific and task-related. Moreover, while a number of major surveys have been conducted to investigate different security issues, they have been commercially oriented surveys and not formal academic studies.

The literature also reveals that most previous studies lack an overall and comprehensive view of the AIS security issue. Each of these studies tried to deal with a particular security dimension. Some of them focused on threats facing AIS (Abu-Musa 2003; 2004a; 2006a and b; Keller *et al.* 2005; Loch *et al.* 1992; Ryan and Bordoloi 1997; Whitman 2004). Other studies focused on security controls (Abu-Musa 2004b; 2007a and b; Henry 1997; Kankanhalli *et al.* 2003), while others combined the security threats and controls in one study (Cerullo and Cerullo 2005; Chang and Yeh 2006; Gupta and Hammond 2005; Yeh and Chang 2007).

Moreover, the literature reveals that the majority of previous studies focused only on one of the activities of the management framework for AIS security. Doherty and Fulford (2005), Hong *et al.* (2006) and Kadam (2007) focused on the security policy. Kruger and Kearney (2006) and Peltier (2005) addressed the security training and awareness issue. Gerber and Von Solms (2005) covered risk assessment. Bhaskar (2005) and Mitropoulos *et al.* (2007) addressed the incident handling issue, whereas Hunton (2002) and Rodetis (1999) focused on the disaster recovery and business continuity plans. Gordon and Loeb (2006) were concerned with the security budget, while Freeman (2007) and Karabacak and Sogukpinar (2006) focused on the security standards and certification.

The literature also shows that much research on IS security has been overwhelmingly focused on the technical aspects with limited consideration to the non-technical issues such as security policy, training and awareness, and security budget. Wood (1995) argued that no matter how sophisticated the information security technology is, controls will not be sustainable unless the non-technical factor has been adequately addressed. Chang and Yeh (2006) also indicated that effective information security should address both IT and non-IT related issues instead of simply considering IT aspects of the IS.

In an attempt to fill these gaps, the current study aims to present an integrated view of the AIS security in UK companies by addressing both the technical and non-technical aspects of security. The current study investigates the sources and types of threats facing AIS security, the different types of security controls implemented to prevent or reduce security threats, and the existence of a management framework for AIS security within UK companies in different industry sectors.

The researcher hopes that the study results may increase managers' awareness in different industry sectors of the different sources and types of AIS security threats facing their companies so that they can take the appropriate precautions. In addition, it is hoped that the study results may highlight the various types of security controls implemented in the different industry sectors investigated to increase the managers' awareness of these controls. Furthermore, the current study presents a management framework for AIS security; if properly implemented, it may help different companies to secure their AIS and their sensitive information.

1.4 Objectives, questions, and hypotheses of the research

A review of the literature shows that most previous studies lack an overall and comprehensive view of the AIS security issue. Each of these studies tried to cover a particular security dimension. Some of them focused on threats facing AIS, others focused on security controls, whereas others covered only one of the activities that form the IS security management framework. Thus, the current study is an attempt to fill this gap and to present an integrated view of AIS security. More specifically, the current study has six main aims. The first is to examine the existence of an adequate AIS security management framework within UK companies in different industry sectors. The second is to investigate the different types of AIS security threats facing UK companies in different industry sectors. The third is to identify the security controls implemented by UK companies to prevent or reduce security threats. The fourth is to investigate the effect of the different types of security controls implemented for the reduction of AIS security threats facing UK companies, while the fifth is to examine the relationship between the AIS security effectiveness level and the security threats level within UK companies. Finally, the study aims to investigate the security perception among different industry sectors in the UK.

This study is an attempt to investigate the level of the AIS security among UK companies in different industry sectors. In particular, this study seeks to find answers to the following questions:

1. Is there an adequate management framework for AIS security among UK companies in different industry sectors?
2. What are the most common sources and types of security threats facing AIS of UK companies in different industry sectors?
3. What types of security controls are implemented to prevent or reduce security threats in different industry sectors in the UK?
4. Are there significant differences between different industry sectors in the UK concerning the types of AIS security threats, AIS security controls and the existence of an adequate management framework for AIS security within companies?
5. What is the impact of the security controls implemented and the AIS security effectiveness level achieved on the reduction of AIS security threats facing UK companies in different industry sectors?

In order to achieve the objectives of the current study and to examine the relationship between its main variables five hypotheses will be tested:

H1: There are no significant differences among UK companies in different industry sectors concerning the existence of a management framework for AIS security.

H1.1: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security policy and the frequency of updating this policy.

H1.2: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security training and awareness program and the security awareness level.

H1.3: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS risk assessment program and the frequency of undertaking this program.

H1.4: There are no significant differences among UK companies in different industry sectors concerning the existence of security incident handling procedures, disaster recovery and business continuity plans and the frequency of testing and updating these plans.

H1.5: There are no significant differences among UK companies in different industry sectors concerning the existence of a security budget and areas of spending on AIS security.

H1.6: There are no significant differences among UK companies in different industry sectors concerning the awareness level of the British Standard for Information Security Management BS 7799 and the certification under ISO 27001.

H1.7: There are no significant differences among UK companies in different industry sectors concerning the techniques used to evaluate AIS security effectiveness, the success indicators of AIS security management, and the effectiveness level of AIS security management.

H2: There are no significant differences among UK companies in different industry sectors concerning the sources and types of AIS security threats.

H3: There are no significant differences among UK companies in different industry sectors concerning the types of controls implemented to prevent or reduce security threats.

H4: There is no significant relationship between the different types of security controls and the reduction of AIS security threats facing UK companies.

H5: There is no significant relationship between AIS security effectiveness and the AIS security threat level in UK companies.

1.5 Methodology

To achieve the research objectives and to test the hypotheses, the current study employed quantitative and qualitative approaches using a postal questionnaire and semi-structured interviews. The first stage involved a postal questionnaire. This method was chosen because of the advantages it provides compared to other research methods, its specific relevance to the nature of the study, and its popularity in previous research in IS security for example Abu-Musa (2004a and b), Chang and Ho (2006), Henry (1997), Huang *et al.* (2006), Kankanhalli *et al.* (2003) and Kotulic and Clark (2004) (see Chapter 3).

The final version of the questionnaire was sent by post to the IT managers of 800 UK listed companies in different industry sectors. A total of 104 responses was received, of which 65 responses were usable for statistical analysis, resulting in a usable response rate of 8.1 percent (see Chapter 4). Despite the low response rate, the

literature reveals that it is comparable with many previous security studies given the very sensitive and intrusive nature of the AIS security issue. Given the nature of the hypotheses (Section 1.4) and the type of data collected (nominal, ordinal), nonparametric tests were employed to analyse the data collected, namely, a Kruskal-Wallis One-Way Analysis of Variance, a Chi-Square Test of Independence, and Spearman's Rank Correlation. In addition, a series of stepwise regressions were run in an attempt to identify the significant effect of the different types of security controls implemented by UK companies on the reduction of AIS security threats facing the companies (see Chapter 4).

The second stage involved semi-structured interviews. This method has been increasingly recommended and utilised in recent years in IS research for instance Kotulic and Clark (2004) and Keller *et al.* (2005). The semi-structured interviews were conducted after the questionnaire in order to clarify and confirm the results obtained from the questionnaire analysis, to achieve a high degree of validity and reliability, to enrich the quality of information collected, and to fill in any gaps in data that might occur in the questionnaire's results. After collecting the questionnaires, all the 12 respondents who agreed to participate in a follow-up face-to-face interview were contacted and nine interviews were conducted. The small number of interviews is not surprising, given that security research is the most intrusive type of research and there is undoubtedly a general mistrust of any outsider attempting to gain data about the security practices within companies (Kotulic and Clark 2004). All the interviews were audio recorded and notes were taken. The interviews were transcribed in full and the qualitative data analysis software (NVivo) was used to support Miles and Huberman's (1994) approach in analysing interview data (see Chapter 5).

1.6 Structure of the thesis

There are six chapters in this thesis. This chapter has provided an outline of the current study. It has briefly discussed the background of the research, the importance of the research, and presented its objectives, questions, and hypotheses. It also briefly introduced the research methodology.

Chapter 2 reviews the literature and presents an integrated view of the AIS security issue. It describes the meanings, components and importance of AIS and explores

their role in organisations. It also explores the different classifications and types of threats facing AIS security. Moreover, this chapter describes the meanings, importance of and responsibility for AIS security, focusing on the different dimensions of security and paying particular attention to the security management. Finally, it investigates the different classifications and types of security controls used and employed to prevent or reduce security threats.

Chapter 3 focuses on the methodology used in the current study. It presents the conceptual framework of the research, explaining the main variables of the current study, and demonstrates the research objectives, questions and hypotheses. It explains the research design, the data collection methods used in previous studies concerning AIS security and the methods employed in the current research namely a mail questionnaire and semi-structured interviews, emphasising the strengths and weaknesses of each method, along with justifications for their use. The chapter then proceeds by providing a detailed explanation of the procedures followed in each method, the questionnaire design and layout, the pilot test of the questionnaire, and the sampling and administration of both methods. The chapter briefly presents the statistical methods applied to analyse the research data and the ethical considerations of the research.

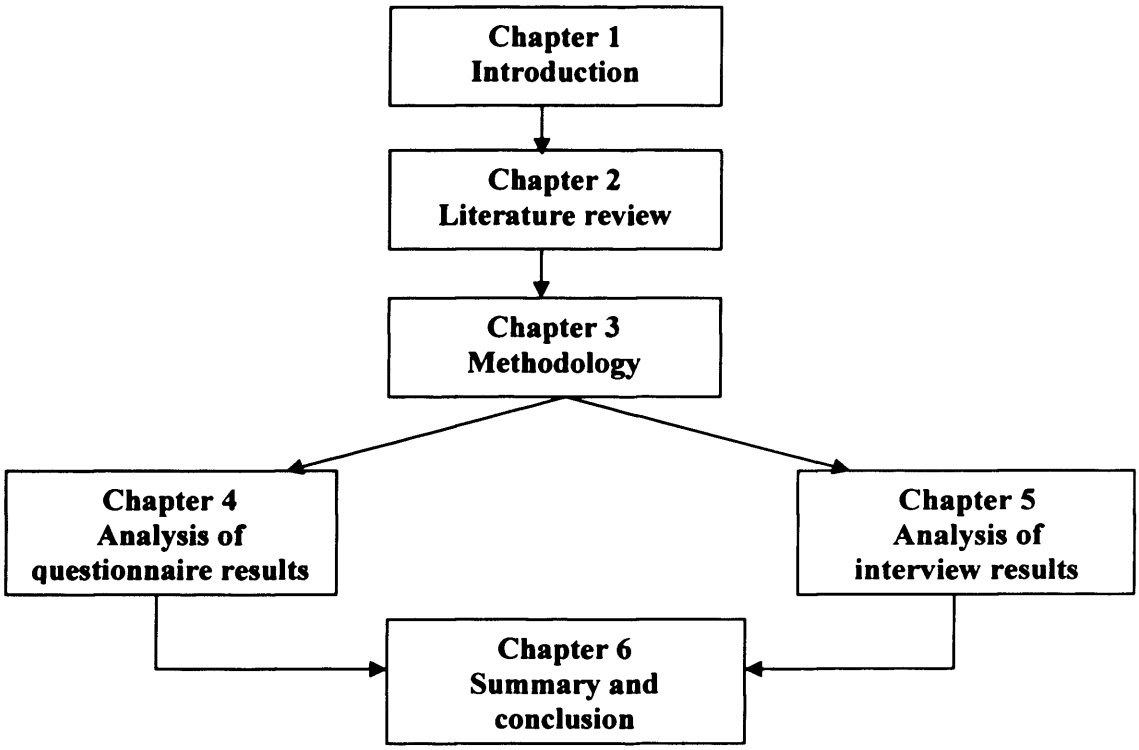
Chapter 4 is devoted to the questionnaire data analysis. It begins by presenting the sample size and response rate of the current study. It also provides a full discussion of the statistical methods employed to analyse data from the questionnaire and the justifications for selecting these methods. The chapter then presents the profile of the participants and their companies and provides their opinions regarding AIS security within their companies and the main findings of the questionnaire.

In Chapter 5, a full discussion of the interview data analysis is presented. The chapter begins by presenting the sample size of the interview, how interviewees were contacted, and the date, time and duration of each interview. It proceeds by discussing the approach used in analysing interview data and how the qualitative data analysis software (NVivo) was used to support Miles and Huberman's (1994) approach in the current study, with a particular emphasis on the advantages and disadvantages of using NVivo software in analysing interview data. The profile and opinions of the

interviewees and the main characteristics of their companies are then presented with the main findings of the interviews.

Finally, Chapter 6 concludes the study. It reviews the research aims and objectives, and presents the data collection methods used. It also provides a summary of the main findings of the research, and the recommendations drawn from these findings. The limitations of the research and suggestions for future research are then presented. The structure of the thesis is presented in Figure 1.1.

Figure 1.1 The structure of the thesis



1.7 Summary of the chapter

This chapter has provided an overview of the current study. It began by discussing the background of the research, and then revealed its importance. The objectives, questions and hypotheses of the research were then presented, followed by a brief introduction to the research methodology and the structure of the thesis.

The following chapter reviews the literature and presents an integrated view of the AIS security issue. It describes the meanings, importance of and responsibility for the AIS security, focusing on the different dimensions of security and paying particular attention to security management. It also demonstrates the different classifications and

types of the AIS security threats facing companies, and the different classifications and types of security controls used to prevent or reduce security threats in different countries paying particular attention to the UK.

Chapter 2

Literature Review

2.1 Introduction

In today's global society, the significance of information is widely accepted and IS are truly pervasive throughout organisations (ISACF 2001). The information created, issued, stored and transmitted by a company's AIS is one of its most valuable assets and is considered a critical resource, enabling the company to achieve its objectives (DTI 2004a and b; Flowerday and Von Solms 2005). Furthermore, information and Information Technology (IT) systems that support it are very important business assets. Their availability, integrity and confidentiality are essential to maintain competitive edge, profitability, compliance and respected company image (Von Solms 1999).

Consequently, it seems that having the right information at the right time can make the difference between profit and loss, success and failure in today's business environment (Gerber and Von Solms 2001).

However, with the rapid change in IT, with the development and increasing spread of user-friendly systems and with the great desire of companies to acquire and implement up-to-date computerised systems and software, AIS are becoming more available to all types and sizes of companies. This enables accounting tasks to be accomplished much faster and more accurately than before (Abu-Musa 2003). Consequently, due to the higher levels of interconnectivity of AIS both within and among companies, these companies face the growing risk of their systems being compromised. Mitchell *et al.* (1999) indicated that IS are subject to many forms of security threats. Such threats cost companies millions of pounds annually. They can also result in the loss of customers and credibility, even causing operational breakdown and ultimately affecting profitability. In addition, there are frequent reports in accounting and financial publications of computer-related data errors, incorrect financial information, and violation of internal controls, thefts, fires and sabotage (Qureshi and Siegel 1997).

There is also extensive evidence to suggest that the security threats to information and AIS are now growing in number, variety and most importantly, the severity of their impact (Collette and Gentile 2006). Deloitte confirms this fact in its 2006 Technology, Media & Telecommunications Security Survey by indicating that "security incidents are in the news every day and the overall risks are growing" (DTT 2006b, p.3). In addition, more than half of the companies surveyed claimed that their systems had been breached over the last 12 months. Even worse, both the magnitude and complexity of the attacks are increasing.

The DTI Information Security Breaches Survey (DTI 2006) indicated that every UK company suffers several security incidents a day. More recently, the BERR Information Security Breaches Survey (BERR 2008) revealed that although fewer companies had security incidents in the last year than two years previously, the average seriousness of incidents had increased. Consequently, the cost to UK companies is likely to be significant.

Because of these losses, companies are now recognising the problems and are trying to take positive steps to defend their IS including AIS and to increase security controls (Romney and Steinbart 2003). However, according to the Global Information Security Survey (Ernst & Young 2005), information security is not doing nearly enough to keep up with the rapid changes in the business environment. The gap continues to widen between the growing risks and what information security is actually doing to address these risks. Moreover, even though many companies have recognised this gap, action is still required to close it by applying adequate information security practices.

The aim of this chapter is to examine the literature and to present an integrated view of the AIS security issue. First, the chapter begins by describing the meanings, components, importance and role of AIS. It goes on to explore the different AIS security threats. It then describes the meanings, importance of and responsibility for AIS security, focusing on the different dimensions of security and paying particular attention to security management. Finally, it investigates the different types of security controls employed to prevent or to reduce security threats.

2.2 AIS and the need for security

Companies today are more dependent upon their AIS than ever before. However, the increasing use of the internet and online data processing has made access to these systems more available and easier for many users, which has led to a corresponding increase in AIS security abuses. Consequently, the need to understand and to employ adequate systems security has become a key business management issue.

2.2.1 What is meant by AIS?

Before considering the meaning of AIS, it is essential to examine the meaning of each word of the term "accounting information systems" individually.

"Accounting" is the combined activities of recording economic data, processing and analysing these data and presenting the resulting information in financial terms. Accounting is the information a company uses to achieve efficient operations and effective management. "Information" is a set of outputs from AIS or any other IS. It serves as the basis for making decisions and taking actions. "System" represents a set of two or more interrelated components that interact to achieve a certain goal. However, within the accounting profession today, the term system or systems usually refers to "Computer Systems" (Romney and Steinbart 2003; Wilkinson 1989).

Based on the above, the term "information systems" describes the organised collection, processing, transmission and dissemination of information in accordance with defined procedures, whether automated or manual (Poore 1999). Moreover, the term "accounting information systems" can be defined as "a collection of data and processing procedures that creates needed information for its users" (Bagranoff *et al.* 2005, p.5). In addition, an AIS is "a set of components that collect accounting data, store it for future uses and process it for end users" (Romney and Steinbart 2003, p.8).

It is important to note that not all AIS are computerised or even need to be, but most of the ones in business today are, in fact, computerised. On the other hand, AIS have traditionally focused on collecting, processing and communicating financial-oriented information to the company's external parties for example investors, creditors and tax agencies, and internal parties such as management. However today, AIS are concerned with non-financial as well as financial data and information.

From the above, the researcher concludes that AIS are systems concerned with collecting, processing and storing data and disseminating financial and non-financial information to interested parties.

2.2.2 Components of AIS

In performing their activities, AIS require specific components or elements. The nature of these components depends on the degree of automation of these systems. Wilkinson (1989) indicated that in the traditional AIS that employ manual techniques, the components consist of documents, journals, ledgers, files, reports and other outputs, non-computerised processing devices, methods and controls. However, with the increasing level of automation, the computerised AIS consist of five components (Boritz *et al.* 1999; Romney and Steinbart 2003) as follows:

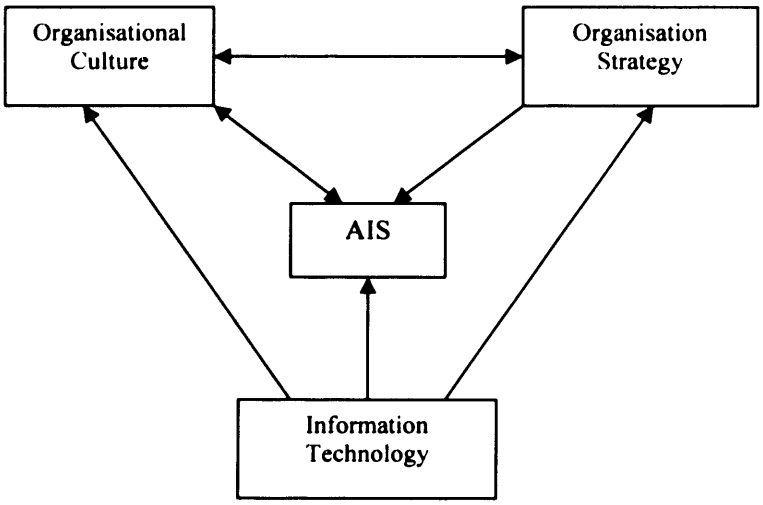
- Personnel involved in operating and using the system;
- Procedures involved in collecting, processing and storing data about companies' activities;
- Data about companies' business processes;
- Software used to process companies' data; and
- IT infrastructure including computers, peripheral devices and network communications devices.

In addition, AIS can be as simple as a personal computer-based payroll application with a single user, or they may be as complex as a multi-application, multi-computer system accessed by an unlimited number of users inside or outside the company.

2.2.3 Factors influencing the design of AIS

According to Romney and Steinbart (2003), three main factors can have an influence on the AIS design in any company namely IT, organisational culture and the organisation's strategy (Figure 2.1). IT can change the way that accounting and other business activities are performed. AIS should be designed to reflect the value of the company, and therefore organisational culture has an effect on its design. Moreover, an organisation's strategy has a significant influence on the company as a whole.

Figure 2.1 Factors influencing design of AIS



(Source: Romney and Steinbart 2003, p.6)

2.2.4 Role of AIS

Reviewing the literature concerning the role of IS in general and AIS in particular reveals that AIS can perform three main functions in a company (Bagranoff *et al.* 2005; Romney and Steinbart 2003). These functions are:

- Collecting and storing data about the company's activities, the resources affected by those activities, and those who participate in the various activities so that management, employees and interested outsiders can review what has happened;
- Transforming data into information that is useful for making decisions that enable management to plan, execute and control activities; and
- Providing adequate controls to safeguard the company's assets, including its data, to ensure the availability, accuracy and reliability of data.

2.2.5 Why do AIS fail?

However, despite the significant role of AIS in any company and the usefulness of the computerised AIS, systems sometimes fail. As mentioned before, AIS consist of personnel, procedures, data, software and hardware; consequently, if one of these components fails, the whole system may fail. Boritz *et al.* (1999) suggested some common symptoms of unreliable systems, namely:

- Frequent failures that deny internal and external users access to essential systems services;

- Unauthorised access, making the systems vulnerable to viruses, hackers and loss of data confidentiality;
- Loss of data integrity, including corrupted, incomplete and fictitious data; and
- Serious maintenance problems resulting in unintended negative side-effects from system changes such as unavailability of system services, loss of data confidentiality or integrity.

From the above, it seems that the main characteristics of reliable AIS are:

- Availability i.e. systems are available when needed;
- Security i.e. systems are protected against unauthorised access;
- Integrity i.e. systems processing is complete, accurate and timely; and
- Maintainability i.e. systems can be updated in a manner that provides continuous availability, security and integrity.

2.3 Security threats

Companies today have become increasingly dependent on AIS more than ever before. These systems have grown increasingly more complex to meet our escalating needs for information. However, as systems' complexity and our dependence on them increase, companies face significant risks related to ensuring the security and integrity of those systems that is AIS can generate many direct and indirect benefits and as many direct and indirect risks. In addition, the literature reveals that companies, their information, AIS and networks are faced with a large number of security threats from a wide range of sources.

2.3.1 What is meant by security threats?

A review of the literature shows that there is some confusion concerning the meaning of threats, risks, incidents, vulnerabilities, and attacks.

A threat is any possible event or sequence of actions that might lead to a violation of one or more security goals. The term "threat" is not limited to the adversary that could cause harm but to events that could lead to harm (Tsiakis and Stephanides 2005). According to Pfleeger and Pfleeger (2007, p.6), security threats can be defined as "circumstances that have the potential to cause loss or harm". This loss could consist of the absence of data or a resource within an information system, financial loss, or

loss of company credibility (Mitchell *et al.* 1999). In addition, the DTI Information Security Policy Team stated, "a threat is a potential cause of an unwanted incident which may result in harm to a system or organisation" (DTI 2004a, p.7). Furthermore, the National Information Systems Security Glossary (NSTISSI 4009 2000, p.55) defined a threat as "any circumstance or event with the potential to adversely impact an IS through unauthorised access, destruction, disclosure, modification of data and/or denial of service".

It can be concluded that security threats are any event that can have an adverse impact on a company's IS in general and AIS in particular. These threats can either be singular or form part of a combination of multiple threats, and they can come both from inside and from outside the company.

A risk represents "the possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability" (NSTISSI 4009 2000, p.47). A risk is "the level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring" (NIST 800-53 2005, p.26). Straub and Welke (1998) indicated that security risk is that the company's information and IS are not sufficiently protected against certain kinds of damage or loss. A risk is the possibility that a certain threat will have a negative effect on a company's IS in general and AIS in particular.

The National Information Systems Security Glossary (NSTISSI 4009 2000, p.62) defined a vulnerability as "a weakness in an IS, system security procedures, internal controls, or implementation that could be exploited". A vulnerability represents a weakness of an asset or group of assets that can be exploited by a threat (DTI 2004a, p.7). A vulnerability is a weakness in IS in general or AIS in particular that can be exploited by a certain threat or by a group of threats.

An incident is "an assessed occurrence having actual or potentially adverse effects on an IS" (NSTISSI 4009 2000, p.29). An information security incident is "one or more unwanted or unexpected events that have a significant probability of compromising business operations and threatening information security" (DTI 2004a, p.7).

Therefore, an IS security incident represents one or more unexpected events that can have an adverse impact on a company's IS in general or on AIS in particular.

On the other hand, an attack is a type of incident involving the intentional act of attempting to bypass one or more security controls of IS (NSTISSI 4009 2000) in general and AIS in particular.

Thus, the literature supports the view that companies and their IS and AIS are subject to increasing numbers and types of security threats.

2.3.2 Classifications of security threats

The literature reveals that there are various classifications of security threats. As mentioned, some previous studies focused on security threats in general, others addressed AIS security threats, others were concerned with computer security threats, while others presented information security threats.

Parker (1981) classified security threats according to the type of act into natural disasters, errors and omissions, and intentional acts. Rainer *et al.* (1991) also classified AIS security threats under three main groups: physical threats; unauthorised access; and authorised users, which may be caused by internal and external sources.

Loch *et al.* (1992) presented a four-dimensional IS threat classification system including sources, perpetrators, intent and consequences. The sources of threats can be inside or outside the company; the perpetrators can be human or non-human; the intent can be accidental or intentional; and the consequences can be disclosure, modification, destruction or denial of service. Abu-Musa (2003) added another dimension in which security threats can be classified into physical or logical security threats. Chang and Yeh (2006) also classified IS assets and the corresponding threats into two types: IT and non-IT-related threats. IT-related threats are those involving software, hardware, data and network, while, non-IT-related threats are those related to personnel, administration and physical/environmental facilities.

Regarding the information security threats, Icove *et al.* (1999) grouped information threats into seven categories: software, hardware, data, network, physical, personnel

and administration, where administration includes security regulations and policies. In addition, Mitchell *et al.* (1999) classified information security threats into passive and active threats. The passive threats represent unpredictable natural or physical disasters and accidental human errors occurring completely at random, while the active threats represent deliberate and malicious attacks on IS, which can potentially be predicted and avoided, can be carried out by insiders or outsiders and may be the result of direct or indirect action.

Posthumus and Von Solms (2004) presented three main sources from which business information risks may arise: natural risks, technical risks and human risks. Natural risks include events such as floods, earthquakes or fires, which can cause considerable damage, not only to the company's business information assets, but also to its physical structures. Technical risks arise as a result of a growing dependence on technology and include numerous potential hardware and software failures that can occur, whereas, human risks result from the deliberate or accidental acts of human beings and can possibly create the greatest area of concern regarding the protection of a company's critical information assets.

In addition, Wiant (2005) presented four principal means by which sensitive information is exposed. Those means include intentional theft by unauthorised agents outside the company; theft or sabotage by former employees or disgruntled current staff; accidental exposure by current employees; and other various types of disclosures by company members and from inappropriate use of information among secondary users. Parker (1984) argued that the accidental exposure by employees is the most common problem, which is usually due to employees' negligence, ignorance or carelessness. Manrique (2005) and Whitman (2004) confirmed that the accidental acts by employees remain a high priority threat to information security.

With respect to computer security threats, Qureshi and Siegel (1997) classified computer security risks into three major categories: destruction, modification and disclosure, where each may be further classified into intentional and unintentional acts. Threats can also come from computer criminals and disgruntled employees who intend to defraud, sabotage and hack, and computer users who are careless or

negligent. In addition, threats can come from the environment in the form of natural disasters.

Katz (2000) indicated that a computer network can be attacked in a number of ways with different degrees of damage, and these attacks can take different forms: a denial of service (an attack on the availability of information); theft of information (an attack on the ownership of information) and the corruption of data (an attack on the integrity of information). In addition, Garg *et al.* (2003) classified IT security incidents into web site defacement, denial of service, theft of customer and credit card information. Moreover, Austin and Darby (2003) stated that threats to digital security come in many shapes and sizes; however, they fall into three main categories: network attacks, intrusions, and malicious acts.

Based on the above, it seems that security threats concerning information, IS, AIS, computers or IT can be classified into:

- Passive/active security threats;
- Internal/external security threats;
- Human/non-human security threats;
- Intentional/non-intentional security threats;
- Physical/logical security threats; and
- IT-related/non-IT-related threats.

2.3.3 Types of security threats

The literature reveals that companies their information, IS and networks, irrespective of their size and type, are faced with different security threats. However, it seems that some threats are more prevalent in certain locations or countries than in others.

In the UK, a study was conducted by Mitchell *et al.* (1999) to investigate the attitudes to information security among commercial organisations. The results showed that computer failure and fire, followed by computer viruses were considered the most serious security threats. One third of companies felt that their information security was at risk from disgruntled employees. In comparison, 50 percent believed that mistakes by authorised employees threatened security. However, only 40 percent of companies felt that the internet was a serious threat to their information. More

recently, the majority of companies have come to recognise the internet as one of their most serious security threats. Lee *et al.* (2008) indicated that internet misuse has emerged as one of the major concerns of managers in today's business environment.

In addition, the DTI Information Security Policy Team (DTI 2004a) indicated that the following threats, among others, might cause harm, damage, or loss to the company's information: system failure; disgruntled employees; unauthorised access by competitors; denial of service attacks; theft of laptops; fraud and deception; and identity theft. According to the DTI Information Security Breaches Survey (DTI 2006), viruses and malicious software continue to be the most common cause of security incidents for UK businesses. In addition, there has been an increase in the number of instances of staff misuse of IS. Significant attempts to break into networks are the most reported types of attack by an outsider. The survey also indicated that the most common type of theft and fraud involving computers is the physical theft of computer equipment, while the accidental systems failure or data corruption is the second highest incident type after virus infection.

Although, it seems that computer viruses were the most common cause of security incidents for UK businesses, the virus threat is not now identified as a key concern to the majority of companies. The BERR Information Security Breaches Survey (BERR 2008) indicated that companies reported few virus infections and this could be because corporate anti-virus defences have significantly improved.

Regarding the USA, one of the studies was carried out by Loch *et al.* (1992). The researchers developed a list of 12 threats, derived from the literature, and conducted a survey to explore the perception of IS security executives regarding the security threats to their company's IS. Respondents were asked to rank the top three of the following threats for microcomputers, mainframes and networks. These security threats are:

- Accidental entry of bad data by employees;
- Intentional entry of bad data by employees;
- Accidental destruction of data by employees;
- Intentional destruction of data by employees;
- Unauthorised access to data/system by employees;

- Inadequate control over media (disks, tapes);
- Poor control over manual handling of input/output;
- Access to data/system by outsiders (hackers);
- Access to data/system by outsiders (competitors);
- Entry into the system of computer viruses, worms;
- Weak, ineffective, inadequate physical control;
- Natural disasters: fire, flood, loss of power, communications.

The results revealed that natural disasters and employees accidental actions were ranked among the top threats by all three environments. The accidental destruction of data by employees, accidental entry of bad data by employees and inadequate control over media were ranked as the top three security threats in microcomputers. Accidental entry of bad data by employees, natural disasters and accidental destruction of data by employees received the top three ranks in mainframes, whereas natural disasters, access to system by hackers and weak/ineffective controls were the top threats in the network environment.

Since AIS security has become one of the major concerns for companies, Davis (1997) conducted an important study similar to the study conducted by Loch *et al.* (1992), in which a sample of CPAs were surveyed about AIS security threats in four computing environments: microcomputers, minicomputers, mainframes, and networks. From a list of 17 potential threats, the respondents were asked to rank the top three threats applicable to each of the four computing environments. The results revealed that employees are a common threat for the four environments, which confirmed the results of the study conducted by Loch *et al.* (1992). The results showed that the following threats are ranked as the top three threats in the four computing environments:

- Microcomputers: accidental destruction of data by employees, introduction of computer viruses to systems and inadequate control over storage media;
- Minicomputers: accidental entry of bad data by employees, unauthorised access to data/systems by employees and poor segregation of information systems duties (i.e. programming and operations);
- Mainframes: poor segregation of information systems duties, unauthorised access to data/systems by employees and natural disasters e.g. fire; and

- Networks: introduction of computer viruses to systems, unauthorised access to data/systems by outsiders and unauthorised access to data/systems by employees.

It can be concluded from both Loch *et al.* (1992) and Davis (1997) studies that different computing environments have different levels of security risks. Consequently, a system of microcomputers with connections to an external network such as the internet was viewed as the highest risk environment, whereas a mainframe environment was viewed as having the lowest threat level. Cavusoglu *et al.* (2004) argued that the increased interconnectivity among computers enabled by the internet raised the scale and scope of security threats.

In another study, Ryan and Bordoloi (1997) examined the security threats associated with the client/server versus the mainframe environment. Respondents were asked to rate the seriousness of 15 potential security threats to their company in both environments. The results revealed that three threats were related to major loss of computer resources or data: natural disasters, single point of failure and the loss due to inadequate backups or log files. The results revealed also that the average ratings of seven security threats were significantly different for computing environments. In each of these seven cases, the perceived risk was rated higher in the mainframe environment. These significant security threats are:

- Accidental destruction of data by employees;
- Accidental entry of erroneous data by employees;
- Intentional destruction of data by employees;
- Intentional entry of erroneous data by employees;
- Loss due to inadequate backups;
- Natural disaster; and
- Single point of failure.

The results also indicated that viruses, bombs and worms are of paramount concern in the client/server environment, which confirms the results of many previous studies.

Moreover, the IFAC International Information Technology Guidelines (IFAC 1998) stated that threats might arise, among others, from technical conditions, natural disasters, environmental conditions, human factors, unauthorised access or viruses. In

addition, other threats, such as outsourced operations are increasing in significance. Romney and Steinbart (2003) confirmed these threats and indicated that companies face four main types of AIS security threats, namely: natural disasters (fire, floods, etc.); software errors and equipment malfunctions (hardware failures, software errors, operating system crashes, power outages, etc.); unintentional acts (accidents caused by human carelessness, failure to follow procedures, poorly trained personnel, errors or omissions, lost data, etc.) and intentional acts i.e. computer crimes (sabotage, computer fraud, etc.).

In another study to identify and rank current threats to information security and to present current perceptions of the level of severity of these threats, Whitman (2004) developed a list of information security threats and asked respondents to rank these threats. The threat ranked most serious by respondents was deliberate software attacks, followed by deliberate acts of espionage. The act of human error or failure remains a high priority as a valid threat. It seems that these findings support the findings of Loch *et al.* (1992) indicating that the same threats that faced IS managers over 10 years earlier, were still prevalent when this study was conducted.

Furthermore, in a more recent study Kros *et al.* (2005) indicated that IS security breaches occur in many forms, including theft of proprietary information, financial fraud, system penetration, denial of service, sabotage and virus infection.

Based on the responses of computer security practitioners in USA corporations, government agencies, financial institutions, medical institutions and universities, the Computer Crime and Security Survey (Gordon *et al.* 2006) revealed that the attacks on or misuse of computer systems include: viruses (65 percent); laptop/mobile hardware theft (47 percent); insider abuse of net access (42 percent); unauthorised access to information (32 percent); denial of service (25 percent); system penetration (15 percent); abuse of wireless network (14 percent); theft of proprietary information (9 percent); telecom fraud (8 percent); misuse of public web application and website defacement (6 percent); and sabotage (3 percent). It is clear from the results that the majority of respondents suffered virus attacks. However, the results of a recent survey (Richardson 2007) revealed that the number of companies suffering virus attacks has dropped and this could be because anti-virus vendors have become faster at reacting

to new virus threats. On the other hand, insider abuse of network access or e-mail has become the most prevalent security problem facing companies.

Moreover, the respondents to the DTT Global Security Survey (DTT 2006a) indicated that their top threats include privacy issues (62 percent), increasing sophistication of attacks (59 percent) and emerging technologies (47 percent). A year later, the respondents to the survey addressed human error (79 percent), technology (73 percent), and third parties (46 percent) as the root causes of failures of their companies' IS (DTT 2007).

From the above, it seems that investigating the types of security threats has received much attention from USA academics and practitioners. It is clear also that the insiders for example employees' accidental and intentional acts are the major threats facing companies. Lin (2006) argued that there would always be some risk that authorised employees will misuse data they have access to in the course of their work. In addition, Mattsson (2007) argued that many abuses and accidents occur because people have access to data that they do not need to see, or do need to see but should not be able to alter or delete.

Furthermore, in order to investigate the security threats in developing countries, Abu-Musa (2006b) conducted a study to investigate security threats to computerised AIS in the Egyptian Banking Sector (EBS). The entire population (66 banks) was surveyed using a self-administered questionnaire. The results revealed that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and human-made disasters, employees' sharing of passwords and misdirecting printouts are the most significant security threats to computerised AIS in the EBS. Furthermore, Abu-Musa (2006a) used the same list of security threats in another study to investigate the perceived security threats to computerised AIS, through their frequency of occurrence, in Saudi Arabian organisations. The results revealed that almost half of the responding organisations suffered financial losses due to security breaches. The results also revealed that accidental and intentional entry of bad data, accidental destruction of data by employees, employees' sharing of passwords, introduction of computer viruses, destruction of output, unauthorised document visibility and misdirecting printouts are

the most significant perceived security threats to the computerised AIS in Saudi Arabian organisations. Thus, both studies indicated that there is strong agreement among respondents regarding AIS security threats, which means that the types of security threat are almost the same in the developing countries.

In Taiwan, Chang and Yeh (2006) conducted a study to explore the concerns of companies in different industries regarding IS threats facing them, and the countermeasures prepared to protect them from such threats using a mail questionnaire. The results revealed that banking businesses suffer the most significant IS threat, followed by technology, distribution/service, and manufacturing. The results showed that the manufacturing businesses considered the network to be a major threat while the banking businesses regarded the network and regulation as their main threats. The technology companies were more concerned about the network and data, whereas the distribution/service businesses considered the network, regulation, and software as their major threats. It is clear that the network was considered a major security threat in all the industry sectors investigated.

Based on the previous studies conducted in the UK, USA, Egypt, Saudi Arabia and Taiwanese organisations, it seems that employees' accidental and intentional acts and the network are the most common security threats facing companies.

The Information Security Industry Survey (Briney 2001) addressed the human factor in security and presented some of the insider breaches experienced by companies. The results revealed that the majority of companies (76 percent) suffered use of unauthorised software, which is followed by illegal use of company resources (63 percent); using company resources for profit (50 percent); abuse of computer access controls (58 percent); physical theft or sabotage (42 percent); use of unauthorised hardware (54 percent); electronic theft, or intentional destruction of information (24 percent) and fraud (13 percent). Leach (2003) argued that many companies suspect that their internal security threat is more pressing than their external security threat. Vroom and Von Solms (2004) also indicated that despite the vital role of employees in a company's success they are the weakest link when it comes to information security. In addition, Keller *et al.* (2005) pointed out that over half of respondents in their study felt that the primary threats to data came from internal personnel.

In another study, Cerullo and Cerullo (2005) describe a hypothetical model of a complex IT network that points out the major access points vulnerable to threats, which provides accountants and IT professionals with examples of generic network security threats. According to their model, the network can be vulnerable to four categories of threats: human threats e.g. hackers, espionage, password crackers, sabotage, social engineering, cyber crime and fraud; human non-malicious threats e.g. data entry errors, inadequate access controls, inadequate training and policies; accidents e.g. destruction of data, disks, and documents, failure of hardware, software or computer programs; and natural disasters e.g. floods. It is clear that this study addressed a wide range of IS and computer security threats facing companies, which can enhance the awareness of accountants and IT professionals regarding these threats.

On the other hand, Haugen and Selin (1999), Manrique (2005) and Romney and Steinbart (2003) addressed computer fraud and abuse. They indicated that computer fraud and abuse represent intentional acts of compromising a company's IS and computers. More specifically, computer fraud includes the following:

- Unauthorised theft, use, access, modification, copying and destruction of software or data;
- Theft of money by altering computer records or the theft of computer time;
- Theft or destruction of computer hardware;
- Obtaining information or tangible property illegally through the use of computers.

In addition, perpetrators have devised many methods to commit these intentional acts including viruses, worms, bombs, Trojan horse, hacking, cracking, data leakage, denial of service attacks, software piracy, e-mail threats, password cracking, social engineering, browsing and spamming. More recently, Clarke (2007) argued that staff fraud is on the rise, which could hit not only the finances but also the reputation of the business.

From the above, it seems that companies are facing a large number of security threats, and since most, if not all, companies now depend on computerised AIS in carrying out their activities, security threats facing them are increasingly complex, which can lead to extensive damage for example business interruption, financial loss, loss of data and

information, and even bankruptcy. Consequently, the need to understand and employ adequate security controls is an issue no business owner can ignore.

2.4 AIS Security

The security issue has received considerable attention from both academics and practitioners. It has become a major concern to all sizes and types of organisations.

In considering the UK, the priority given to "security" remains high across all sizes of companies. According to the DTI Information Security Breaches Survey (DTI 2006), three quarters of UK businesses rate "security" as a high or very high priority. More recently, the BERR Information Security Breaches Survey (BERR 2008) indicated that the majority of respondents believed that information security is a high or very high priority to their senior management. In addition, the American Institute of Certified Public Accountants' 19th Top Technology Initiatives Survey (AICPA 2008) stated that, for six consecutive years, the survey identified information security as the country's number one technology concern.

2.4.1 What is meant by AIS security?

Reviewing the literature concerning the security issue indicates that there is no clear agreement on the meaning of security. There is some confusion among academics and practitioners regarding the terms "Security", "Information Security", "IT Security", and "IS Security". Most of the previous studies used them - to a great extent - as synonymous terms.

Security

The term "Security" means different things to different people. To some of them, it is concerned with preserving data integrity, whereas to others it is concerned with securing privacy for proprietary and restricted information (Granat 1998). Security is defined as "traditional methods (security officers, fences, alarms) used to increase the likelihood of a crime-controlled, tranquil, and uninterrupted environment for an individual or organisation in pursuit of objectives" (Purpura 2002, p.7). In more detail, security is "any method (e.g. security officers, safety, auditing, insurance) used by an individual or organisation to increase the likelihood of preventing and

controlling loss (e.g. of people, money, productivity, materials) resulting from a host of adverse occurrences (e.g. crime, fire, accident, error, poor supervision or management, bad investment)" (Post *et al.* 1994, p.10).

On the other hand, many security definitions focus only on information. According to the IFAC International Information Technology Guidelines (IFAC 1998, p.4), "Security relates to the protection of valuable assets against loss, disclosure, or damage. In this context, valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure". In addition, the KPMG Information Risk Management Group (KPMG 1998) stated that "Security" is the practices and procedures that ensure that information, generally held in electronic format, is safeguarded from unauthorised access, modification or accidental change and is readily available to authorised users on request.

Moreover, according to the International Organisation of Standardisation (ISO/IEC 15408-1 1999), the concept of "Security" refers to the capability of a software product to protect data and information in order to avoid unauthorised individuals or systems being able to read and modify them (Villarroel *et al.* 2005). The Information Security Glossary also defined the term "Security" as "the protection of information availability, integrity and confidentiality" (Abu-Musa 2002b, p.150). Furthermore, Hong *et al.* (2003) indicated that security is to combine systems, operations and internal controls to ensure the integrity and confidentiality of a company's data and operational procedures.

From the above, it is clear that there are different meanings for security; however, most of the definitions focus only on one dimension that is data and information security, which indicates the importance of companies' data and information in today's business environment.

Information Security

Similarly, there are many definitions for information security. The Technology, Media & Telecommunications Security Survey (DTT 2006b) stated that information security

is commonly considered to revolve around three fundamental principles: confidentially, integrity, and availability of information and many information security definitions can support this fact.

Information security is defined as "all the aspects related to achieving and maintaining confidentially, integrity, availability, auditability (accountability), authenticity and reliability" (ISO/IEC TR 13335-1, 1996, p.1). The Information Security Governance Guidance (ISACF 2001, p.9) stated that information security is "protecting the interests of those relying on information and the systems and communications that deliver the information from harm resulting from failures of availability, confidentiality and integrity". In addition, both the DTI Information Security Policy Team (DTI 2004a, p.6) and the National Institute of Standards and Technology (NIST 2005) indicated that information security involves the preservation of confidentiality, integrity and availability of information. Moreover, Ekenberg *et al.* (1995, p.709) stated that information security includes IT security i.e. the protection of IT systems (computers, communication systems, etc.) and their data. They also stated, "Information security is the protection of proprietary knowledge and data against any accidental or deliberate compromise to their integrity, confidentiality or availability".

However, other definitions for information security address other dimensions or principles. Peltier (2001, p.266) stated that "information security encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorised or accidental modification, destruction, disclosure, loss or access to automated or manual records and files as well as loss, damage or misuse of information assets". Anderson (2003, p.310) proposes a definition for information security addressing important dimensions of security such as assurance, risks and controls and refers to it as "enterprise information security" which means "a well-informed sense of assurance that information risks and controls are in balance". In addition, the International Organisation of Standardisation (ISO/IEC 17799 2005) addresses other important dimensions, and indicated that information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities.

It can be concluded that there is no wide agreement on the meaning of information security given that it is sometimes referred to as IT security or computer security.

AIS Security

Reviewing the literature reveals that the majority of academics and practitioners have used the term "IS security" equivalent to "computerised IS security" or "computer security". Jenkins and Pinkney (1978, p.393) stated "security is usually defined as meaning that the computer facilities are available at all required times, that data is processed completely and accurately and that access to the data in computer systems is restricted to authorised people".

According to the National Information Systems Security Glossary (NSTISSI 4009 2000, p.30), IS security is "the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorised users, including those measures necessary to detect, document, and counter such threats".

Moreover, Tryfonas *et al.* (2001) indicated that IS security is a set of principles, regulations, methodologies, techniques and tools established for protecting an IS or any of its parts, from potential threat. In addition, from the definition mentioned by Theoharidou *et al.* (2005, p.473), it seems that IS security is a broader term which includes IT and non-IT elements as well. They stated that IS security refers to "the protection of all elements constituting IS (i.e. hardware, software, information, people and processes)".

From the above, the researcher concludes that IS security is a broad term that includes all activities - IT and non-IT - that aim to protect companies' IS and to minimise exposure to risks.

However, a review of the literature reveals that there is no agreed definition of the term "AIS security". However, since AIS is a major element of companies' whole IS, AIS security should be regarded as an integral part of the overall IS security of those companies. Consequently, the researcher suggests that the term "AIS Security" should refer to the protection of all components that collect, store and process accounting data for end-users.

2.4.2 The importance of security

Without doubt, security has become a pervasive concern for all companies today and continues to rise in importance. The proliferation of interconnected IS and networks has meant that no business can afford to neglect this issue. According to recent surveys, the frequency of security incidents is increasing at an alarming rate. In addition, as dependence on the internet grows, concerns over security and associated issues continue to be listed as a company's top challenge (Garg *et al.* 2003).

The DTI Information Security Breaches Survey (DTI 2006) indicated that the UK continues to embrace the internet, with the vast majority of even small businesses enjoying the benefits of broadband connections. Consequently, this new business environment is accompanied by new security threats and the number of companies affected is still twice the level seen a decade ago. The majority of UK companies had a security incident in 2005 and the actual number of reported incidents was up from 2004. On average, every UK company suffered several security incidents a day (up from one a month in 2004) (DTI 2004c; 2006). Moreover, the BERR Information Security Breaches Survey (BERR 2008) stated that the average seriousness of incidents had increased.

However, it seems that most of the previous studies dealt with information security in general, without particular attention to AIS security. This could be because the survival and success of IS in general and AIS in particular depends largely on the confidentiality, integrity and availability of their critical and sensitive information, and because of the importance of data and information in today's business environment.

On the other hand, there is wide agreement among academics and practitioners regarding companies' security risks, the reasons for these risks and the benefits of keeping their information and IS secure.

The IT Governance Institute of the Information Systems Audit and Control Foundation (ISACF 2001) stated that IS can generate many direct and indirect benefits, and as many direct and indirect risks. These risks have led to a gap between the need to protect systems and the scope of controls applied. This gap can be the

result of the widespread use of technology, interconnectivity of systems, increasing rate of technological change, attractiveness of conducting electronic attacks against companies, and external factors such as legislative, legal and regulatory requirements or technological developments.

The IFAC International Information Technology Guidelines (IFAC 1998) indicated that security failures might result in both financial losses and/or intangible losses such as unauthorised disclosure of sensitive information. In addition, IS threats may arise from intentional or unintentional acts and may come from internal or external sources. They may originate from, among others, technical conditions, human factors, unauthorised access, or viruses. Consequently, adequate information security controls help to ensure the smooth functioning of IS and protect a company from loss caused by security failures. The DTI Information Security Policy Team (DTI 2004a and b) also stated that the protection of a company's information resources is vital both for the continued health of the business and for compliance with legal, regulatory and contractual demands. In addition, the availability, integrity and confidentiality of the company's information may be critical for its continued success.

Consequently, the impact of an information security breach may be far greater than what might be expected. Not only will the loss of sensitive or critical information directly affect a company's competitiveness and cash flow, it could also damage its reputation and have a long-term adverse effect. It might take years for a company to establish its reputation and image as a trustworthy and reliable business but a security breach could destroy this in a matter of hours (DTI 2004b). In addition, Posthumus and Von Solms (2004) argued that information security helps a company to mitigate the various risks to its information through the application of relevant security controls. The information security assists the company in sharing its information in a trustworthy way in order to build trusting relationships with its customers, suppliers and other business partners. In turn, this will improve its cash flow and profitability.

The International Organisation of Standardisation (ISO/IEC 17799 2005) confirms the above and indicates that defining, achieving, maintaining and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance and commercial image.

In addition, Nyanchama (2005) and Schneier (2001) stated that the direct losses caused by security incidents include loss of productivity e.g. time spent to recover and restore service, downtime for personnel who depend on service availability to conduct their jobs, direct loss of business if service availability is impacted and the theft of trade secrets and customers' information. On the other hand, indirect losses include reputation-related loss e.g. loss of customers, damage of brand and loss of goodwill, compliance penalties and potential liabilities. According to Schneier (2001), most European countries have strict privacy laws and companies can be held liable if they do not take serious steps to protect their information and customers. The USA also has similar laws in particular industries such as banking and health care.

Consequently, companies must keep their information confidential, available when needed and protected from damage, destruction and loss of integrity, which requires participation of employees in all company levels and from shareholders, suppliers, customers, external parties, and outside specialists if needed.

2.4.3 The evolution of security

Security has moved a long way from the early days when physical security formed the backbone of a company's security controls. Today security is all about policies, standards, awareness programs, strategies, compliance, etc. In addition, the scope of security has become much wider than just directly protecting the data, information and software of a business. Management has started to realise that security governance has become their direct responsibility, and that serious personal consequences, specifically legal, could flow from ignoring this security issue.

However, the literature reveals that there is little attention among academics and practitioners, apart from Von Solms, regarding the evolution of security. He addressed the evolution of security from different perspectives. First, Von Solms (1996) addressed the evolution of security using the scope of and responsibilities for information security. Regarding the scope of information security, computing started with central mainframe computers in the 1960s, and only the IT personnel had access to the facilities. From the middle 1970s, PCs, information sharing, local area networks, etc. were introduced. Many new non-IT personnel were introduced to computers, but access to IS was restricted to authorised employees within the

company's boundaries. Many companies engaged in inter-company electronic trading and linked their IT facilities. The companies linked to the internet and to the IT networks of business partners. Consequently, the scope of authorised access to a company's IS has expanded from within the computer room to within the company's boundaries to outside these boundaries.

In addition, in the past information security was limited to physical security and the responsibility was mainly on the operations manager. With the move of computing into business areas, away from large central mainframes, the IT manager became responsible for security over the business system applications on networks and mainframe computers. Thus, the responsibility for information security has moved through the years from the bottom upwards, and it has expanded to another level that is IT management. Top management realised that the well-being of their company depends on the information security status, so they must ensure that adequate security is in place. However, it seems that, since Von Solms's paper, other technological advancements have emerged and the scope and responsibility for security has been extended so that security has become the ultimate responsibility of the top management. More recently, Von Solms (2005) has argued that the position of the information security manager has been an established position in most UK companies. The Global Security Survey (DTT 2007) also indicated that the role of the information security manager is rising through the ranks to the upper levels of the company.

On the other hand, Von Solms (2000; 2006) stated that the evolution of information security could be divided into four waves. The "first wave" up to the early 1980s was mainly characterised by a very technical approach to information security i.e. the "Technical Wave". The "second wave" from the early 1980s to middle 1990s was characterised by a growing management realisation of and involvement with the importance of information security, supplementing the technical wave i.e. the "Management Wave". The "third wave" from the last few years of the 1990s was characterised by aspects like best practices and codes of practice for information security management, international information security certification, cultivating information security as a corporate culture, and dynamic and continuous information security measurement i.e. the "Institutional Wave". The "fourth wave" from the beginning of 2000 until now, can be seen as the "Information Security Governance

Wave" and is characterised by the development and crucial role of the information security governance. Thus, nowadays, top management has started to become personally accountable for the security of their IS on which they base their planning and decisions.

Furthermore, Gerber and Von Solms (2001) classified the evolution of computers and related technologies and thus security into three distinct eras, namely, the computer-centric era, IT-centric era and information-centric era. Through these eras, the security controls protecting the computer and information-related assets, also evolved. Physical controls formed the core of the protection controls during the computer-centric era. Technical controls started to play a very important role during the IT-centric era. However, in the information-centric era, where all companies became very dependent on their information resources and most users got direct access to IS, the operational controls such as security policies, procedures, standards and guidelines started to play a major role.

From the above, it seems that information has grown to become the lifeblood of all companies today; therefore, they must ensure that they have sound security controls in place to maintain the confidentiality, availability and integrity of their information.

2.4.4 Roles and responsibilities for security

For security to be effective, it is necessary that roles, responsibilities and authorities are clearly communicated and understood by everyone in the company (IFAC 1998). In addition, these roles and responsibilities should cover all aspects of security, as well as the individual responsibilities of all parties using the company's IS (Hone and Eloff 2002). The DTI Information Security Policy Team (DTI 2004b) indicated that responsibilities may vary according to the company's size and nature i.e. some smaller businesses may not need a full-time information security manager, while large companies may need to employ a team to support the role of a full-time information security manager. Consequently, every company has its own unique needs and must assign its own security functions in the most appropriate manner to its employees.

However, the literature reveals that some academics and practitioners consider security as the responsibility of employees at all levels in the company, while others

focus only on the role of accountants in security. The OECD Guidelines for the Information Systems and Networks (OECD 2002) stated that all participants who develop, own, provide, manage and use IS and networks are responsible for these IS and networks' security. Those participants should understand their security responsibility and should be accountable in a manner appropriate to their individual roles. They should also review their own policies, practices, measures and procedures regularly and assess whether they are appropriate to their environment.

In addition, the DTI Information Security Policy Team (DTI 2004b) stated that all staff within the company should know who is nominated to fulfil the security roles and what their responsibilities are in this respect. For example, the CEO should provide management direction and support for information security and formally approve the company's security policy; the information security policy owner should be responsible for the distribution and review of the policy; the senior management should support and implement the policy, and ensure staff are aware of their responsibilities. In addition, the information security manager should ensure that the security policy is properly implemented and the users should follow the security policy and procedures.

The IFAC International Information Technology Guidelines (IFAC 1998) added other responsibilities for security. For example:

- Data owners should classify data according to their sensitivity and should maintain the accuracy and integrity of the data existing in the IS;
- Process owners should ensure that appropriate security, consistent with the company's security policy, is embedded in their IS;
- Technology providers should assist with the implementation of information security; and
- IS auditors should provide independent assurance to management on the appropriateness of the security objectives, and whether security policy, standards, measures, practices and procedures are appropriate.

In addition, the Information Systems Audit and Control Association (ISACA 2005) confirms that senior management should communicate that every employee is accountable for information security by ensuring that expectations are clearly

communicated in the company's information security policies and demonstrate that violations will not be tolerated. Pironti (2005) also stated that the Chief Information Security Officer is responsible for all elements of the information security program, establishing threat level for the entire company and also reporting to senior management.

From the above, it is clear that there are many security roles and responsibilities and these roles are now gaining more importance in the upper levels of the company.

On the other hand, other studies have addressed the accountants' security roles and responsibilities. Chandra and Calderson (2003) indicated that the accounting function is often charged with the responsibility of securing organisational assets including information. Consequently, the accounting profession has developed various control frameworks that identify risks and security measures related to business information resources and other assets such as the Canadian Institute of Chartered Accountants (CICA 1998), COBIT (2000) and SysTrust (AICPA 2002). These frameworks challenge the accounting profession to design and maintain control systems in a manner that safeguards a company's IS.

From the above, it seems that the accountant's responsibility for security extends beyond the accounting information to include all company information, whether financial or non-financial.

Bagranoff *et al.* (2005) confirmed this fact and argued that AIS now are concerned with non-financial as well as financial data and information. Consequently, accounting is a company's primary producer and distributor of many different types of information. Romney and Steinbart (2003) also stated that AIS primary objective is to assist management in the control of a business organisation. Thus, the accountant can help achieve this objective by designing effective control systems and by auditing or reviewing the existing control systems to ensure their effectiveness. Consequently, management expects accountants to take a proactive approach in eliminating system threats, and to detect, correct, and recover from threats when they occur.

From the above, it is clear that accountants play a significant role in maintaining the security not only of AIS, but also for IS and the company as a whole. Accountants are important members of the team that develops and modifies IS. In addition, Qureshi and Siegel (1997) stated that accountants must insist on security controls within their companies and on their recommendations to clients. Accountants should be familiar with security risks and advise everyone in the company about those risks. Moreover, Davis (1997) suggested that accountants could work with systems designers to develop adequate security measures as the technology evolves rather than waiting until the technology has been implemented. Accountants also could educate management and system users on all AIS security aspects.

Despite the important role of accountants in AIS security, companies must ensure that employees at all levels and in every function receive an adequate security training and awareness, and that all parties (managers, employees and other users) understand the company-wide impact of lax security.

2.4.5 Principles of security

There is a wide agreement among academics and practitioners regarding the principles of security. Abu-Musa (2002b), DTI (2004a and b), Fried (1994), the IFAC International Information Technology Committee (IFAC 2002) and Kruger and Kearney (2006), among others, stated that the principles of security are most frequently expressed in the triad of confidentiality, integrity and availability.

Confidentiality is "the characteristic of information being disclosed only to authorised persons, entities, and processes at authorised times and in the authorised manner". Integrity is "the characteristic of information being accurate and complete and the information systems' preservation of accuracy and completeness". Availability is "the characteristic of information and supporting information systems being accessible and usable on a timely basis in the required manner" (Poore 1999, p.35).

In addition, the IFAC International Information Technology Committee (IFAC 2002) addressed three more principles for accounting information security, namely authenticity, authorisation, and non-repudiation. Authenticity relates to the traceability of a business transaction to the individual who initiated it. Authorisation means that

only authorised persons may access certain data, information and systems, and use the rights defined for this system. Non-repudiation relates to the difficulty for a person initiating a transaction to deny its validity given that the transaction was unintended or unauthorised (IFAC 2002). The National Information Systems Security Glossary (NSTISSI 4009 2000, p.39) also defined non-repudiation as "assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data".

Furthermore, Abu-Musa (2002b) mentioned three more principles of information security, namely, validity, privacy and accuracy. Validity refers to the total accuracy and completeness of information. Privacy can be assured by imposing rules of confidentiality for the use of personal data that are safeguarded by security actions and functions (Parker 1981), whereas accuracy refers to the maintenance of the data's legitimate relationship to what it represents.

From the above, it can be concluded that there are main principles of information security in general and accounting information security in particular upon which most academics and practitioners agree, namely confidentiality, integrity and availability. There are supplementary principles as well that include authenticity, authorisation, non-repudiation, validity, privacy and accuracy.

Despite this wide agreement regarding the main group of security principles, some authors, sometimes consider them as security objectives and they have presented other security principles. The IFAC International Information Technology Guidelines (IFAC 1998) indicated that the security objective is supported by eight core principles, namely accountability, awareness, multidisciplinary, cost effectiveness, integration, reassessment, timeliness and social factors. In addition, the OECD Guidelines for the Security of Information Systems and Networks (OECD 2002) provided nine principles for IS and networks security, which are awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment.

On the other hand, the International Information Security Foundation have organised the generally accepted system security principles into a three-level hierarchy:

pervasive principles, broad functional principles and detailed security principles (Poore 1999). The pervasive principles provide general guidance to establish and maintain information security and include accountability, awareness, ethics, multidisciplinary, proportionality, integration, timeliness, assessment and equity. It is clear that there are some common principles for both the IFAC (1998) and the OECD (2002).

The broad functional principles represent the conceptual goals of information security. They include information security policy, education and awareness, accountability, information management, environmental management, personal qualifications, system integrity, information systems life cycle, access control, operational continuity and contingency planning, risk management, network and infrastructure security, legal, regulatory and contractual requirements of information security and finally, the ethical practices. On the other hand, the detailed security principles specifically address methods of achieving compliance with the broad functional principles with respect to existing environments and available technology.

It seems that these principles can not only provide general guidance and represent the conceptual goals of information security, but can also disclose, almost all the information security dimensions. However, there are other important security dimensions mentioned in the literature which must be considered.

2.4.6 Other dimensions of security

These days, it is quite widely accepted that security has moved away from its technical image, and has a wide range of other aspects that must be taken into account in creating a secure IT environment in a company. Tryfonas *et al.* (2001) indicated that information security is a field combining technical aspects as well as social, cultural and legal or regulatory aspects, whereas Schultz (2005, p.426) addressed the human factor in security and stated that "People are in control of technology, not vice versa". Chang and Yeh (2006) also indicated that effective information security should address both IT and non-IT related issues instead of simply considering IT systems.

Ekenberg *et al.* (1995) presented some models that can reveal many aspects of security. First, security could be structured according to what is to be protected (the kinds of targets) into personal, physical, information, functional, environmental and business security. Second, is the traditional organisational-oriented approach in which the security field could be divided into physical, information and personnel security. Third, is the event/threat-oriented approach (WAECUP approach) where adverse events (threats) are grouped into five major categories: waste, accident, error, crime and unethical/unprofessional practices. Finally, the fourth is the process-oriented model which includes generic security functions i.e. functions that are used to carry out all security activities and include prevention, protection, enforcement, investigation, inspection, detection, reporting and deterrence.

Furthermore, in a more recent study Von Solms (2001) provides a holistic and comprehensive view of security and presents many security dimensions, namely the strategic/corporate governance, governance/organisational, policy, best practice, ethical, certification, legal, insurance, personnel/human, awareness, technical, measurement/monitoring/metrics and audit dimensions. It is clear that Von Solms considered most of the important security dimensions. By identifying these dimensions, realising their importance, and considering them in securing a company, Von Solms makes it easier to understand the complexities of information security, and to approach information security in a structured way (Von Solms 2001).

2.4.7 Factors affecting security

The literature reveals that many factors can have a significant effect on security. Lindup (1996) stated that technology is one such factor. The changes in technology not only create new opportunities, but also affect the way business is done. Technology can have an impact on security in three ways: by introducing new security vulnerabilities, by changing the way business is done, and by changing the way the workplace is organised. If managers are to succeed in providing the security required by a company, they must look at the broad changes in existing technologies, and the security implications of a new technology.

Wiant (2005) provided three factors that contribute to good security measures in a company, namely sufficient budget, time to focus on security and staff to focus on

security. Wang (2005) also presented some dynamic forces that interact with each other and have significant impacts on security. These forces include:

- Internal competition in information security i.e. the conflicts among different departments, since security costs money, effort and time;
- Suppliers' power i.e. suppliers are a key element in information security strategy, without them, security falls apart;
- Complements i.e. internal audit department, compliance department and external regulatory bodies help the business focus more on information security;
- Customer power i.e. customers of information security in the company are mainly senior management and business functions that deal with IT and information, since management controls the security budget; and
- Threats of entry relating to the information security services i.e. outsourcing.

On the other hand, Gansler and Lucyshyn (2005) stated that providing adequate IS security could be a challenge for the following reasons:

- The security landscape is constantly changing, since the number of companies and users on the internet is ever increasing;
- Although in the past, a great deal of technical sophistication was required to penetrate a computer network, now attacks are possible by much less well-informed attackers;
- Improving internet security is, to a great extent, hard; and
- Users are commonly known to be bad at considering risk.

In another study, Finne (1996) addressed many factors that affect a company's information security. He presented these factors in the form of 12 modules that together form a company's information security. These modules include computer security, operation security, protection against theft, fire and water damage, electricity distribution, external and internal threats, communication, contingency planning, personnel security, incident reporting and attitudes towards information security issues. It is clear that some factors represent security controls that affect security positively and the others are security threats that affect security negatively.

On the other hand, the ISO/IEC 17799 (2005) and Von Solms (1998) presented some factors that are critical to the successful implementation of information security within a company. These factors are:

- Security policy, objectives, and activities that reflect business objectives;
- A framework for implementing, maintaining, monitoring, and improving security that is consistent with the organisational culture;
- Visible support and commitment from all levels of management;
- A good understanding of the information security requirements, risk assessment and risk management;
- Communicating the information security policy and standards to all interested parties;
- Providing appropriate security training and awareness;
- Establishing an effective security incident management process; and
- Implementing a measurement system for evaluating the performance regarding the security management.

However, despite the importance of these factors, they are just the starting point for implementing security and every company should consider the factors consistent with its objectives and activities.

2.4.8 Security management

Information and IS security have become an important part of the core business processes in every company. Companies are faced with contradictory requirements to deal with open systems on the one hand and assure high protection standards on the other hand (Trcek 2003). The implementation and management of information and IS security, therefore, required a structured and disciplined process (Vermeulen and Von Solms 2002).

Eloff and Von Solms (2000) indicated that IS security management is a stream of management activities that aim to protect the IS and create a framework within which such systems operate as expected by the company. Nyanchama (2005) also stated that information security management is a process that includes planning, execution, monitoring and feedback (Information Security Life Cycle). It addresses security risks in a company. It involves the visioning, planning and execution of a security

management program with a view to minimising these risks. It also involves strategy, tactics and the operations of a security program and is predicated upon continuous improvement. In addition, IS management aims not only to protect information and IS but aims to ensure the continuity of the company (Karyda *et al.* 2005).

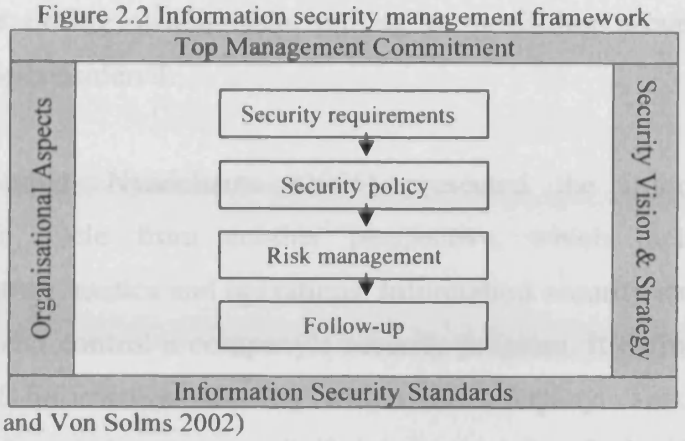
On the other hand, Fulford and Doherty (2003) argued that effective information security management depends on a number of key factors. These factors include: the need for senior management commitment and support, assessment of potential security risks and threats, implementation of appropriate controls to minimise those risks and threats and the communication of all security issues to information and IS users through relevant education and training.

On the other hand, Vermeulen and Von Solms (2002) indicated that information security management should be treated like any vital business function with all its activities based upon business needs and backed by the company's top management, who carry the ultimate responsibility of this information. They presented a framework for information security management as shown in Figure 2.2 below.

Figure 2.2 shows the different elements of information security management that can be classified into three phases: preparation, implementation and maintenance. The preparation phase includes:

- Top management commitment, given that management is ultimately responsible for information security and their support is essential for resources allocation and for gaining employees support for security;
- Information security standards, given that they can provide companies with an approach to information security management;
- Organisational aspects of information security, given that an effective security management requires the responsibility of certain staff to implement it; and
- Security vision and strategy in order to ensure the integrated implementation of the information security management.

Figure 2.2 Information security management framework



(Source: Vermeulen and Von Solms 2002)

The implementation phase includes the company's security requirements, the development of an information security policy and risk management. The maintenance phase includes the follow-up element, given that the information security management is an ongoing process and not merely a one-off activity.

The DTI Information Security Policy Team (DTI 2004a) provided a process cycle for the information security management that includes four phases. First, design the management system, including identification of business requirements, assessments of risks and impacts, establishment of information security policy and selection of adequate controls. Second, implement the management system, including implementation of controls and procedures, allocation of resources and responsibilities and training and awareness. Third, monitor, review and reassess the management system, including effectiveness of controls and procedures, business changes, incident reports and risks, threats and impacts; and finally improve and update the management system, including corrective or preventive actions to improve existing controls or to implement new controls.

From the above, it seems that information security management frameworks or cycles are, to a great extent, similar and they include all the necessary elements required for an effective information security management within a company. In addition, Karyda *et al.* (2005) agreed with these frameworks and indicated that the IS security management includes a planning phase, an implementation phase during which security plans are put into action, an assessment or audit phase and finally an

awareness phase during which tasks aiming at providing security training and education must be considered.

On the other hand, Nyanchama (2005) presented the information security management life cycle from another perspective, which includes three key components: strategy, tactics and operations. Information security strategy is a means to define, direct and control a company's security program. It defines the scope and accountability of information security within the company. Tactical components ensure that security requirements are built into programs and specific projects, from design to implementation, whereas operations include monitoring of the security infrastructure and proactive assessment and response to incidents and vulnerabilities.

It is clear that, if properly implemented, security management enables a company to reduce security risks to acceptable levels, to satisfy the legal, regulatory and contractual requirements, to take proactive action to protect information and IS across the entire company, to increase productivity, to enhance the overall security posture, and most importantly, to ensure the continuity of the company. Thus, because of the importance of security management, it is essential to discuss some of its main elements (security requirements, program, policy, training and awareness, risk assessment, incident handling, business continuity plans, security budget, standards and certification and security effectiveness) in more detail.

2.4.8.1 Security requirements

In order for companies to implement an appropriate set of controls and manage security effectively, various security requirements need to be considered. Gerber and Von Solms (2005) indicated that security requirements are concerned with the amount of security required for the effective protection of information resources. However, to ensure that the correct level of security is obtained, security requirements need to be determined based on the unique characteristics of each company.

The literature reveals that there is wide agreement among academics and practitioners concerning the main security requirements. Gerber and Von Solms (2001; 2005) and the ISO/IEC 17799 (2005) have presented three main sets of security requirements. The first is derived from assessing a company's risks, which could lead to significant

losses in business if they occur. The second addresses the legal, statutory, regulatory and contractual requirements that a company, its partners, contractors and service providers have to satisfy, whereas the third includes the set of principles, objectives, procedures and business requirements for information processing that a company has developed to support its operations.

On the other hand, Posthumus and Von Solms (2004) have indicated that security requirements stem from sources both internal and external to a company, where the external requirements include information security standards and best practices, and legal and regulatory issues associated with security. However, the internal requirements are concerned with a company's personal internal needs for ensuring confidentiality, integrity and availability of their sensitive information, and those requirements for protecting the critical infrastructure that forms the "information backbone" of most companies today. These external and internal requirements therefore help to address the various important aspects of risks that most companies face. In addition, these requirements together with the accepted security standards and other best practices form the basis of an effective approach to information security. Consequently, information security requirements have become a primary force to determine the security controls needed to manage security effectively.

2.4.8.2 Security program

Information security has matured from a concept that is dealt with technically and is event-driven, to one that is approached from a business perspective and is process-driven (Pironti 2005). An information security program is the best approach to reach this goal. The existence of a security program is the cornerstone of an effort to transform security into a proactive activity driven by the business leadership, instead of a reactive one driven by the technologists within a company. By introducing a structured approach to information security, a company can increase its security posture and reduce security costs. It can also gain advantage in its efforts to ensure compliance to security standards and regulations (Pironti 2005).

The literature reveals that there is a wide agreement among academics and practitioners regarding the key elements of an effective information security program. The USA General Accounting Office (GAO 1998; 2004) and the National Institute of

Standards and Technology (NIST 2005) stated that an effective information security program should include:

- Periodic assessments of risks, including the magnitude of harm that could result from unauthorised access, use, disclosure, modification or destruction of information and IS that support a company's operations and assets;
- Policies and procedures that are based on risk assessments, that reduce risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each company's IS;
- Subordinate plans for providing adequate security for networks, facilities or IS;
- Security training and awareness to inform personnel of security risks associated with their activities and responsibilities;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices and security controls;
- A process for planning, implementing and evaluating corrective actions to address any deficiencies in policies, procedures and practices;
- Procedures for detecting, reporting and responding to security incidents; and
- Plans and procedures to ensure continuity of the company's IS operations.

However, there are several challenges that companies must overcome to implement security programs successfully (Booker 2006). They include the time and cost necessary to establish a database of critical networks and information assets, and the lack of synergy given that separate technical teams can be responsible for the management of different technical controls. In addition, although different security approaches are demanded by local regulatory and business requirements, the company's global policies and practices must still be consistently applied.

On the other hand, Garcia (2006) argued that in order to increase the effectiveness of the information security program, security must be a business priority for the top management. Security requires a continuous improvement process that includes techniques to measure effectiveness, and it should be a company-wide priority with security responsibility and accountability established at all company levels.

Furthermore, the Information Systems Audit and Control Association (ISACA 2005, pp.9-10) provided two groups of critical elements of information security program

success: priority and additional critical elements. The priority critical elements include senior management commitment to and support for information security initiatives, management understanding of all security aspects, security planning prior to implementation of new technologies, integration between business and information security, alignment of security with a company's objectives, and executive and line management ownership and accountability for implementing, monitoring and reporting on information security. On the other hand, the additional critical elements include employee training and awareness on security issues, consistent enforcement of security policies and standards, placing security within a company's hierarchy, information security budget, ability to cost-justify security and generally accepted best practices for information security.

The above shows the importance of an information security program within companies today. In addition, most academics and practitioners agree on the critical elements of these security programs and on their importance.

2.4.8.3 Security policy

There is a wide agreement within the academic and practitioner communities that a security policy is the basis for the dissemination and enforcement of sound security practices within a company (Doherty and Fulford 2006). Security policy is at the heart of any information security strategy (Eveloff 2005). It is the start of security management (Higgins 1999). Security policy is the first and most important layer of security available to a company (Whitman 2003).

According to D'Arcy and Hovav (2007), a security policy includes statements of organisational goals and beliefs, existing controls and employees' responsibilities. Their purpose is to provide detailed guidance to users regarding acceptable use of organisational IS resources in order to ensure a safe environment. Walker (1985, p.62) stated that a security policy is "the set of laws, rules and practices regulating how an organisation manages, protects and distributes sensitive information". It is a direction-giving document for security within a company, it demonstrates management commitment to and support for information security, as well as defining the role information security has to play in reaching the company's objectives (Hone and Eloff 2002). Wood (1995) argued that policies are high-level statements intended

to provide guidance for decision makers. Further, Gaston (1996) stated that information security policy is a broad guiding statement of goals to be achieved with regard to the security of corporate information resources. Consequently, security policy is a vital part of a company's strategy for achieving IS security. It explains the need for IS security to all the company's information resource users.

Hong *et al.* (2003) indicated that an information security policy aims at planning security requirements, forming consensus in a company, drafting and implementing a policy and reviewing the policy on a regular basis in order to meet the organisational security requirements. Whitman (2004) also indicated that a good security policy should outline responsibilities, define authorised and unauthorised users of IS, provide venues for employee reporting of system threats, define penalties for violations and provide ways for updating the policy.

In addition, Higgins (1999) argued that without a policy, security practices would be developed without a clear distinction of objectives and responsibilities. Moreover, Wood (1995) pointed out that security policies are important in assuring the proper implementation of controls, guiding the security product selection and development process, demonstrating management support for information security, avoiding liability for inadequately addressing security matters and achieving consistent and complete security within a company.

However, despite the importance and the vital role that the security policy plays in a company, many academics and practitioners have argued that it is not always easy to put this document together. There are often different opinions within a company as to what constitutes a policy. Many questions are asked as to what should be incorporated into this document, what it should look like, how long it should be, who needs to approve it, etc.

First, it is important to know that a company's security policy depends on various factors including, among others, the value and sensitivity of information, the impact that the loss or misuse of information would have on the company and its legal requirements (Steinke 1997). In addition, Karyda *et al.* (2005) provided some factors that affect the formulation and implementation of security policy including the

organisational structure, security culture within a company, management active participation and visible support, ongoing security training and awareness program, and the continuous evaluation of the effectiveness of the security policy. It is clear that all these factors are important and affect the formulation, implementation and adoption of a company's security policy.

Moreover, the literature reveals that there is no clear agreement regarding the procedures involved in establishing a security policy. Lindup (1995) suggested seven steps for developing and implementing a security policy that begin with formulating a draft policy, followed by a period of internal discussion, deciding the final content of the policy by the information security officer, formally accepting the policy by the CEO, disseminating the policy throughout the company, monitoring compliance by internal auditors and finally, taking action in case of non compliance.

In addition, Kabay (1996) presented five procedures for establishing a security policy including assessing and persuading top management, analysing information security requirements, forming and drafting a policy, implementing and maintaining the policy. Furthermore, Karyda *et al.* (2005) argued that a security policy must combine technical and organisational guidelines addressing security requirements at the organisational level. In addition, the formation of a security policy includes the process of policy formulation, implementation and adoption. However, despite all these steps and procedures for establishing a security policy, a question remains as to "what constitutes a policy?"

There is wide agreement in the literature regarding what can be included in a security policy. The DTI Information Security Policy Team (DTI 2004b), the IFAC International Information Technology Guidelines (IFAC 1998) and Trcek (2003) indicated that, as a minimum, a security policy should include:

- The scope, objectives and importance of information security to the company;
- A statement indicating management support for the security goals and principles;
- Brief statements indicating minimum standards, procedures and requirements for specific security issues e.g. consequences of security policy violations, legal, regulatory and contractual requirements; security training and awareness, security breach detection, and business continuity planning;

- Definitions of general and specific security roles and responsibilities;
- Details of the process for reporting and responding to security incidents; and
- References to more detailed security policies, procedures, or standards.

In addition, Hone and Eloff (2002) have suggested other elements to be included in a security policy such as the approval of security policy, the purpose of security policy, the user declaration and acknowledgement and other general elements such as the authors, date of policy and review date of this policy. Although these elements may not be considered the main elements of a security policy, they can still ensure its official status within a company.

To achieve its objectives, certain characteristics should be considered in writing a security policy. It should be short and easy to read, the writing style should reflect the organisational culture, the policy should be clear and comprehensible to all users in a company, and it should be reviewed periodically after major technological changes and regulatory requirements to ensure that it remains current as well as relevant to the company's security objectives. Above all, a policy must be realistic (Hone and Eloff 2002).

However, despite all this concern, a security policy sometimes fails to play an important role in a company. Doherty and Fulford (2005) gave some reasons for such ineffective policy implementation, namely the difficulties of raising employees' awareness of a policy, difficulties of enforcing the policy, complexity of applying the policy standards, insufficiency in resources available for policy enforcement and a failure to tailor policies as a result of greater reliance on international standards.

Many previous studies were also conducted to investigate the vital role of a security policy from different perspectives. Fulford and Doherty (2003) conducted a study to investigate the uptake, content, dissemination and impact of information security policies in UK companies. A questionnaire was developed in three sections. The first section investigated the existence, dissemination and the frequency within which a security policy is updated. The second section focused on the coverage of a security policy, and the third section addressed the factors affecting a policy success. In another study, Doherty and Fulford (2005) explored how a variety of issues relating

to the uptake and application of security policies for instance existence, age, updating and how the scope of a security policy impacted upon the incidence of security breaches within large companies.

Wiant (2005) conducted a study to examine the effectiveness of an information security policy in influencing the reporting of both computer abuse incidents and the associated seriousness of those incidents. In addition, Hong *et al.* (2006) investigated the dominant factors of building an information security policy and the effect of this policy on elevating a company's security level. A questionnaire was developed to collect information about the information security policy establishment and the policy's function, contents and implementation items.

It can be concluded that the information security policy is one of the most important documents in a company, the heart and basis of successful security management and a guideline that dictates the rules and regulations of a company regarding all security aspects. Therefore, policies must be written with due care.

2.4.8.4 Security training and awareness

According to the Information Security Forum (ISF 2007), security awareness is the extent to which every member of staff understands the importance of information security, the levels of security appropriate to the company, their individual security responsibilities and how to act accordingly. There is wide agreement in the literature that effective information security begins with awareness. Awareness of the risks and available safeguards is the first line of defence for IS security (OECD 2002). Von Solms (2000) argued that employees are in most cases the biggest threat to a company's IS. Consequently, combating employees' ignorance has motivated companies to start with a comprehensive security awareness program. In addition, due to the intensified need for improved information security, many companies have established security awareness programs to ensure that their employees are informed and aware of security risks, thereby protecting themselves and their profitability (Kruger and Kearney 2006). Peltier (2005) added that an effective security program cannot be effected without implementing employee awareness and training program to address policy, procedures and tools. Moreover, Eveloff (2005) argued that employee training and awareness is the most important of all information security

measures and indicated that employees should receive ongoing training on common security risks encountered in the workplace, what risky activities to avoid and when and how to report security problems.

Given the important role of security training and awareness programs, many studies have been conducted to explore this issue. Thomson and Von Solms (1998) highlighted the need for education in the workplace through a security awareness program and provided some techniques borrowed from the field of social psychology that could be utilised to improve the effectiveness of the awareness program and which have been largely ignored in current awareness programs. Siponen (2000) provided a conceptual foundation and a framework for IS security awareness. This study outlined the behavioural framework including selected motivation/behavioural theories. It also addressed how people respond to awareness activities and the methods available to increase awareness. In another study, Peltier (2005) identified the elements that make up a successful security awareness program, the role that employees play in this program, how to establish the scope of awareness program, how to segment the audience and how to ensure that the content is effective in getting the message to the users.

In addition, Kruger and Kearney (2006) provided a model for measuring information security awareness in companies that may assist in providing feedback to the top management on the success of a security awareness program, and may assist them in their function of controlling and directing security strategic objectives. They argued that risks continuously change and consequently any awareness program needs to be measured and managed on an ongoing basis. Moreover, Chen *et al.* (2008) conducted an inter-cultural study to investigate if users from the USA and Taiwan exposed to the same situational awareness learning would have a different performance in security awareness outcomes. The findings revealed that American users who received situational security awareness training outperformed those users who received traditional face-to-face instructions. However, Taiwanese users did not perform significantly differently between these two techniques. They concluded that awareness of risks and safeguards is the first line of defence in any company; however, how risks are addressed can be dissimilar in different cultures.

In another study, Kritzinger and Smith (2008) proposed a conceptual view of an Information Security Retrieval and Awareness (ISRA) model that can be used by industry to enhance security awareness among employees. This model consists of three parts, namely the ISRA dimension (non-technical security issues, IT authority levels and information security documents), information security retrieval and awareness, and measuring and monitoring. This model focuses on non-technical security issues because compared to technical issues these have always been neglected.

Despite the importance of employees' security training and awareness in all companies today, the previous studies revealed that security training and awareness is the countermeasure most neglected by companies compared to other security practices. This is further discussed in the following chapters.

2.4.8.5 Risk assessment

The Department of Trade and Industry (DTI 2004a, p.6) defined risk assessment as "the assessment of threats to, vulnerabilities of, and impacts on information and information processing facilities and the likelihood of their occurrence. Risk assessment includes the identification, analysis and management of risks". Since business risks arise from both internal and external sources and they evolve and change overtime, risk assessment provides a basis for deciding how to manage those risks (Amoruso *et al.* 2005).

Gomez and Paxmann (2006) indicated that companies are requested to perform risk assessment for their financial risks. In addition, to be compliant with ISO 27001, companies must demonstrate the establishment and use of risk assessment methodology relevant to the business, considering information security, legal and regulatory requirements (Kouns 2007).

The literature underlines the important role of risk assessment in organisations. Risk assessment allows the determination of an acceptable level of risk and assists in the selection of appropriate controls to manage the risk of potential harm to IS in light of the nature and importance of the information to be protected (Finne 1998; OECD 2002). Kouns (2007) argued that if a company has a well-structured risk assessment

framework, it could not only minimise the negative impact from threats, but also maximise the positive impact from opportunities. A well-implemented control may provide security for a time, but a well established risk assessment methodology will provide the means for a company to protect the business at all times.

In addition, Poore (1999) stated that the risks to information and IS should be assessed periodically. Periodic assessment identifies and measures the variances from available and established security controls and the risk associated with such variances. Since threats change overtime, it is important that companies periodically reassess risks and reconsider the appropriateness and effectiveness of the policies and controls they have selected (GAO 1999).

Given the importance of risk assessment, many studies have been conducted to investigate this issue. Kotulic and Clark (2004) proposed and tested a theoretical model to study the process that leads to effective Security Risk Management (SRM) programs. The description of the model, the methodology designed to test the model, and the problems faced while testing the model were presented. However, given their poor response rate, they concluded that information security research is one of the most intrusive types of organisation research, and they recommended a cautious approach for security studies that are of such a sensitive nature. In another study, Sherer and Alter (2004) pointed out that IS risk literature produced several hundred risk factors and many overlapping risk components that are difficult for managers to access and use in a meaningful way. As a result, they focused on organising these risk factors to make them more useful and meaningful for business managers using nine elements namely work practices, participants, information, technologies, products and services, customers, environment, infrastructure and strategies.

Gerber and Von Solms (2005) argued that the evaluation of risk related to IT alone is unrealistic and a holistic view of assessing risks should instead be adopted. Consequently, they suggested an alternative more comprehensive approach to risk analysis and investigated the factors that this alternative approach should include in order to manage risks holistically. Their approach proposed to analyse not only risks to tangible assets, but also risks to information or intangible assets, while considering risks posed due to cultural, legislative and other sociological issues.

Moreover, Tsohou *et al.* (2006) examined the potential of cultural theory as a tool for identifying patterns in the stakeholders perceptions of risk and its effect on IS risk management. They adopted a model for the risk management process based on Frosdick (1997), ISO/IEC 27001 (2005), and NIST 800-30 (2002), which includes three risk management stages namely initiation, risk analysis (risk identification, estimation and evaluation), and risk mitigation (designing, implementing and monitoring). In another study, Lindberg (2006) proposed a simplified risk management model that will provide quantitative results based on subjective human inputs. This model includes six steps: risk element definition (identifying risks), impact rating (impact on the company when a loss is experienced), likelihood rating (probability of negative event), existing countermeasures rating, risk level calculation (based on impact, likelihood and countermeasures), and risk level reporting.

More recently, Zhou *et al.* (2008) presented an IS project risk checklist that aims at supporting risk assessment, decision making concerning risk control, and planning of risk mitigation strategies in the public sector. The proposed risk checklist includes five main risk dimensions, namely pre-project (requirement specification, contractual relationships, project planning and organisational environment), customer (internal and external environment, end-user and management), project management (human resources, project planning, monitoring and reporting), technological issues (IS infrastructure) and development (systems analysis, design, development, testing, installation and maintenance).

From the above, it can be concluded that security risk assessment has become a major concern and plays a vital role in security management within all companies today.

2.4.8.6 Incident handling, disaster recovery and business continuity plan

An incident handling plan is a document that guides a company in continuing its operations at either full or reduced capacity following the occurrence of disruptive events and in dealing with the consequences of these occurrences in the context of its IS security requirements (Warigon 1999). Incidence response is the process that attempts to minimise the damage from security incidents and malfunctions that inevitably occur in a corporate environment, monitors and learns from such incidents (BSI 1999). According to the DTI Information Security Breaches Survey (DTI 2006),

there has been a rise in the number of UK businesses that have formal procedures to respond to security incidents when they arise. More recently, the BERR Information Security Breaches Survey (BERR 2008) also revealed that more UK businesses have procedures to respond to security incidents than two years ago, with four fifths of large businesses reporting their existence.

Moreover, disaster recovery and business continuity planning is the process of implementing procedures to assure the availability of IS processing capabilities in the event of a disaster (Ward and Smith 2002). The rapidly changing business, regulatory and threat environment to which most companies are exposed requires that sustained efforts be made to ensure the ongoing availability of a reliable business continuity plan for critical business processes and services (CICA 2005). The goal of a business continuity plan is to preserve and protect the essential elements of a company and maintain an acceptable level of operations throughout a disaster and afterwards as the company recovers (Rodetis 1999). In addition, it ensures the availability of plans to counteract or minimise the impact of interruptions to business activities caused by the unavailability of IS (Ward and Smith 2002).

There is wide agreement in the literature that a disaster recovery and a business continuity plan must be tested and be kept current. Rodetis (1999) argued that business continuity plans must be "living documents", they should be updated constantly and require a full time specialist. Smith (2004) indicated that a business continuity plan must be well documented and tested frequently. Since companies frequently change to keep up with new technologies, new internal and external policies, and new ways of doing business, a business continuity plan must be checked regularly to keep pace with this change. Without testing, the adequacy of the plan remains unknown. Testing helps to assess the viability of the plan, identify and correct any deficiencies, and evaluate the capabilities of the response teams (Landry 2006, Woodman 2007).

The DTI Information Security Breaches Survey (DTI 2006) stated that UK businesses appear better protected against disasters than two years previously. There has been an increase in the number of companies with disaster recovery plans. However, two fifths still do not have a disaster recovery plan in place. In addition, the BERR

Information Security Breaches Survey (BERR 2008) revealed that although disaster recovery plans are increasingly common, only half of the plans were tested in 2007. This leaves these companies ill prepared to respond to challenges facing them during a disaster.

Few studies have been conducted into the incident handling, disaster recovery and business continuity plan issues. Nosworthy (2000) presented a practical risk analysis approach as part of the development of a structured business continuity management (BCM) programme. Nosworthy argued that in order to apply business continuity measures in a consistent, manageable and cost effective manner a company-wide approach to a business continuity risk analysis should be applied to the business as a whole and not just the IT department. Gerber and Feldman (2002) offered advice to companies on how to select a team and develop a plan that will ensure their ability to remain in business in the event of a disaster. They indicated that the first step is to choose a crisis management team that includes the company's executive, financial officer, human resources representative, IS or technology officer, risk management representative, public relations representative and internal and external legal counsel. The second step is to create a risk management plan that incorporates procedures intended to first prevent or mitigate disasters of all kinds and the third step is planning how to handle the crisis. Moreover, Hancock (2002) addressed the basics of security crisis management and the logical steps required to ensure that a crisis does not get out of hand namely determining if a crisis really exists, determining the damage and extent of the crisis and managing the crisis.

The Canadian Institute of Chartered Accountants (CICA 2005) presented the issues that need to be addressed as part of a company's overall business continuity plan in order to ensure the rapid recovery of its critical IS and services. Bhaskar (2005) proposed an integrated framework for coordinating computer security incident response teams (CSIRTs) to get a company's computer related infrastructure back to an operational condition as soon as possible. In another study, Smith and Jamieson (2006) investigated the key drivers and inhibitors for IS security and business continuity management in e-government using the data collected from a cross section of government organisations. The main issues that appeared relevant to a large number of organisations as key drivers or inhibitors for IS security and business

continuity management were training and awareness, management support and appropriate funding. In addition, Vael and Neyer (2006) addressed business continuity mismanagement. They presented the challenges facing companies during a disaster including lack of senior management support, lack of supporting technology with the potential financial, operational, reputation, and legal impacts if processes are not resumed in a timely manner, lack of understanding of risk exposures and of the process of eliminating, mitigating or accepting them, wasted investments, missing time frames with suppliers and customers and the inability to manage expectations of the board, shareholders, customers, business partners, regulators and employees.

In a recent study, Mitropoulos *et al.* (2007) explored the nature of security information management systems (SIMS) while proposing a set of requirements that could be satisfied by these systems for the efficient and effective handling of security incidents. They proposed incident response (IR) policy requirements for SIMS, a role-based access control approach for a corporate IR capability with the use of the system, and various mechanisms that could be mandated by appropriate policies for enhancing the overall security of SIMS. Moreover, Fonseca (2007) addressed the human factor in business continuity plans and argued that excellent plans can fail because of an often overlooked factor that is human beings.

Due to the increasing security incidents and the rapidly changing business, regulatory and threat environment to which most companies are exposed, it is vital for all types of companies to have security incident handling procedures and business continuity plans in place to deal with these incidents and to assure the availability of IS in the case of a crisis.

2.4.8.7 Security budget

The costs associated with security activities relate to many items including hardware, software and personnel. The main drivers for information security expenditure are to protect a company's information and its reputation (DTI 2006). However, spending the right amount on security continues to challenge UK businesses, since over-expenditure reduces profitability, while under-investment can leave the business exposed. In addition, Willison and Backhouse (2006) indicated that security budget is influenced by management perception.

A review of the literature reveals that security is still perceived as an IT issue. Most companies still do not have a security budget separate from their IT budget (DTT 2007) and the security budget is expressed as a percentage of IT budget. However, according to the results of the Computer Crime and Security Survey (Richardson 2008), not all money in the security budget comes from IT. Increasingly, security is viewed as a problem that is far broader than technology alone. Consequently, in some instances part of the security budget comes from audit and legal departments.

However, Gordon and Loeb (2006) argued that little research had been done about the budgeting process used in deciding how much to spend on security. They, therefore, conducted a study to examine the way companies make decisions regarding security expenditures. They assessed whether companies approach the budgeting process for security expenditures in a rational economic manner based on cost-benefit analysis. Their results showed that some companies depend on a formal net present value analysis, whereas others approach these expenditures with a modified economic analysis that is examining the costs and benefits of information security activities, but with less emphasis on formally quantifying the benefits.

2.4.8.8 Security standards, evaluation and certification

For years, the business community has been searching for an adequate approach or technique for evaluating the security of information and IS, and simultaneously searching for a practical security standard, one that can provide a company with best practices and can be both cost-effective and reasonably achievable.

However, the literature reveals that the evaluation of information and IS security is not an easy task and one in which there is a lot of confusion and inconsistency. Conrath and Sharma (1993) in an extensive study in the IS evaluation literature revealed that there were no generally accepted performance measures. Von Solms (1996) presented a number of evaluation and certification techniques and schemes that can be linked to information security. These techniques are Trusted Security Evaluation Criteria Schemes, ISO 9000 (BS 5750) i.e. the leading international quality assurance scheme, the Code of Practice for Information Security Management (BS 7799) and self- evaluation.

In addition, Abu-Musa (2002c) agreed with Von Solms (1996) and indicated that information security evaluation could be done against one of the following criteria:

- Trusted Security Evaluation Criteria, which includes the Trusted Computer Security Evaluation Criteria (TCSEC), the Information Technology Security Evaluation Criteria (ITSEC), and the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC);
- The ISO 9000 Series of Standards;
- Code of Practice for information security management (BS 7799); and
- Comparisons.

However, Conrath and Sharma (1993) stated that no single measure is adequate, so a combination is necessary to avoid the deficiencies of each method and to enhance the potential benefits through integration of these methods. Consequently, in their study, they combined the checklist questionnaire and the risk analysis methods in evaluating computer based IS.

Furthermore, the literature reveals that many organisations and standardisation bodies have been producing information and IS security standards, guidelines and best practices. The AICPAs and the CICAs developed the SysTrust: Principles and Criteria for Systems Reliability (AICPA/CICA 2001). Thus, a system is reliable when measured against four essential principles: availability, security, integrity and maintainability.

BSI IT Baseline Protection Manual developed by the German Federal Information Security Agency (BSI 2000) presented a set of recommended standard security controls or safeguards. Its goal is to achieve a security level for IT systems that is reasonable and adequate to satisfy normal protection requirements and can serve as the basis for IT systems and applications requiring a high degree of protection (Hone and Eloff 2002).

In addition, the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) technical committees produced the GMITS (ISO/IEC TR 13335) Guidelines for the Management of IT Security. The

ISO/IEC TR 13335 consists of five parts under the general title: Information Technology - Guidelines for the management of IT Security:
Part 1: Concepts and models for IT Security (1996);
Part 2: Managing and planning IT Security (1997);
Part 3: Techniques for the management of IT Security (1998);
Part 4: Selection of safeguards (2000); and
Part 5: Safeguards for external connections (2003).

Moreover, the Information Systems Audit and Control Foundation developed the Control Objectives for Information and Related Technology (COBIT 2000). Its objective is to research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted IT control objectives for day-to-day use by business managers and auditors.

The Standard of Good Practice developed by the Information Security Forum (ISF 2005) provides an achievable target for companies against which they can measure their performance regarding information security management. It examines information security from a business perspective and focuses on how companies can keep the business risk associated with critical IS under control in today's ever-changing technological environment.

In the USA, the National Institute of Standards and Technology (NIST 800-14 1996) developed the Generally Accepted Principles and Practices for Securing Information Technology Systems (GAASP) to provide a baseline that companies can use to establish and review their security programs.

From the above, it is clear that many organisations and standardisation bodies have been producing security standards, guidelines, principles and evaluation techniques. However, most of them are technical and therefore impractical in terms of meeting business needs. Gordan (2005) argued that there was no one standard or set of best practices that had emerged as a generally accepted international security standard.

As the trend in information security has recently changed from technical security controls to a concern for overall risk management, which shifts information from a

strictly IT focus to a business practice issue, one set of standards has come forward that helps organisations in successfully managing risks in this new environment: the British Standard on Information Security (BS 7799).

The British Standard BS 7799 (now ISO 27000) started its life as the UK Department of Trade and Industry (DTI) Code of Practice for Information Security. It was first published in September 1993. In 1995, it became a British Standard and was renamed BS 7799 (Sweren 2006; Von Solms 1999). The original BS 7799 comprised two parts: a code of practice (part 1) and a specification for an information security management system (part 2). In 1999, it was revised with the addition of accreditation and certification components. These components comprise BS 7799 part 2 which was updated in 2002. In 2003, part 1 was fast-tracked through ISO and became 17799 (ISO 17799). Then in 2005, the BS 7799 part 2 became ISO 27001.

Lineman (2005) argued that several changes to business environments and new ways of doing business guided the development of the revised standards. These changes include the growing dependence on the use of external services, changes in risks and threats facing businesses, emerging technologies and greater connectivity and the impact of this on information security, and the growing security requirements for regulatory compliance.

The literature reveals that the British Standard BS 7799 is widely acknowledged as an important framework for security in both the UK and overseas (DTI 2006; Gordan 2005). In addition, in 2007, the ISO built on this standard to create a family of International Standards on Information Security (27000 series). Sweren (2006) presented this series as follows:

- 27000 - Vocabulary and Definitions;
- 27001 - Information Security Management System Requirements (Certification) (replaced BS 7799 part 2);
- 27002 - Code of Practice (replaced BS 7799 part 1);
- 27003 - Implementation Guidance;
- 27004 - Information Security Management Metrics and Measurement Standard;
- 27005 - Information Security Risk Management Standard; and

- 27006- Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.

Security professionals have claimed that ISO 17799 (part 1: Code of Practice) was one of the leading standards of information security. It is a suitable model for information security management and an appropriate vehicle for addressing information security management in modern organisations (Ma and Pearson 2005). In addition, ISO 27001 (part 2: Certification) is the set of requirements for developing an information security management system. This is the standard that a company will need to adhere to in order to receive ISO 27001 certification. Compliance with or certification in ISO 27001 will give the company strong IT-related controls that will also help satisfy the requirements of many regulatory standards. It ensures that the right people, processes and technology are in place that are appropriate to the business and that facilitate a proactive approach to managing security and risk (Brenner 2007). Certification to ISO 27001 assures clients, employees, suppliers, business partners and future customers that a company has a continuous protection methodology allowing a flexible, effective and defensible approach to security compliance (Kouns 2007). This certification can provide third-party assurance that a company is serious about information security and managing associated risks (Brenner 2007).

The ISO 27001 (2005) presents a number of controls that can be considered as a good starting point for implementing information security. These controls fall into two basic categories: legislative controls and common best practices. Legislative controls are considered essential to a company from a legislative point of view and include data protection and privacy of information, protection of organisational records and intellectual property rights. On the other hand, the common best practice controls include:

- Information security policy document;
- Allocation of information security responsibilities;
- Information security awareness, training and education;
- Business continuity management;
- Management of information security incidents and improvements;
- Technical vulnerability management; and
- Correct processing in applications.

In addition, the standard consists of 15 sections, where each section provides a wide range of security control measures relevant to the specific section. These sections are the risk management, security policy, organisation of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, software acquisition, development and maintenance, incident management, business continuity management, and compliance.

Despite the worldwide acceptance of this standard, the DTI Information Security Breaches Survey (DTI 2006) revealed that the penetration of BS 7799 into UK businesses remains disappointing. Among people responsible for their companies' information security, only one in ten is aware of the contents of the standard; however, the adoption of the standard continues to rise among those who are aware of it. The survey results revealed that there is a wide potential audience for the standard, but the pricing and distribution of it are acting as barriers, in particular to small companies. In addition, the BERR Information Security Breaches Survey (BERR 2008) indicated that awareness of the standard is greater among respondents who hold a security qualification.

The literature further reveals that a few studies have addressed the British Standard and its two parts. Ma and Pearson (2005) conducted an empirical investigation into the validity, reliability and robustness of the international standard ISO 17799 through a web-based survey. Karabacak and Sogukpinar (2006) proposed a quantitative survey method for evaluating ISO 17799 compliance. In a recent study, Saleh *et al.* (2007) examined the development of a mathematical model that enables the investigation of companies' compliance with ISO 17799 and with its associated standard ISO 27001. This model is based on strategy, technology, organisation, people and environment (STOPE).

From the above it seems that there are a large number of standardisation bodies and organisations, and a large number of standards, best practices, guidelines, principles and evaluation techniques for information and IS security. However, ISO 27000 is the only standard that has gained worldwide publicity in both the UK and overseas. It helps companies in identifying, assessing, mitigating and monitoring information

security risks and threats by following a rigorous process-based approach and in selecting and implementing appropriate controls in order to ensure that risks and threats are reduced to an acceptable level.

2.4.8.9 AIS security effectiveness

Scott (1995) indicated that effectiveness is related to the level of achievement of objectives such as improving short-term and long-term IS performance and resource allocation. Measuring IS effectiveness has been an important research issue in the literature. DeLone and McLean (1992) conducted a comprehensive examination of previous research in this area. They provided six categories for IS success indicators namely system quality, information quality, use, user satisfaction, individual impact and organisational impact.

Wright (2006) indicated that measuring security effectiveness eases the process of monitoring the effectiveness of security management, reduces the number of security incidents, motivates staff when senior management set targets and provides tangible evidence to auditors and assurance to senior management that a company is in control. In addition, security should be monitored and periodically reassessed. These assessments can be a valuable means of identifying areas of non-compliance, reminding employees of their responsibilities and demonstrating management commitment to the security program (GAO 1998).

Despite the importance of measuring security effectiveness, a few studies have been conducted to cover the IS security effectiveness. Kankanhalli *et al.* (2003) proposed an integrative model of IS security effectiveness and empirically tested this model through a survey distributed among IS managers from various sectors of the economy. In their model, IS security effectiveness refers to the ability of IS security measures to protect against people's unauthorised or deliberate misuse of IS assets (hardware, software, data and computer services). IS security effectiveness was measured using perceptual responses to six questions: overall deterrent effect, overall preventive effect, effect in protecting hardware, software, data and computer services. In another study, Huang *et al.* (2006) used a balanced scorecard (BSC) framework to set up a performance index for information security management in companies and they provided a list of 35 key performance indicators. These indicators are considered as

references for the manufacturing industry to guide the linkage of business strategies and performance indicators for information security projects.

More recently, Hagen *et al.* (2008) have examined the implementation of organisational information security measures and assessed the effectiveness of such measures using data collected from the information security managers of Norwegian organisations. They categorised these measures into four main groups namely security policy, procedures and control, non-technical tools and methods, and the creation of organisational and individual security training and awareness. The results revealed that security policies, procedures and controls are applied more often whereas training and awareness are applied less frequently within the companies. In addition, Furnell and Papadaki (2008) addressed technical and human factors in security assessment. They recommended companies to test security from the perspectives of both the technology and the people; however, they argued that security assessment needs to be carefully considered and planned, given that both technical and human factors carry a risk that the test could compromise security.

The previous studies therefore reveal the importance of measuring security effectiveness, which makes it one of the main elements of companies' security management today.

2.5 Security controls

The selection and implementation of appropriate security controls for IS is an important task that can have major implications on the operations and assets of any company. However, with the evolution of IS from a paper-based system to a mainframe-based computer system then to a client/server system and now to an internet-based environment, new risks and threats arise and consequently new controls need to be developed to help mitigate or control those risks.

2.5.1 What is meant by security controls?

There are different meanings for controls. Eloff and Von Solms (2000, p.247) stated that the term "control" can be defined as being "a number of measured steps to take in order to realise a specific objective". The term "general controls" is used in most

previous studies as computer, IT or infrastructure controls (Flowerday and Von Solms 2005) and refers to the environment within which computer-based application systems are developed and maintained. These general controls are, therefore, used to ensure that applications be properly developed and implemented (Eloff and Von Solms 2000).

The National Information Systems Security Glossary (NSTISSI 4009 2000, p.50) defined the term "security safeguards or controls" as "the protective measures and controls prescribed to meet the security requirements specified for an IS. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas and devices". According to the National Institute of Standards and Technology (NIST), security controls include management, operational and technical controls that can protect the confidentiality, integrity and availability of systems and information (NIST 800-53 2005, p.1).

However, Parker (1991) stated that the term "information security controls" refers to the techniques used to reduce the likelihood that security threats will result in unauthorised access or disclosure of information, loss of systems or data integrity and disruption of systems availability.

Consequently, AIS security controls are the techniques or countermeasures used to safeguard the confidentiality, integrity and availability of AIS and information.

2.5.2 Classifications of security controls

Reviewing the literature has shown that there are diverse views regarding the classifications of security controls. Security controls could be classified according to their purpose into: preventive, detective, and corrective controls (Bagranoff *et al.* 2005; Flowerday and Von Solms 2005; Lin 2006; Romney and Steinbart 2003). Abu-Musa (2004b), Chang and Yeh (2006), Kankanhalli *et al.* (2003) and Qureshi and Siegel (1997) added another classification namely deterrent controls. However, it seems that both preventive controls and deterrent controls have the same function in hindering or preventing security threats. Security controls therefore could be classified into preventive, detective and corrective controls.

Security controls can also be classified according to their association with data or transaction processing stages into input, processing, storing and output security controls (Abu-Musa 2004b; Bagranoff *et al.* 2005). On the other hand, Nota (1988) classified controls according to stages of data manipulation process into access, input, computation, output and back-up controls. Input controls ensure the validity, accuracy and completeness of data entered into AIS. Processing controls focus on manipulation of accounting data after they have been entered into the computer. Output controls ensure the output's validity, accuracy and completeness; output is directed only to authorised persons, whereas storing security controls ensure that all stored data and programs are secured against unauthorised access, manipulation, alteration and disclosure.

Moreover, Gerber and Von Solms (2001) categorised security controls according to the evolution of computing eras - the computer-centric, IT-centric and information-centric era - into physical, technical and operational controls. Physical controls such as locked doors and cameras were used to protect the entrance to and continued operation of the computing facility. Technical controls such as user identification and authentication, access controls, and encryption are employed given the remote access to IS. Operational controls are the security policies, procedures, standards and guidelines that contribute with both physical and technical controls to protect IS and information in the information-centric era.

Dhillon and Moores (2001) addressed computer crimes and classified controls into three categories: technical, formal and informal controls. Technical controls restrict access to buildings and rooms or to computer systems and programs. Formal controls establish rules, ensuring compliance with laws and procedures and identifying security roles and responsibilities, whereas informal controls address security training and awareness programs conducted within companies.

However, the USA National Security Telecommunications and Information Systems Security Committee (NSTISSAM INFOSEC/1-99 1999) addressed the insider threats of IS and classified countermeasures into technical and procedural countermeasures. Technical countermeasures include access control, identification and authentication, encryption, operation system controls, system administration, event logging, audit and

intrusion detection tools. Procedural countermeasures include personnel security procedures (e.g. background checks and employee responsibilities), users' security procedures (e.g. segregation of duties, accountability, audits, passwords, and authentication), security policies related to the protection of IS (e.g. access controls, accountability, maintenance procedures, reportable incidents, contingency procedures, and legal issues). It is clear that those procedural countermeasures include the formal and informal controls mentioned before by Dhillon and Moores (2001).

Furthermore, the USA National Institute of Standards and Technology (NIST 800-53 2005) classified security controls into management, operational and technical controls. Management controls address the risk management and information security management and include risk assessment, planning, system and services acquisition, certification, accreditation, and security assessments. Operational controls are implemented and executed by people and include personnel security, physical and environmental protection, contingency planning, maintenance, system and information integrity, incident response, and training and awareness. In addition, technical controls are implemented and executed by IS through mechanisms contained in the system's hardware or software and include identification and authentication, access controls, audit and accountability, and system and communications protection.

On the other hand, Romney and Steinbart (2003) classified controls according to the AIS reliability principles into availability, security, maintainability and integrity controls. Availability controls ensure system availability and they include minimising system downtime and a disaster recovery plan. Security controls ensure that the system is protected against unauthorised physical and logical access and include segregation of duties, physical and logical access controls, protection of computers and networks, and internet controls. Maintainability controls ensure that the system can be modified as required without affecting its availability, security and integrity and includes project development, acquisition controls and change management controls. Moreover, integrity controls ensure that system processing is complete, accurate, timely and authorised and include input validation, online data entry controls, data processing and storage controls, output controls and data transmission controls.

In a more recent study, Yeh and Chang (2007) classified security countermeasures into two major categories. IT-related countermeasures include software, hardware, data and network security controls, whereas non-IT-related countermeasures include physical facilities and environment, personnel, regulation, compliance with legal requirements and risk transference controls.

From the above, security controls can be classified as follows:

- According to purpose, into preventive, detective, and corrective controls;
- According to their association with data processing stages, into input, processing, storing, and output security controls;
- According to the evolution of computing eras, into physical, technical, and operational controls;
- According to their role in minimising crimes, into technical and procedural (formal and informal) controls;
- According to their security function, into management, operational, and technical controls; and
- According to AIS reliability principles, into availability, security, maintainability and integrity controls.

2.5.3 Types of security controls

The literature reveals that some types of security controls are implemented by the majority of companies, while the use of other controls is still in its infancy.

In the UK, Mitchell *et al.* (1999) conducted a study to investigate the attitudes of UK companies to information security. The results revealed that although the majority of companies did not have a formal information security policy, they all used safeguards to protect their electronic information. The most common security measures used include physical and technical access controls to information; however, the reliance on technical security measures was higher than on physical measures. The results also revealed that the majority of companies used remote backup and storage of electronic information, followed by computer access controls; however, only 45 percent were protecting IS from fire. The least popular method was the marking of equipment and movable data storage. In addition, the most commonly used technical measures were anti-virus controls, followed by application and network access controls, however,

only 33 percent used firewalls, followed by user identification (ID) and encryption techniques to secure their corporate information. In addition, only one company used other safeguards such as software licence monitoring, software audit alert tools and smart cards.

In addition, the DTI Information Security Breaches Survey (DTI 2006) revealed that the majority of UK businesses are restricting access to most major computing facilities. Ninety seven percent of companies are using locks, 49 percent are monitoring this access through logs or cameras; however, environmental controls are present in just under a half of these facilities. The results also revealed that almost every company irrespective of size installs anti-virus software on its computers. An increasing number of companies are implementing intrusion detection or prevention software. UK businesses still overwhelmingly depend on user IDs and passwords to check the identity of users attempting to access their systems. Strong authentication is becoming more common in large companies, with hardware tokens and biometrics seeming to give greater security benefits than software tokens. Firewalls remain the main defence for websites. However, over half of all UK businesses are taking no steps to protect themselves against the emerging technologies that pose a potential security threat such as MP3 players, USB sticks, digital cameras and portable hard discs. The survey concluded that security awareness in the UK business community has never been better; however, the gap between the companies addressing information security and those that are not is widening.

More recently, the BERR Information Security Breaches Survey (BERR 2008) indicated that almost every UK business makes backups and the majority take these backups off-site. However, two thirds of companies continue to rely solely on physical security controls to protect their computer equipment - PCs and laptops - and the data they contained and they do not take enough steps in encrypting their sensitive data. Again, two thirds of companies seem to be either unaware of the risks of emerging technologies or unwilling to spend money on protecting themselves from these risks. In addition, the majority of businesses use anti-spyware scanning software as well as anti-virus software. UK businesses are now restricting staff access to the internet through establishing an acceptable usage policy, blocking inappropriate sites, monitoring usage, filtering incoming e-mail, encrypting e-mails exchanged with

business partners, and scanning outgoing e-mails as well. In addition, the growth in remote access is one of the drivers for using strong (multi-factor) authentication controls like tokens, smart cards, or biometrics. Moreover, the survey revealed that the number of companies using a wireless network is increasing, which drives UK companies, particularly financial services companies to implement WPA (Wi-Fi protected access) or stronger encryption over their wireless transmissions.

Henry (1997) conducted a survey of 261 companies in Hampton Roads, Virginia, USA to determine the nature of their accounting systems and security methods in use. The results revealed that the majority of companies backed up their accounting systems, secured their systems with passwords but only 42.7 percent utilised protection from viruses. Physical security and authorisation for changes to the system were employed by less than 40 percent of companies. In addition, only 15 companies used encryption for their accounting data, and almost 45 percent of the sample conducted some sort of audit of their accounting data.

In a study to identify and rank current information security threats, Whitman (2004) investigated companies' spending priorities to protect against these threats. The results revealed that the most common protection mechanism employed by all companies is the user name/password access control, followed by media backup and virus protection software, audit procedures and firewalls.

In another study, Gupta and Hammond (2005) mailed a questionnaire to 1000 small business owners in Lynchburg, Virginia, USA, investigating the protection technologies used by their companies. The results revealed that the majority of companies use technologies such as power surge protectors, data backup systems, system access controls, anti-virus software, and firewalls. In addition, Keller *et al.* (2005) focused on how small businesses are managing information security. The results revealed that all companies use anti-virus software and firewalls; however, less than two thirds of companies utilise passwords. Although it seems that security controls used by small companies are similar to those of large companies, it is clear that small companies use limited types of controls compared to large companies, and this could be because of the limited resources devoted to security.

In another study, Cerullo and Cerullo (2005) provided guidance to accountants and IT professionals on identifying significant risks and implementing security measures to manage these risks. They were given a list of security measures to protect against threats. They include security measures to protect against human threats e.g. antivirus software, authentication/authorisation servers, biometrics, electronic scanning devices, firewalls, intrusion detection and penetration devices and passwords, and security measures to protect against human non-malicious threats such as a corporate code of conduct and environmental controls. In addition, they include security measures to protect against accidents e.g. card activated locks, environmental controls, internal and external file labels, motion-detection devices and preventive maintenance; and security measures to protect against natural disasters and other unexpected disruptions such as environmental controls. Accountants and IT professionals therefore can select the most suitable security measures based on their experience and on cost-effectiveness.

On the other hand, the respondents to the Computer Crime and Security Survey (Gordon *et al.* 2006) were asked to identify the types of security technology used by their organisations. The results revealed that the majority of respondents used firewalls, followed by anti-virus software, anti-spyware, server-based access control lists and intrusion detection systems. On the other hand, only 20 percent of respondents reported the use of biometrics with a one third increase compared to the 2005 survey (Gordon *et al.* 2005). This result confirmed that the use of biometrics in business and accounting was still in its infancy and many issues about its role in IS security were unresolved (Amoruso *et al.* 2005; Chandra and Calderson 2003; Down and Sands 2004). More recently, the results of the Computer Crime and Security Survey (Richardson 2008) revealed that nearly all respondents reported the use of anti-virus software and firewalls, followed by virtual private networks (VPN) and anti-spyware software. However, only 23 percent of organisations were still using biometrics, only a three percent increase compared to the 2006 survey. Joyce (2008) argued that although the biometric technique was still not widely used, this technology could be found in large organisations where the security need is high such as financial services and government agencies.

From the above, it seems that some security controls are well known and are used by the majority of USA organisations. These include passwords, ant-virus and anti-spyware software, firewalls, and data backups followed by intrusion prevention and detection systems and encryption. However, other controls are not common for instance biometrics.

In a parallel study, Abu-Musa (2004b) investigated the opinions of the heads of internal audit departments and computer departments in the entire population of the Egyptian Banking Industry (EBI) regarding the computerised AIS security controls implemented within their banks. A checklist was developed which included security controls under ten main security control groups. The results revealed that the heads of computer departments paid relatively more attention to the technical problems of AIS security controls e.g. software and electronic access security controls, data and data entry security controls, bypassing security controls, and user programming security controls. However, the heads of internal audit departments emphasised behavioural and organisational security controls such as segregation of duties and output security controls. The results revealed that some controls are more common in the Egyptian business environment as well e.g. virus protection software, data encryption, and backups of software and data, whereas other controls such as biometrics have rarely been used in this country.

In a more recent study, Abu-Musa (2007b) examined the existence and adequacy of the CAIS security controls implemented in Saudi organisations to prevent, detect and correct security breaches. The results highlighted a number of inadequately implemented controls and some recommendations were made to the Saudi organisations. For example, they were recommended to restrict access to sensitive data to authorised employees only. Mandatory vacations and rotation of duties should be considered. Computers should be installed in locked areas, sensitive data should be encrypted to reduce the chance of unauthorised exposure, and adequate output security controls should be put in place.

From the above, it can be concluded that some security controls are used by nearly all companies irrespective of type, size and location, whereas other controls such as biometrics are still uncommon despite their importance in improving the effectiveness

of internal controls. Moreover, despite the large number and variety of security controls or countermeasures available today, emerging technologies continue to proliferate within the business environment and therefore companies should be adequately prepared to address associated security challenges and risks.

2.6 Summary of the chapter

This chapter has provided a review of the literature in the field of AIS security. First, the chapter reviewed the literature concerning the meanings, main components and role of AIS in organisations. The chapter then provided an overview of the various classifications and types of security threats facing companies' information, IS, IT and computers, and particularly those threats facing companies in different countries. The chapter also highlighted the meanings of security in general and particularly the AIS security in previous studies, the evolution and importance of security, the roles and responsibilities for security, the principles of security and the factors affecting security. The chapter then examined how companies manage security and discussed the main elements of security management, namely security requirements, policy, training and awareness, risk assessment, incident handling, business continuity plans, standards and certification, and evaluation techniques. The review shows that IS security management has become a necessity and if properly implemented, enables companies to reduce security risks to acceptable levels, to satisfy the legal, regulatory and contractual requirements, to enhance their overall security posture and most importantly to ensure their continuity.

Finally, the chapter has examined the literature concerning the various classifications and types of AIS security controls implemented in most companies to prevent or reduce their security threats. This review shows that the priority given to security has been translated into action, security controls have improved and the confidence in those controls is high. However, emerging technologies continue to proliferate and companies must be adequately prepared to address associated risks.

The following chapter presents the conceptual framework that has guided the development of the objectives, questions and hypotheses of the current research. It proceeds by explaining the research design, data collection methods available in previous studies concerning AIS security and those methods employed in the current

research namely a postal questionnaire and semi-structured interviews, emphasising the strengths and weaknesses of each method, along with the justification for their use. A detailed explanation of the procedures followed in each method will be provided.

Chapter 3
Methodology

3.1 Introduction

The preceding chapter reviewed the literature and presented an integrated view of AIS security issues. It began by describing the meanings, components and importance of AIS and exploring its role in organisations. It proceeded by exploring different AIS security threats. Then, it described the importance of and responsibility for AIS security, focusing on the different dimensions of security and paying particular attention to security management. Finally, it investigated the different types of security controls used to prevent or to reduce security threats.

The aim of this chapter is to present the conceptual framework, which guides the development of objectives, questions and hypotheses of the current research. Then it explains the research design, the data collection methods available in previous studies concerning AIS security and those methods employed in the current research, a postal questionnaire and semi-structured interviews, emphasising the strengths and weaknesses of each method, along with the rationale for their use.

The chapter then proceeds by providing a detailed explanation of the procedures followed in each method, the questionnaire design and layout, the pilot test of the questionnaire, sampling and administration of both methods, the statistical methods applied to analyse the research data and the ethical considerations of the research.

3.2 Conceptual framework of the current research

A valuable part of the initial planning process is the development of a conceptual framework for the research (Smith 2003). A conceptual framework is "a representation, either graphically or in narrative form of the main concepts or variables, and their presumed relationship with each other" (Punch 1998, p.56). According to Sekaran (2003, p.86) a theoretical framework is "a conceptual model of how one theorises or makes logical sense of the relationships among the several factors that have been identified as important to the problem".

The conceptual framework is the foundation on which the entire research project is based. It elaborates the relationships among variables, explains the theory underlying these relations, and describes the nature and direction of the relationships. It can bring clarity and focus, helping the researcher to see and organise the research questions more clearly. It plays a predominant role in research, implying a systematic organisation of and relationships between concepts and it offers the conceptual foundation to proceed with the research (Ghauri and Gronhaug 2002; Punch 1998; Sekaran 2003). The entire research should be based on the theoretical framework.

In Chapter 2, it was mentioned that the security issue has received considerable attention from both academics and practitioners. In the UK, the priority given to security remains high across all sizes and types of companies. According to the DTI Information Security Breaches Survey (DTI 2006), three quarters of UK businesses rate security as a high or very high priority. In addition, the results of the American Institute of Certified Public Accountants' 19th Top Technology Initiatives Survey (AICPA 2008) indicated that "security" has been the number one technology concern in the USA for six consecutive years.

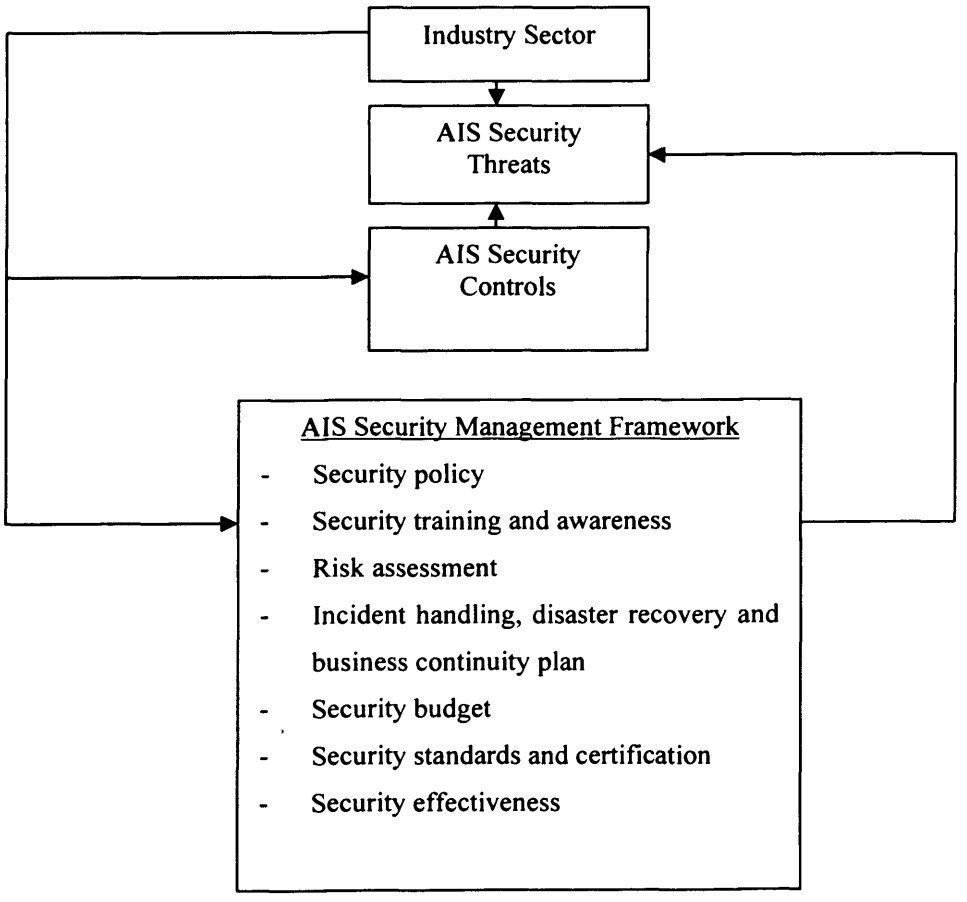
However, despite this importance, the literature regarding IS security in general and AIS security in particular reveals that security research is fragmented and no comprehensive framework was discovered. Cannoy *et al.* (2006) stated that through the analysis of hypotheses, frameworks and variables, security research appears to be highly fragmented. Most previous studies included diagrams, charts and tables; however, none of them included major constructs and their relationships, only proposing a model for a specific topic or clarifying a technical system, and many of the frameworks proposed are extremely specific and task-related.

In addition, the literature review reveals that most previous studies lack an overall and comprehensive view of the AIS security issue. Each of these studies tried to address a particular security aspect. Some of them addressed AIS security threats (Abu-Musa 2004a; 2006a and b; Keller *et al.* 2005; Loch *et al.* 1992; Ryan and Bordoloi 1997; Whitman 2004). Others focused on controls (Abu-Musa 2004b; 2007a and b; Henry 1997; Kankanhalli *et al.* 2003), while others combined security threats and controls in one study (Chang and Yeh 2006; Gupta and Hammond 2005; Yeh and Chang 2007).

Moreover, the majority of the previous studies focused only on one activity of the AIS security management framework. Doherty and Fulford (2005), Hong *et al.* (2006) and Kadam (2007) addressed the security policy. Kruger and Kearney (2006) and Peltier (2005) focused on security training and awareness. Gerber and Von Solms (2005) covered the risk assessment. Bhaskar (2005) and Mitropoulos *et al.* (2007) addressed incident handling, whereas Hunton (2002) and Rodetis (1999) focused on disaster recovery and business continuity plans. Gordon and Loeb (2006) were concerned with security budgets, while Freeman (2007) and Karabacak and Sogukpinas (2006) addressed security standards and certification.

The current study is an attempt to present an integrated view of AIS security, and a comprehensive conceptual framework for the research is proposed as shown in Figure 3.1.

Figure 3.1 Conceptual framework of the research



The conceptual framework shown in Figure 3.1 presents the relationship between the main variables of the study, namely the industry sector, AIS security threats, AIS security controls and AIS security management framework.

Contingency theory states that in order to survive or to be effective, a company must fit its characteristics to contingencies that reflect its situation (Donaldson 2001; Drazin and Van de Ven 1985). Contingency theory attempts to establish functional relationships between environmental variables and organisational variables, and therefore, recognises and responds to these variables in order to attain organisational objectives effectively (Hong *et al.* 2003; Lee *et al.* 1982).

Moreover, Ashby's law of requisite variety states that control can be obtained only if the variety of the controller is at least as great as the variety of the situation to be controlled (Beer 1981, p.41). According to Lewis and Stewart (2003), the application of Ashby's law to companies means that the company must generate at least as much variety (e.g. security controls) in order to control the variety in its environment. Tushman and Nadler (1978) indicated that the application of Ashby's law is consistent with the contingency concept of fit between a company and its environment. If the company possesses too much variety then it is wasting resources and its performance is lower than it should be. However, if the company possesses too little variety then it will be exposed to higher levels of risk. Consequently, the maximum performance requires that the company's variety should match that of the environment.

The environment of an organisation can be classified into the industry and the macro environments (Dill 1958; Grant 1998). The industry environment includes technology, competition, customer/market and resources sectors and tends to have a direct impact on the competitive situation of individual organisations. The macro environment is made up of the political/legal, economic and social/cultural sectors and has an indirect influence on individual organisations (Daft *et al.* 1988; Dill 1958; Ducan 1972).

According to Hong *et al.* (2003), security levels are dynamic and contingent upon the environmental variables of a company for example technological change. Thus, with the rapid change in IT, with the great desire of companies to implement up-to-date

computerised systems and software and with the higher levels of inter-connectivity among systems both within and among companies, this rapidly changing technology has created significant risks related to AIS security. Consequently, new controls need to be developed to help mitigate those risks and to reduce security threats, which constantly adapt themselves to new environments (Abu-Musa 2003; 2004b; Chou *et al.* 1999). The technological change, therefore, leads to change in the number, type and severity of AIS security threats and the number and type of controls implemented to reduce those threats.

In addition, AIS security management is a stream of management activities that aim to protect AIS and create a framework within which such systems operate as expected. If properly implemented, the AIS security management framework enables companies to reduce security risks to acceptable levels (Eloff and Von Solms 2000). AIS security management is a part of contingency management to prevent and detect security threats, vulnerabilities, and impacts inside and outside of a company. Companies therefore should adopt security management measures such as security policy and risk assessment in order to meet the demands of a fast-changing environment (Hong *et al.* 2003).

Furthermore, there is a high degree of agreement that companies in different industry sectors tend to have different uses for IS (Jarvenpaa and Ives 1990) and, therefore, different security requirements (Chang and Yeh 2006; Kankanhalli *et al.* 2003; Straub 1986). Consequently, a company's approach to security depends on its industry sector.

3.2.1 The main variables of the research

From the above, it seems that there are some relationships between the main variables of the current study. These variables are discussed in more detail as follows:

3.2.1.1 AIS security threats

As mentioned Chapter 2, security threats are any event that can have an adverse impact on a company's IS in general and AIS in particular. Lin (2006) argued that security threats are acts or incidents that could affect a company's IS. These threats

can either be singular or form part of a combination of multiple threats, and they can come both from inside or outside the company.

A risk is the possibility that a certain threat will have a negative effect on a company's IS. Tsiakis and Stephanides (2005) argued that a company has four alternatives to deal with its security risks: to accept it, ignore it, assign it to someone else, or to mitigate or reduce it through appropriate security controls or safeguards. In addition, Moses (1992, p.236) indicated that risk reduction could be achieved by avoiding or transferring a risk, reducing the likelihood of threats, reducing possible impacts, detecting unwanted events, and recovering. Consequently, a company could reduce the likelihood of security threats or minimise their impact through appropriate safeguards or controls.

Chang and Yeh (2006) argued that companies should prepare appropriate security measures to minimise security threats. Lin (2006) also indicated that companies should be well prepared for all possible security threats to protect their AIS. He argued that a combination of preventive and detective controls could mitigate these threats. In addition, Vidalis and Kazmi (2007) pointed out that reacting is expensive in security; companies therefore should be proactive and prevent attacks from happening or minimising the impact of the threats. The frequency of security threats therefore depends on the readiness of a company by using appropriate security controls. "AIS security threats" is therefore one of the main variables that depends on the AIS security controls implemented and on a company's industry sector.

The literature review reveals that companies, their IS and AIS are subject to increasing numbers and types of security threats. Consequently, many previous studies focused on this variable and covered it from different perspectives. Some studies focused on IS security threats (D'Arcy and Hovav 2007; Kros *et al.* 2005; Lin 2006; Loch *et al.* 1992; Ryan and Bordoloi 1997; Yeh and Chang 2007). Other studies addressed AIS security threats (Abu-Musa 2002a; 2004a; 2006a and b; Beard and Wen 2007; Davis 1997; Rainer *et al.* 1991). Others again are concerned with information security threats (Keller *et al.* 2005; Mitchell *et al.* 1999; Whitman 2003 and 2004; Wiant 2005), whereas others focused on computer security threats (Haugen and Selin 1999; Katz 2000; Manrique 2005; Qureshi and Siegel 1997).

On the other hand, some studies investigated the types and frequency of the occurrence of each type of security threats (Abu-Musa 2004a; 2006a and b; Keller *et al.* 2005), while others are concerned with ranking the top security threats (Davis 1997; Loch *et al.* 1992) and rating the seriousness of each threat (Ryan and Bordoloi 1997). Abu-Musa (2006a) conducted a study to investigate the perceived threats of computerised AIS in Saudi Arabian organisations using a security threats checklist. The respondents to the questionnaire were asked to indicate the frequency of occurrence of each security threat by choosing one among five available choices ranging from "less than once a year" to "more than once a day".

Loch *et al.* (1992) investigated MIS executives' concern about a variety of threats. Respondents were asked to rank the top three of 12 threats to their organisation's IS security for microcomputers, mainframes and networks. In a similar study, Ryan and Bordoloi (1997) examined the security threats associated with client/server versus mainframe environment. Using a questionnaire incorporating a list of 15 major potential security threats, respondents were asked to rate the seriousness of each threat to their company in both environments in a scale ranging from one to ten.

Whitman (2004) conducted another study to identify and to rank threats to information security, to provide information on the frequency of attacks from these threats and the prioritisation for expenditures companies are placing in order to protect against them.

From the above, it seems that there are large numbers of security threats facing companies. Since most, if not all, companies today depend on computerised IS in carrying out their activities, security threats facing them are increasingly complex which can lead to extensive damage e.g. business interruption, financial loss, loss of data, loss of reputation and even bankruptcy. Consequently, there is a great concern from academics and practitioners regarding security threats.

The current study investigates the most common sources and types of AIS security threat among UK companies in different industry sectors and the frequency of their occurrence. Respondents were asked to rank the top three sources of security threats to their company's AIS from a range of the most likely threats and to indicate the

frequency of occurrence of each type of threat by choosing one among six choices (none, once a year, once a month, once a week, once a day, more than once a day). The current study is an attempt to discover the most common types of security threats facing IS in general and their AIS in particular in order to implement appropriate security controls to prevent or reduce these threats and to protect their systems.

3.2.1.2 AIS security controls

The National Information Systems Security Glossary (NSTISSI 4009 2000, p.50) defines the term "security safeguards or controls" as "the protective measures and controls prescribed to meet the security requirements specified for an IS. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas and devices". Consequently, AIS security controls are the countermeasures used to safeguard the confidentiality, integrity and availability of AIS.

The literature reveals that there is a great concern among academics and practitioners regarding IS security controls. Abu-Musa (2007a and b) conducted a study to examine the existence and adequacy of implemented computerised AIS security controls to prevent, detect and correct security breaches in Saudi organisations. A self-administered questionnaire was used incorporating an AIS security controls checklist which classified controls into 11 groups and used "yes" or "no" questions. Respondents were asked to choose one of the two choices.

Henry (1997) collected information on accounting systems and their security methods in Virginia. A section in the survey asked respondents about the basic security measures used with accounting systems. Mitchell *et al.* (1999) investigated the attitudes to information security among UK organisations.

Gupta and Hammond (2005) conducted a study to gather information about IT related security issues in small firms in both manufacturing and service. A questionnaire was mailed to business owners in Virginia to investigate the protection technologies used by their organisations. In another study, Keller *et al.* (2005) focused on how small businesses are managing information security and the associated risks. Semi-

structured interviews were conducted and interviewees were asked to indicate the tools used in their companies to deal with their security threats.

In addition, Chang and Yeh (2006) examined whether the security preparation of firms matches the severity of IS threats they perceive in developing countries. This study also discussed the appropriate threat mitigation strategies for four sectors. The questionnaire included a section to assess the scope of security countermeasures, which are divided into seven different categories: software, hardware, data, network, physical facilities and environment, personnel and regulations, and respondents were asked to choose the measures they employed under each category. In a more recent study, D'Arcy and Hovav (2007) used a web-based survey to elicit respondents' IS misuse intentions and awareness of security countermeasures within their organisations. The survey items were measured on a seven-point scale ranging from "strongly disagree" to "strongly agree".

Based on the above, it seems that every company, regardless of its size and location, is concerned with preparing itself for all possible types of security threats. Tsiakis and Stephanides (2005) indicated that security safeguards or controls limit a threat from becoming a reality. Kadam (2007) stated that a company should utilise all possible controls to be able to prevent IS security threats and maintain the customer's confidence by having appropriate technical, procedural and administrative controls. Chang and Yeh (2006) argued that a lack of robust security controls raises a company's security threats. Adequate controls help to ensure the smooth functioning of IS and protect the company from loss caused by security failures (IFAC 1998). Consequently, a company's managers and employees should be knowledgeable of all types of security threats and controls to protect their systems.

AIS security controls are, therefore, one of the main variables in the current study, which are implemented to reduce AIS security threats. In order to investigate the security controls implemented by UK companies in different industry sectors, the researcher developed a list of security controls and the respondents of the questionnaire were asked to indicate whether they are using each control, they are planning to use it or there are no plans to use it. The current study is an attempt to investigate the types of controls implemented in UK companies and to examine

whether there are significant differences among industry sectors regarding these different types of controls.

3.2.1.3 AIS security management framework

A security management framework is a structured process for the implementation and ongoing management of information security in a company (Vermeulen and Von Solms 2002). Due to new security needs that have been introduced by the advances in IT, IS security has become a necessity for all companies. However, the implementation of integrated IS security across a company is a complex process that requires proper management. Consequently, a security management framework must exist not only to protect IS and information but to ensure the continuity of the company (Karyda *et al.* 2005).

In addition, Posthumus and Von Solms (2004) stated that effective information security could have a positive impact on a company. However, in order for companies to manage information security effectively, various security requirements and guidelines need to be considered. These security requirements and guidelines stem from sources both internal and external to the company.

However, Hong *et al.* (2003) pointed out that the approach to information security management varies with different researchers and companies. The literature review reveals that there are various approaches in dealing with IS security management. Some studies covered IS security management in general such as Vermeulen and Von Solms (2002), while other studies focused only on one of the activities that form an IS security management framework. Doherty and Fulford (2005), Hong *et al.* (2006) and Kadam (2007) focused on security policy. Kruger and Kearney (2006) and Peltier (2005) covered security training and awareness. Gerber and Von Solms (2005) addressed risk assessment. Bhaskar (2005) and Mitropoulos *et al.* (2007) covered incident handling whereas Hunton (2002) and Rodetis (1999) focused on disaster recovery and business continuity plans. Gordon and Loeb (2006) addressed the security budget, while Freeman (2007) and Karabacak and Sogukpinas (2006) focused on security standards and certification. In addition, Huang *et al.* (2006), Kankanhalli *et al.* (2003) and Wright (2006) addressed security effectiveness.

According to Von Solms (2005), these activities are generally accepted as making up the information security management in organisations. In addition, they are essential in order properly to manage IS security and to avoid the potential consequences of any neglect of these activities.

Based on the above, an AIS security management framework is one of the main variables in the current study that depends on a company's industry sector. If properly implemented, this framework enables a company to reduce security threats to acceptable levels, to protect information and IS and to ensure the continuity of the company. The security management framework includes the following activities:

- Security policy
- Security training and awareness
- Risk assessment
- Incident handling, disaster recovery and business continuity plan
- Security budget
- Security standards and certification
- Security effectiveness

Security policy: The US National Security Telecommunications and Information Systems Security Committee (NSTISSAM INFOSEC/1-99 1999) stated that a security policy is a set of laws, rules, and practices that regulate how a company protects its IS and the data within them. Reviewing the literature reveals that there is a high degree of agreement that the security policy is at the heart of any information security strategy and it is the start of security management (Eveloff 2005; Higgins 1999). Poore (1999) argued that the lack of policy could result in a company subjecting its IS to undue risks and increasing the potential for unacceptable loss, liability or harm to the company and other relevant parties. In addition, Briney (2000) indicated that companies with a security policy are paying closer attention and therefore are better able both to detect and to react to security incidents and are more secure than other companies.

The literature reveals that it is not enough to establish a security policy; this policy must be updated regularly (Briney 2000; Steele and Wargo 2007; Wiant 2005).

Based on the importance of the security policy and its vital role in any company, many previous studies have been conducted to investigate the security policy from different perspectives (Section 2.4.8.3 in Chapter 2). For example, Fulford and Doherty (2003) conducted a study to investigate the uptake, content, dissemination and impact of information security policies in UK companies. Doherty and Fulford (2005) explored how a variety of issues relating to the uptake and application of security polices e.g. existence, age, updating and scope of a security policy impacted upon the incidence of security breaches within large companies. In addition, Hong *et al.* (2006) investigated the dominant factors of building an information security policy and the effect of this policy on elevating a company's security level.

Consequently, the current study investigates the existence and frequency of updating AIS security policy among UK companies in different industry sectors. The respondents of the questionnaire were asked whether they have a security policy covering AIS in their companies, and the frequency of updating this policy.

Security training and awareness: Employees' training and awareness is the most important of all information security measures and a critical component of the information security program (Bowen *et al.* 2007; Eveloff 2005). Peltier (2005) argued that an effective security program cannot be implemented without implementing an employee awareness and a training program to address policy, procedures and tools. Given the vital role of security training and awareness programs in companies, many studies have been conducted to explore this issue as was mentioned in Chapter 2 (Section 2.4.8.4) e.g. Chen *et al.* (2008), Kritzinger and Smith (2008), Kruger and Kearney (2006), Peltier (2005), Siponen (2000) and Thomson and Von Solms (1998). For example, Siponen (2000) provided a conceptual foundation and a framework for IS security awareness. Peltier (2005) identified the elements that make up a successful security awareness program, and Kruger and Kearney (2006) provided a model for measuring information security awareness in companies.

Consequently, to explore this issue in more detail, the current study investigates the existence of AIS security training and awareness programs for managers, employees and other users among UK companies in different industry sectors. The respondents were given some statements concerning the security training and awareness activities

and were asked to indicate their level of agreement with these statements using a scale ranges from "strongly disagree" to "strongly agree". The researcher investigated the differences among industry sectors in the UK concerning the level of attention paid to security training and awareness.

Risk assessment: Businesses are exposed to unlimited security risks unless they have a formal risk management framework in place to enable risks to be identified, evaluated, and managed (Shaw and Daniels 2002). Due to the increasing risks to which companies are exposed, many studies have been conducted to investigate this issue as was shown in Chapter 2 (Section 2.4.8.5) such as Gerber and Von Solms (2005), Kotulic and Clark (2004), Lindberg (2006), Sherer and Alter (2004), Tsohou *et al.* (2006) and Zhou *et al.* (2008). For example, Kotulic and Clark (2004) proposed and tested a theoretical model to study the process that leads to effective Security Risk Management (SRM) programs. Lindberg (2006) proposed a simplified risk management model that will provide quantitative results based on subjective human inputs, whereas Zhou *et al.* (2008) presented an IS project risk checklist that aims at supporting risk assessment, decision making concerning risk control, and planning of risk mitigation strategies in the public sector.

Consequently, to explore this security issue in more detail, the current study investigates the existence and frequency of updating AIS risk assessment programs among UK companies in different industry sectors. Respondents of the questionnaire were asked whether they have an AIS risk assessment program and the frequency of updating this program. Respondents were also given some statements concerning the risk assessment activities within their companies and they were asked to indicate their level of agreement with these statements using a "strongly disagree" to "strongly agree" scale.

Incident handling, disaster recovery and business continuity plan: Due to the increasing number of security breaches occurring within organisations and the constant news of large companies and government departments suffering financial and non-financial losses, Williams (1995) argued that it must make better business sense to take a preventive approach and to try to deal with such breaches as soon as possible. The sooner action is taken, the cheaper it will be for the company in the long

run. Consequently, it is vital for all types of companies to have security incident handling procedures in place to deal with any security incident and to react quickly to any disruption in normal business processes. In addition, a business continuity plan is a critical component of the security management system (Smith and Jamieson 2006). It assures the availability of IS in the case of a crisis or other serious disruption in services.

As was shown in Chapter 2 (Section 2.4.8.6), a number of studies have been conducted to investigate the incident handling, disaster recovery and business continuity plan issues such as Bhaskar (2005), Fonseca (2007), Gerber and Feldman (2002), Hancock (2002), Mitropoulos *et al.* (2007), Nosworthy (2000), Smith and Jamieson (2006) and Vael and Neyer (2006). For example, Gerber and Feldman (2002) offered advice to companies on how to select a team and develop a plan that will ensure their ability to remain in business in the event of a disaster. Smith and Jamieson (2006) investigated the key drivers and inhibitors for IS security and business continuity management in e-government using the data collected from a cross section of government organisations. In addition, Fonseca (2007) addressed the human factor in business continuity plans and argued that excellent plans can fail because of an often overlooked factor namely human beings.

Based on the important role of incident handling, disaster recovery and business continuity plans, the current study investigates the differences among the industry sectors in the UK regarding the existence and the frequency of updating incident handling procedures and business continuity plans. Respondents of the questionnaire were asked whether their companies experienced any AIS security incidents in the last year, whether they have security incident handling procedures and business continuity plans in place, the frequency of updating these plans, if any, and the actions taken by their companies to reduce future security incidents.

Security budget: With the increasing number of security incidents in the daily news, companies are now uncertain about how much to spend on security and what to spend it on (Kleinfeld 2006). In addition, according to the DTI Information Security Breaches Survey (DTI 2006), spending the right amount on security continues to challenge UK companies. The literature review reveals that security is still perceived

as an IT issue. Most companies still do not have a security budget separate from their IT budget (DTT 2007) and the security budget is expressed as a percentage of IT budget.

Despite the important role that the security budget plays in companies today, few studies have been conducted to investigate this issue as mentioned in Chapter 2 (Section 2.4.8.7) such as Gordon and Loeb (2006) and Willison and Backhouse (2006). Consequently, in order to explore different aspects of the security budget, the current study investigates the differences among UK companies in different industry sectors regarding the existence of a security budget, its percentage and the top areas of spending on AIS security. Respondents of the questionnaire were asked about the existence of a security budget within their companies, and if any, what percentage of this budget is spent on AIS security. Respondents were given a list of areas of spending on AIS security and were asked to rank the top three areas of spending in their companies.

Security standards and certification: To protect the companies' information and IS, many different standards and guidelines have been proposed. The British Standard for Information Security Management BS 7799 (now ISO 27000) with its two parts: ISO 17799 (Code of Practice) and ISO 27001 (Certification), is widely acknowledged as an important framework for security in both the UK and overseas (DTI 2006).

Karabacak and Sogukpinar (2006) argued that compliance with the standard is the practical process of comparing the applied controls of a company with those in ISO 17799. In addition, certification to ISO 27001 assures clients, employees, suppliers, business partners and future customers that a company has a continuous protection methodology allowing a flexible, effective and defensible approach to security compliance (Kouns 2007). This certification can provide third-party assurance that an organisation is serious about information security and managing associated risks (Brenner 2007). Von Solms (1998) argued that the ideal would be for companies to follow such a complete approach to security management, but unfortunately, most companies do not possess the required resources to introduce and maintain such a comprehensive security program.

The literature review (Section 2.4.8.8 in Chapter 2) also reveals that only a few studies were conducted to discuss the standard and its two parts such as Karabacak and Sogukpinar (2006), Ma and Pearson (2005) and Saleh *et al.* (2007). For example, Ma and Pearson (2005) conducted an empirical investigation into the validity, reliability and robustness of the international standard ISO 17799 through a web-based survey, while Karabacak and Sogukpinar (2006) proposed a quantitative survey method for evaluating ISO 17799 compliance.

Due to the importance and popularity of the British Standard BS 7799, the current study investigates the awareness level of managers and employees among UK companies in different industry sectors. Respondents were asked to indicate their awareness level of the two parts of BS 7799, the awareness level of managers and employees in their companies and whether their companies are certified or are planning to be certified under ISO 27001. The researcher intended to investigate the industry sectors that are more aware and more concerned with this standard.

AIS security effectiveness: Huang *et al.* (2006) argued that after any information security investment, companies have to assess the consequences of business returns and to assess security effectiveness. Wright (2006) indicated that measuring security effectiveness eases the process of monitoring the effectiveness of the security management system, reduces the number of security incidents, motivates staff when senior management set targets and provides tangible evidence to auditors and assurance to senior management that the company is under control.

However, despite the importance of measuring security effectiveness, only a few studies were conducted to cover the IS security effectiveness as mentioned in Chapter 2 (Section 2.4.8.9) including Furnell and Papadaki (2008), Hagen *et al.* (2008), Huang *et al.* (2006) and Kankanhalli *et al.* (2003). For example, Kankanhalli *et al.* (2003) proposed an integrative model of IS security effectiveness and empirically tested this model through a survey distributed among IS managers from various sectors of the economy. In addition, Huang *et al.* (2006) used a balanced scorecard (BSC) framework to set up performance index for information security management in companies and they provided a list of 35 key performance indicators.

Consequently, the current study has investigated the techniques used by UK companies in different industry sectors to evaluate the effectiveness of AIS security and the success indicators of AIS management within these companies. Respondents were given a list of techniques for evaluating AIS security effectiveness and were asked to select those techniques used by their companies. Respondents were also given a list of success indicators of AIS security management and were asked to rank the top three success indicators within their companies.

3.2.1.4 Industry sector

The literature reveals that the industry sector has begun to receive greater attention in IS research in general and IS security research in particular. There is an agreement that a company's approach to information security depends on its industry sector. Sectors vary in how information technologies are used. The same type of IT application might be applied differently across sectors (Chiasson and Davidson 2005). Jung *et al.* (2001) indicated that companies in different industries require different levels of information availability, confidentiality and integrity. Consequently, companies in different sectors tend to have different security requirements.

Kankanhalli *et al.* (2003) developed an integrative model of IS security effectiveness in which the industry sector is one of the independent variables. They indicated that industry type is an important factor affecting IS security practices for several reasons. Financial services companies, for example, are likely to invest heavily on IS and rely extensively on IS for their operations compared to other companies. This industry is information-intensive, and therefore, the potential losses for financial services companies due to IS abuses can be extremely high. In addition, the reputation of these organisations, in terms of reliability and security of financial information, is critical to their success but can be severely damaged by IS abuses.

Chang and Ho (2006) examined the influence of organisational factors on the effectiveness of implementing BS 7799: Information Security Management Standard. They concluded that there are significant impacts of organisational factors including the industry type on the effectiveness of implementing BS 7799 and that some information security related behaviours varied substantially across industry sectors.

Chang and Yeh (2006) investigated the differences in perspective among companies, in different sectors, in relation to information threats to their business and the countermeasures they have prepared in response to these threats. They concluded that businesses should understand their security requirements based on their industry and prepare for appropriate security countermeasures to minimise IS threats. In another study, Yeh and Chang (2007) identified the gaps between manager perceptions of IS security threats and the countermeasures adopted by companies across industries. They also examined the impacts of several variables including industry type on IS security adoption. They concluded that industry type is an important factor that affects the motivation of companies to adopt security countermeasures.

Based on the above, the current study investigates the differences between industry sectors in the UK regarding the sources and types of threats facing AIS security, the different types of security controls implemented to prevent or reduce security threats and the existence of a management framework for AIS security. The researcher aims to investigate the security practices among the different industry sectors in the UK.

3.2.2 The research objectives

The review of the literature shows that most previous studies lack a comprehensive view of the security issue. Each of these studies tried to focus on a particular security aspect. Thus, the current study is an attempt to present an integrated view of AIS security. More specifically, the current study intends to achieve the following objectives:

1. To examine the existence of an adequate management framework of AIS security within UK companies in different industry sectors.
2. To investigate the different types of AIS security threats facing UK companies in different industry sectors.
3. To investigate the security controls implemented by UK companies to prevent or reduce security threats.
4. To investigate the effect of the security controls implemented on the reduction of AIS security threats facing UK companies.
5. To investigate the relationship between AIS security effectiveness of UK companies and their AIS security threats level.
6. To examine the security perception among different industry sectors in the UK.

3.2.3 The research questions

Based on the above discussion, and in order to investigate the AIS security level among UK companies in different industry sectors, the current study seeks to find answers to the following questions:

1. Is there an adequate management framework for AIS security among UK companies in different industry sectors?
2. What are the most common sources and types of security threats facing AIS of UK companies in different industry sectors?
3. What types of security controls are implemented to prevent or reduce security threats in different industry sectors in the UK?
4. Are there significant differences between different industry sectors in the UK concerning the types of AIS security threats, AIS security controls and the existence of an adequate management framework for AIS security within companies?
5. What is the impact of the security controls implemented and the AIS security effectiveness level achieved on the reduction of AIS security threats facing UK companies?

3.2.4 The research hypotheses

To achieve the objectives of the current study and to examine the relationship between its main variables i.e. AIS security threats, AIS security controls, AIS security management framework and the industry sector, the following hypotheses were formulated which are tested and discussed in the following chapters:

H1: There are no significant differences among UK companies in different industry sectors concerning the existence of a management framework for AIS security.

H1.1: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security policy and the frequency of updating this policy.

H1.2: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security training and awareness program and the security awareness level.

H1.3: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS risk assessment program and the frequency of undertaking this program.

H1.4: There are no significant differences among UK companies in different industry sectors concerning the existence of security incident handling procedures, disaster recovery and business continuity plans and the frequency of testing and updating these plans.

H1.5: There are no significant differences among UK companies in different industry sectors concerning the existence of a security budget and areas of spending on AIS security.

H1.6: There are no significant differences among UK companies in different industry sectors concerning the awareness level of the British Standard for Information Security Management BS 7799 and the certification under ISO 27001.

H1.7: There are no significant differences among UK companies in different industry sectors concerning the techniques used to evaluate AIS security effectiveness, the success indicators of AIS security management, and the effectiveness level of AIS security management.

H2: There are no significant differences among UK companies in different industry sectors concerning the sources and types of AIS security threats.

H3: There are no significant differences among UK companies in different industry sectors concerning the types of controls implemented to prevent or reduce security threats.

H4: There is no significant relationship between the different types of security controls and the reduction of AIS security threats facing UK companies.

H5: There is no significant relationship between AIS security effectiveness and the AIS security threat level in UK companies.

3.3 Research paradigm

A paradigm is a set of beliefs or assumptions about the social world that guide a researcher's inquiry (Creswell 1998; Punch 1998). It includes basic assumptions, important questions to be answered and research techniques to be used (Neuman 2000). It is a set of propositions that explain how the world is perceived, thus it may be best defined as a "world-view" (Sarantakos 2005).

In brief, the term "paradigm" refers to "the progress of scientific practice based on people's philosophies and assumptions about the world and the nature of knowledge;

in this context, about how research should be conducted" (Hussey and Hussey 1997, p.47).

There are competing approaches to social research based on different philosophical assumptions about the purpose of science and the nature of social reality (Neuman 2000). Every researcher brings to his research a "set of interlocking philosophical assumptions and stances" (Greene and Caracelli 1997, p.6). Every paradigm includes three basic assumptions: the ontological, epistemological and methodological assumptions (Creswell 2003; Healy and Perry 2000; Hussey and Hussey 1997; Rocco *et al.* 2003; Sarantakos 2005).

- The ontological assumption is concerned with the reality that the researcher investigates i.e. what is the nature of reality? Is it objective and external to the researcher, or is it constructed or subjective?
- The epistemological assumption is concerned with the relationship between the researcher and what is being researched i.e. what kind of knowledge is the researcher looking for and what is the way in which reality is known to the researcher?
- The methodological assumption is concerned with the nature of the research design and methods. It is concerned with the techniques used by the researcher to investigate the reality i.e. how does the researcher gain knowledge about the world, and how is the research constructed and conducted?

Wass and Wells (1994) indicated that the choice of research methodology should not be treated in isolation. Ontology, epistemology, methodology, the research techniques, and even the way in which the research will be presented, should be consistent both with each other and with the particular questions posed by the research. Simply, ontology informs methodology as to the nature of reality or as to what social research is supposed to study. Epistemology informs methodology about the nature of knowledge and where knowledge is to be sought. Methodology following these instructions prepares packages of appropriate research designs to be employed by researchers, instructing them as to where to focus their research activity and how to recognise and extract knowledge (Sarantakos 2005).

The ontological, epistemological and methodological assumptions of social research are "packaged" in paradigms, which guide everyday research. There are two main research paradigms which represent the two extremes of a continuum and which have been subject to a long-standing debate among researchers. These paradigms are the positivistic and the phenomenological paradigms (Easterby-Smith *et al.* 1991; Hussey and Hussey 1997).

3.3.1 Positivistic paradigm

The positivistic paradigm is dominant in accounting research in general and in AIS research in particular. Ontologically, positivist researchers assume that reality is external and objective (Easterby-Smith *et al.* 1991). They assume that an apprehensible reality exists which is driven by immutable natural laws and mechanisms (Guba and Lincoln 1994). In addition, the real world exists independently of subjective consciousness (Wass and Wells 1994, p.9). Turning from ontology to epistemology, positivist researchers view reality through a "one way mirror" where the researcher is removed from the object or phenomenon under study (Guba and Lincoln 1994). That is, reality is "out there" to be discovered objectively and value-free. Thus, researchers are independent from what is being researched (Hussey and Hussey 1997, p.48) that is researchers are detached from the phenomena of interest. A positivistic paradigm is characterised by quantitative scientific methodologies where testable hypotheses relating to relationships between variables are constructed.

Consequently, research based upon positivism tends towards the use of questionnaires for data collection and statistical analysis (Stiles 2003). Positivism is often taken to be identical to quantitative methodology because it contains the ontological and epistemological prescriptions that show how this methodology should conduct research (Sarantakos 2005).

There are some strengths and weaknesses in conducting research under a positivistic paradigm. The methods used can provide wide coverage of a range of situations, they can be fast and economical, and when statistics are aggregated from large samples, they may be of considerable relevance to policy decisions. However, they tend to be rather inflexible and artificial. They are not very effective in understanding the

significance that people attach to actions and they are not very helpful in generating theories (Easterby-Smith *et al.* 1991). However, despite that paradigms are in many cases not explicitly addressed in the research, much AIS research reflects a positivistic orientation as will be discussed later in this chapter.

3.3.2 Phenomenological paradigm

The phenomenological paradigm developed as a result of criticisms of the positivistic paradigm (Hussey and Hussey 1997). Ontologically, reality is not external and objective but it is socially constructed, subjective and given meaning by people (Easterby-Smith *et al.* 1991; Saunders *et al.* 2007). Researchers interact with what is being researched rather than being detached from the phenomena under investigation. Researchers are part of what is being observed and they bring their own interests and values to the research, and their values can affect the interpretation of findings. Researchers try to understand what is happening, they look at the totality of each situation and they develop ideas through induction from data.

Consequently, advocates of this approach tend to draw upon methods that develop meaning from the point of view of participants. They provide a way of gathering data that are seen as natural rather than artificial. They depend on small samples to be investigated in depth or over time and generally favour a qualitative approach to data collection and interpretation (Easterby-Smith *et al.* 1991; Hussey and Hussey 1997).

The phenomenological paradigm has strengths in its ability to look at changes over time, to understand people's meanings, to adjust to new issues and ideas as they emerge and to contribute to the evolution of new theories. However, data collection can take up a great deal of time and resources, and their analysis and interpretation may be very difficult (Easterby-Smith *et al.* 1991).

The ontological and the epistemological assumptions of each paradigm influence the methodology and guide the choice of research designs and instruments. Before selecting the methodology of the research, it is important to pay attention to the features of the two main paradigms mentioned above, in order to ensure that there are no contradictions or deficiencies in the research methodology. Table 3.1 summarises the main features of the two paradigms.

Table 3.1 Features of the two main paradigms

Positivistic paradigm	Phenomenological paradigm
- Tends to produce quantitative data	- Tends to produce qualitative data
- Uses large samples	- Uses small samples
- Concerned with hypothesis testing	- Concerned with generating theories
- Data are highly specific and precise	- Data are rich and subjective
- The location is artificial	- The location is natural
- Reliability is high	- Reliability is low
- Validity is low	- Validity is high
- Generalises from sample to population	- Generalises from one setting to another

(Source: Hussey and Hussey 1997, p.54)

3.3.3 Triangulation

In conducting the research, the researcher's decision to adopt any of the research paradigms will have a strong influence on the choice of research methodology and subsequently on the choice of research methods.

Methodology refers to "the overall approach to the research process, from the theoretical underpinning to the collection and analysis of the data" (Hussey and Hussey 1997, p.54). According to Sarantakos (2005), a methodology is a research strategy that translates the ontological and epistemological principles into guidelines that show how the research is to be conducted. The term "methodology" has a more philosophical meaning, and usually refers to the approach or paradigm that underpins the research (Blaxter *et al.* 2001, p.59). On the other hand, the term "methods" refers to techniques and procedures used to obtain and analyse research data (Saunders *et al.* 2007, p.3).

Sarantakos (2005) indicated that methodologies are closer to research practice than paradigms. Researchers refer to methodologies rather than paradigms when describing their work. It is more common, therefore, for researchers to report conducting "quantitative" than "positivistic" research and/or "qualitative" than "phenomenological" research, where reference to the ontological and epistemological nature of the research is the exception rather than the rule. In social science research, there are two main approaches for research: quantitative and qualitative approaches.

Quantitative research: In broad terms, quantitative research arises from the positivistic paradigm. Quantitative research entails the use of scientific methods and the systematic measurement of phenomena. It rests on measurement and therefore pre-structured data, research questions, conceptual frameworks and designs as well. Quantitative research is concerned with the collection and analysis of numerical data and relies on hypotheses derived deductively from theory, conceptualising reality in terms of the variables and relationships between them. Quantitative research tends to emphasise relatively large-scale and representative sets of data, that is samples are larger than in qualitative research, and generalisation through sampling is usually important. Quantitative research has well developed and codified methods for data analysis. Its methods in general are more unidimensional and less variable than qualitative methods, and it is therefore more easily replicable. Surveys and experiments are probably the most common data collection methods in quantitative research (Blaxter *et al.* 2001; Bryman 1988; Bryman and Bell 2003; Hussey and Hussey 1997; Punch 1998).

Burns (2000) indicated that the main strengths of the quantitative approach lie in precision and control. Control is achieved through sampling and design, while precision is obtained through quantitative and reliable measurement. Standardised measures of variables allow the researcher to state with precision the strength and direction of relationships between variables (Creswell *et al.* 2003).

Quantitative data enable standardised, objective comparisons to be made and the measurements of quantitative research permit overall description of situations or phenomena in a systematic way. In addition, procedures for quantitative data analysis, being well developed and codified, bring "objectivity" to the research.

However, De Vaus (2002) indicated that quantitative research is sometimes portrayed as being sterile and unimaginative. It fails to take account of people's ability to interpret their experiences and construct their own meanings. It sometimes produces trivial findings of little consequence due to the restriction on and the controlling of variables (Burns 2000). Hypotheses that are formed before the research commences bias the course of the study and restrict research options. In quantitative research, methods are given a central position, to the extent that they dictate the parameters of

the research. As a result, the research is limited only to what can be approached through existing methods. Quantitative research neutralises the researchers and their influence on the researched to the extent that they become disembodied abstractions, alienated from the world they are supposed to study (Sarantakos 2005).

Qualitative research: Qualitative research arises from the phenomenological paradigm. A qualitative approach focuses on the meaning, rather than the measurement of social phenomenon (Hussey and Hussey 1997). It is concerned with collecting and analysing information in as many forms as possible (Blaxter *et al.* 2001). It develops theories inductively. Qualitative research stresses the principle of openness and enters the field with few preconceived ideas or pre-structured models or patterns. There are no strict designs, no hypotheses, and no limits in its focus, scope or operation. Design, methods, and processes are open to change. It aims for in-depth and holistic understanding. Samples are usually small and its sampling is guided by theoretical rather than probabilistic considerations. Its methods are less formalised than those methods in the quantitative approach (Punch 1998; Sarantakos 2005). According to Bryman (1988), participant observation and unstructured interviews are the methods most closely associated with qualitative research.

According to Bryman and Bell (2003) and Punch (1998), the qualitative approach has its own strengths. Qualitative methods are flexible. They can be used in a wider range of situations and for a wider range of purposes. Qualitative methods can be more easily modified as a study progresses. Qualitative data have a holism and richness and are well able to deal with the complexity of social phenomena. In addition, qualitative methods enable problems to be investigated in their natural settings.

However, qualitative research is subjective and the research structure and procedures do not ensure the validity and reliability of methods. Qualitative research is unable to measure relationships between variables with the degree of accuracy that is required to establish social trends. Qualitative research tends to be based on small samples, and therefore, does not produce representative results. Consequently, research findings cannot be generalised. In addition, the nature of qualitative research that allows close contact with respondents can lead to some ethical problems. Further, one of the major

limitations of qualitative research is the time required for data collection, analysis and interpretation (Bryman and Bell 2003; Burns 2000; Sarantakos 2005).

Triangulation

Based on the above discussion, it appears that the quantitative and qualitative approaches have important differences. Punch (1998) indicated that the main differences between the two approaches lie in the nature of their data and in the methods used for collecting and analysing these data. However, neither approach is always superior to the other. According to Sieber (1973), both approaches have inherent strengths and weaknesses. Consequently, researchers should utilise the strengths of both techniques in order to understand better social phenomena.

It is not unusual in business research to take a mixture of approaches, particularly in the methods of collecting and analysing data. This allows the researcher to take a broader and often complementary view of the research problem or issue (Hussey and Hussey 1997). At a general level, the reasons for combining the quantitative and qualitative methods are to capitalise on the strengths of the two approaches and to compensate for the weaknesses of each approach (Punch 1998). Combining methodologies can generate complementary data about the phenomenon under investigation (Wass and Wells 1994). In addition, quantitative and qualitative researches are combined in order to provide a general picture (Blaxter *et al.* 2001; Bryman 1988). The current study relies on both a quantitative method (postal questionnaire) and a qualitative method (semi-structured interviews). Thus, it adopts both positivistic and phenomenological paradigms.

The use of different research approaches, methods and techniques in the same study is referred to as "triangulation" (Hussey and Hussey 1997, p.74). Denzin (1970, p.291) defines triangulation as the combination of methodologies in the study of the same phenomenon. He treats triangulation as an approach in which multiple observers, theoretical perspectives, sources of data, and methodologies are combined.

There are common types of triangulation according to Easterby-Smith *et al.* (1991), Hussey and Hussey (1997) and Ryan *et al.* (1992):

- Data triangulation: where data are collected at different times or from different sources;
- Investigator triangulation: where different researchers independently collect data on the same phenomenon and compare results;
- Methodological triangulation: where both quantitative and qualitative methods of data collection are used; and
- Theoretical triangulation: where a theory is taken from one discipline and is used to explain a phenomenon in another discipline.

Sarantakos (2005) mentioned another type of triangulation, sampling triangulation, where two or more samples are employed within the same study. Triangulation is employed for many reasons. Different research methods may reveal different aspects of a phenomenon (Wass and Wells 1994, p.19). This helps to gain a more complete understanding and a comprehensive picture of the phenomenon (Onwuegbuzie and Leech 2005) and often a complementary view of the research problem (Hussey and Hussey 1997). Triangulation raises the researcher above the personal biases that stem from single methodologies (Frankfort-Nachmias and Nachmias 1992) that is biases inherent in any single method could neutralise the biases of other methods (Creswell 2003). Because all data collection methods have limitations, triangulation can cancel out some of the disadvantages of certain methods (Teddlie and Tashakkori 2003).

Through triangulation, the findings from one method can be checked against the findings derived from another method (Blaxter *et al.* 2001). In addition, consistent findings among different data collection methods increase the credibility of research findings (Frankfort-Nachmias and Nachmias 1992). Triangulation improves the trustworthiness of research, strengthens understanding, increases confidence and provides richer findings and more accurate information (Holland and Campbell 2005; Rocco *et al.* 2003). Triangulation can increase the validity and reliability of research (Smith 2003). Through triangulation, the researcher can overcome the deficiencies of single-method studies. Thus, it seems that there is wide agreement among researchers that mixing different types of methods can strengthen a study.

The researcher, therefore, decided to employ both data and methodological triangulation in the current study, where data were collected at different times and

where both a quantitative data collection method (postal questionnaire) and a qualitative data collection method (semi-structured interviews) were used.

The use of interviews to triangulate data collected by questionnaire has been increasingly advocated by many authors and researchers. Saunders *et al.* (2007, p.147) indicated that semi-structured interviews might be a valuable way of triangulating data collected by other means such as questionnaire. Smith (2003) argued that semi-structured interviews could be used in conjunction with a questionnaire to derive the benefits of quantitative and qualitative methods. Frankfort-Nachmias and Nachmias (1992) mentioned that the researcher could use two or more methods of data collection in order to minimise the degree of specificity in bodies of knowledge for instance a questionnaire could be supplemented with interviews.

Hussey and Hussey (1997) considered that it is perfectly possible and even advantageous to use both qualitative and quantitative methods for collecting data for example a questionnaire survey providing quantitative data could be accompanied by a few in-depth interviews to provide qualitative insights and illuminations. Blaxter *et al.* (2001) indicated that the researcher might follow up a survey with some interviews in order to get a more detailed perspective on some of the issues raised.

In addition, Creswell (2003) argued that collecting diverse types of data best provides an understanding of a research problem, so that the study begins with a broad survey in order to generalise results to a population and then focuses, in a second phase, on detailed qualitative, open-ended interviews to collect detailed views from participants. Johnson and Turner (2003) also indicated that the combination of questionnaires and interviews in a study leads to a more complete and interesting depiction of the differences across the samples, while the use of in-depth interviews helps researchers to understand the quantitative findings.

In addition, the literature review reveals that questionnaires and interviews are the most commonly used methods in accounting in general and in AIS security in particular, which are discussed in later sections in this chapter.

3.4 Research Design

A research design is a master plan specifying the methods and procedures for collecting and analysing the information needed (Zikmund 2000). It is the basic plan for a piece of research. The design sits between the research questions and the data, showing how the research questions will be connected to the data, and what tools and procedures should be used in answering them. Therefore, the design needs to follow on from the questions and fit in with the data that will be collected (Punch 1998).

A research design should be effective in producing the required information within the constraints put on the researcher for example time, budgetary, and skills constraints (Ghauri and Gronhaug 2002). It helps to introduce a systematic approach to the research operation, thereby ensuring that all aspects of the study will be addressed and that they will be executed in the right sequence. Thus, it offers order and clarity that make replication easier and enable accurate assessment of its validity and reliability (Sarantakos 2005).

There are many choices to make when developing a research design. The first choice is about which should come first: the theory (deduction) or the data (induction). In other words, this is whether the research should use the deductive approach, in which the researcher develops a theory and hypothesis (or hypotheses) and designs a research strategy to test the hypothesis, or the inductive approach, in which the researcher collects data and develops a theory as a result of the data analysis (Saunders *et al.* 2007).

Hussey and Hussey (1997, p.13) defined deductive research as "a study in which a conceptual and theoretical structure is developed and then tested by empirical observation, thus particular instances are deduced from general inferences". Deduction is the process of establishing logical conclusions by proceeding from general and abstract to specific and concrete phenomena (Sarantakos 2005).

On the other hand, inductive research is "a study in which theory is developed from the observation of empirical reality, thus general inferences are induced from particular instances" (Hussey and Hussey 1997, p.13). In other words, induction is a process where the researcher observes certain phenomena and on this basis arrives at

conclusions. Thus, induction is the process of drawing conclusions by proceeding from the specific and concrete to the general and abstract (Sarantakos 2005). Thus, it seems that deduction is based on logic, while induction is based on empirical evidence. Table 3.2 summarises the main differences between deductive and inductive approaches to research.

Table 3.2 The main differences between deductive and inductive approaches

Deductive approach	**Inductive approach**
- Based on scientific principles	- Based on giving an understanding of the meanings humans attach to events
- Moving from theory to data	- Theory follows data
- The need to explain casual relationships between variables	- A close understanding of the research context
- The collection of quantitative data	- The collection of qualitative data
- A highly structured approach	- A more flexible structure to permit changes as the research progresses
- Researcher independence of what is being researched	- The researcher is part of the research process
- The necessity to select samples of sufficient size in order to generalise conclusions	- Less concern with the need to generalise

(Based on Saunders *et al.* 2007, p.120)

Based on the above discussion and according to the hypotheses developed in Section 3.2.4 above, the current study lends itself more to the deductive approach. The main advantage of the hypothesis-testing or the deductive approach is that there is initial clarity about what is to be investigated, and hence, data can be collected speedily and efficiently (Easterby-Smith *et al.* 1991). In addition, deduction can be a lower-risk strategy, although there are some risks such as the non-return of questionnaires. However, deduction tends to construct a rigid methodology that does not permit an alternative explanation of what is going on (Saunders *et al.* 2007).

However, most research involves both approaches at the same time. De Vaus (2002) argued that in practice there is a constant interplay between constructing theories (induction) and testing them (deduction). In addition, the practice of research does not by any means always fit neatly into these systematic approaches. Saunders *et al.* (2007) stated that not only it is perfectly possible to combine deduction and induction

within the same piece of research, but also it is often advantageous to do so. Thus, it seems that the two approaches rarely occur in isolation.

The second choice of the research design is concerned with the purpose of research. The classification of research purpose most often used in the research methods literature is the threefold one of "exploratory", "descriptive" and "explanatory". This classification is based on what the researcher is trying to accomplish - explore a new topic, describe a social phenomenon, or explain why something occurs (Neuman 2000). In addition, the design becomes more rigorous as we proceed from the exploratory stage, where we attempt to explore new areas of research, to the descriptive stage, where we try to describe certain characteristics of the phenomena of interest, to the explanatory stage, where we examine whether or not the relationships have been substantiated and answers to the research questions have been obtained (Sekaran 2003).

Exploratory study: An exploratory study is undertaken when there are very few or no earlier studies to which the researcher can refer for information about the issue or problem at hand. An exploratory study is needed to gain a better understanding of the dimensions of an issue or problem, to find out what is happening, to seek new insights, to ask questions and to assess phenomena in a new light. The aim of this type of study is to look for patterns, ideas or hypotheses, rather than testing or confirming a hypothesis. It addresses the "what" questions. However, it is difficult to conduct because there are few guidelines to follow. The steps are not well defined and the direction of inquiry changes frequently (Hussey and Hussey 1997; Neuman 2000; Robson 1993; Zikmund 2000).

Descriptive study: A descriptive study is undertaken when the problem is structured and well understood. The researcher begins with a well-defined subject and conducts research to describe it accurately. The aim of this type of study is to portray an accurate profile of persons, events or situations. Thus, the researcher observes and then describes what was observed. It seeks to determine the answers to who, what, when, where, and how questions. It may be an extension of a piece of exploratory research or the first step towards explanation. It does not explain the cause of findings. The data collected are often quantitative and statistical techniques are

usually used to summarise the information (Babbie 1998; Hussey and Hussey 1997; Neuman 2000; Punch 1998; Robson 1993; Saunders *et al.* 2007; Zikmund 2000).

Explanatory study: An explanatory study is a continuation of a descriptive study. The researcher goes beyond merely describing the characteristics, to analysing and explaining why or how it is happening. In this study, the problem is well structured; however, in contrast to descriptive research the researcher is confronted with cause and effect problems. Thus, an explanatory study seeks an explanation of a situation or a problem usually in the form of causal relationships between variables (Ghauri and Gronhaug 2002; Hussey and Hussey 1997; Robson 1993).

Based on the research objectives and questions mentioned in Sections 3.2.2 and 3.2.3 above, the current study seems to fit closely with the description of both descriptive and explanatory studies. The main objectives of the current study are to investigate the different types of AIS security threats facing UK companies and the controls implemented to prevent or reduce these threats, and to examine the impact of these security controls and the security effectiveness level achieved on the reduction of AIS security threats. Thus, the current study lends itself to the category of descriptive research. In addition, it can be considered as explanatory research based on the hypotheses developed in Section 3.2.4.

The third choice of the research design is whether to attempt to sample across a large number of companies or situations or whether to focus on a small number of situations and attempt to investigate them over a period of time. This is a choice between cross-sectional and longitudinal designs (Easterby-Smith *et al.* 1991).

Cross-sectional design: This entails the collection of data on more than one case and at a single point in time. Normally, different companies or groups of people are selected and a study is conducted to ascertain how factors differ. In addition, a cross-sectional study employs samples from different sectors and compares them by using a set of criteria related to the theme of the study. In the context of descriptive studies, the purpose of cross-sectional studies is to establish differences between sections. It can also produce data that will permit the establishment of causal relationships. Cross-sectional study is conducted when there are constraints of time and resources.

The data are collected just once over a short period of time before they are analysed and reported. A cross-sectional study has the ability to describe economically the features of large numbers of people and companies.

However, some problems are associated with this design. The first is how to select a large enough sample to be representative of the total population. In addition, this design does not explain why a correlation exists; only that it does or does not exist (Bryman and Bell 2003; Easterby-Smith *et al.* 1991; Hussey and Hussey 1997; Sarantakos 2005).

Longitudinal design: This is a study, over time, of a variable or group of subjects. Researchers using the longitudinal design examine features of people or companies at more than one time that is respondents are questioned at different moments in time. The purpose of the longitudinal surveys is to examine continuity of response and to observe changes that occur over time. A longitudinal design can produce significant results from a very small number of cases and this can reduce the problems of gaining access if the research is to be carried out in companies. However, it is extremely time-consuming and expensive to conduct. The complexity of data requires very high skills from the researcher. In addition, once started, the study must be continued and there is the problem of losing subjects during the course of the study (Babbie 1998; Easterby-Smith *et al.* 1991; Hussey and Hussey 1997; Zikmund 2000). According to Bryman and Bell (2003), this design is of relatively little use in business and management research, partly because of the time and cost involved.

Based on the above discussion and due to the descriptive and explanatory nature of the current study, a cross-sectional design is well suited for achieving its objectives. The current study aims to investigate the differences among industry sectors in the UK regarding the types of AIS security threats facing companies, security controls implemented to prevent or reduce these threats and the management framework for AIS security within these companies. In addition, the cross-sectional design is well suited when there are constraints of time and resources. Moreover, Orlikowski and Baroudi (2002) argued that cross-sectional studies are the predominant form of research in IS.

3.5 Data collection methods available

Methods refer to a systematic, focused, and orderly collection of data for obtaining information from them in order to solve the research problems or to answer the research questions (Ghauri and Gronhaug 2002, p.85). Zikmund (2000) argued that once the research design has been formalised, the next step is the process of gathering information from respondents. There are many data collection methods in social research. However, De Vaus (2002) indicated that it is difficult to decide which method is the best. The decision depends on the purpose of the study, sample size and distribution, time and money available, and the environment and conditions under which the study is conducted. The choice of the data collection method depends on the degree of accuracy required and expertise of the researcher as well (Sekaran 2003).

Blaxter *et al.* (2001) added other issues that must be considered in reaching the right decision including the literature and familiarity with the subject under study. Moreover, many authors and researchers agreed that the choice of a data collection method is also driven by the research questions (Blaxter *et al.* 2001; Ghauri and Gronhaug 2002; Punch 1998).

Three methods are recommended in the literature of IS in general and AIS security in particular, namely questionnaire survey, interviews and case studies. The characteristics, advantages and limitations of these methods are considered in the following section.

3.5.1 Questionnaire survey

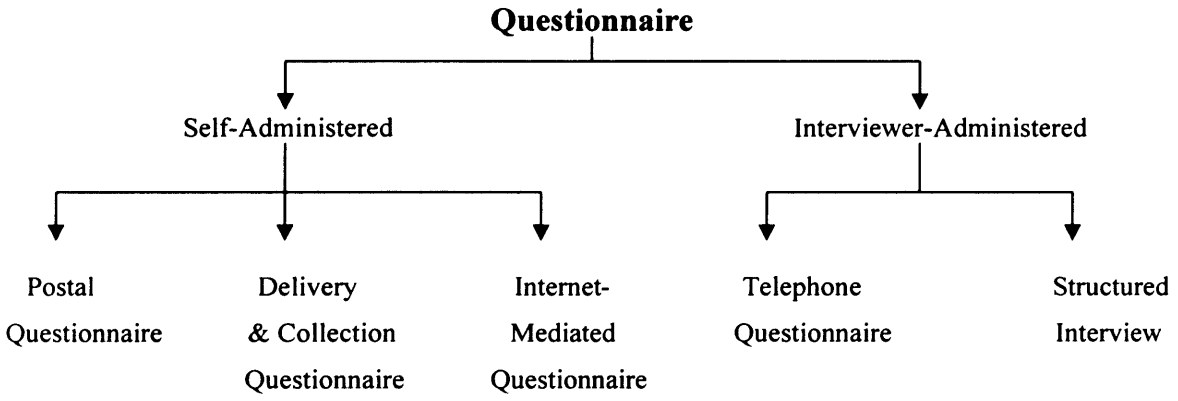
The questionnaire survey is the most commonly used method of data collection in the social sciences in general and accounting research in particular. It is the most popular method used in previous research on IS security (Abu-Musa 2004a and b; Chang and Ho 2006; Davis 1997; Henry 1997; Hitchings 1995; Hong *et al.* 2006; Huang *et al.* 2006; Kankanhalli *et al.* 2003; Kotulic and Clark 2004; Loch *et al.* 1992; Ryan and Bordoloi 1997; Whitman 2004; Yeh and Chang 2007).

Hussey and Hussey (1997, p.161) stated that "a questionnaire is a list of carefully structured questions; chosen after considerable testing, with a view to eliciting

reliable responses from a chosen sample". Questionnaires are associated with both positivistic and phenomenological methodologies. Under a positivistic approach, closed questions should be used, whereas a phenomenological approach suggests open-ended questions.

There are a number of different ways in which questionnaires can be administered. They can be either self-administered questionnaires or interviewer-administered questionnaires as shown in Figure 3.2 below.

Figure 3.2 Types of questionnaires



(Based on Saunders *et al.* 2007, p.357)

The self-administered questionnaires are completed by respondents. They can be sent by post to the intended respondents, who are then expected to complete and return them by post (postal or mail questionnaire). They can be delivered by hand to each respondent and collected later (delivery and collection questionnaire). They also can be administered electronically using the internet (internet-mediated questionnaire). On the other hand, responses to interviewer-administered questionnaires are recorded by the interviewer based on each respondent's answer. They can be administered using telephone (telephone questionnaire) or face-to-face (structured interview) (Blaxter *et al.* 2001; Saunders *et al.* 2007).

The choice between questionnaire methods depends on the nature of the survey, the sample, time and cost constraints, the importance of response rates and the types of questions (De Vaus 2002).

Questionnaires, as with any other method, have both strengths and weaknesses, and hence advantages and limitations that the researcher must be aware of. Questionnaires are less expensive and less time-consuming than other methods, particularly when responses from a large, dispersed population are required (Burns 2000; Hussey and Hussey 1997; Sarantakos 2005). They can be completed at the respondents' convenience. Thus, there is a better chance that respondents will take time to think about their answers, to check personal records and to consult other sources if necessary (Frankfort-Nachmias and Nachmias 1992; Neuman 2000; Zikmund 2000).

They offer less opportunity for interviewer bias because respondents are not influenced by interviewer characteristics or techniques (Frankfort-Nachmias and Nachmias 1992; Oppenheim 1992). They offer greater assurance of anonymity of respondents, which is important, particularly when sensitive issues are involved (Frankfort-Nachmias and Nachmias 1992; Neuman 2000). Moreover, Burns (2000) argued that a questionnaire that can guarantee confidentiality might elicit more truthful responses than would be obtained from a personal interview. In addition, errors resulting from the recording of responses by interviewers are reduced. They are a stable, consistent, uniform measure and free from variation (Sarantakos 2005).

However, there are a number of problems associated with the use of questionnaires. Questionnaires require simple, easily understood questions and instructions. They do not allow the opportunity to correct misunderstandings, to probe for additional information, or to offer explanations or help (Frankfort-Nachmias and Nachmias 1992; Oppenheim 1992). They do not provide opportunities for motivating the respondents to participate in the survey or to answer the questions (Sarantakos 2005). The researcher has no control over the conditions in which the questionnaire is completed. Researchers are not sure whether the right person has answered the questions and whether the order of the questions - where required - was followed (Neuman 2000; Wilson 1996). Incomplete questionnaires cannot be followed up (Burns 2000; Oppenheim 1992).

Moreover, researchers cannot visually observe the respondents' reactions to questions, physical characteristics or the setting (Neuman 2000). Respondents may be limited from providing free expression of opinions particularly in the case of closed-

ended questions (Burns 2000). Finally, and perhaps the most serious problem, is the low response rate, particularly with mail or postal questionnaires (Burns 2000; Frankfort-Nachmias and Nachmias 1992; Neuman 2000; Oppenheim 1992; Sarantakos 2003). Hussey and Hussey (1997) indicated that response rates of 10 percent or less are common and this introduces the problem of sample biases because those who respond may have a particular interest in the topic and, therefore, may not at all represent the population from which they are drawn.

Despite the above disadvantages of questionnaires, every effort was made to minimise these limitations by pre-testing them prior to distribution, which is presented in more detail in Section 3.6.1.2.

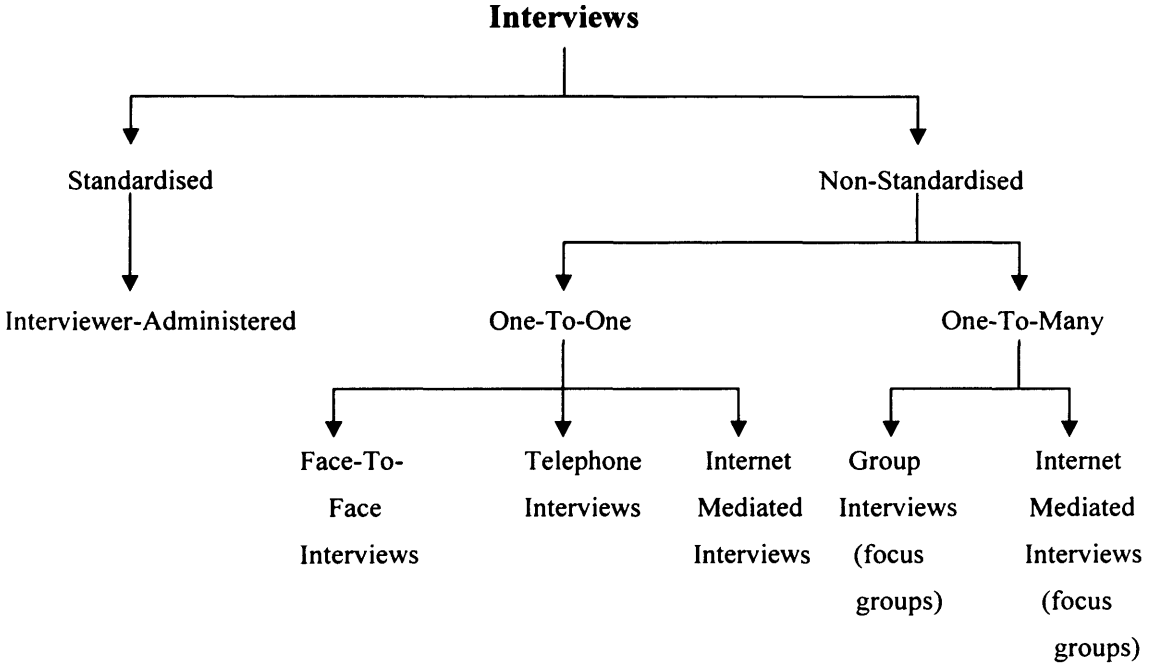
However, some effective techniques can be employed for improving the response rate. An attractive questionnaire design and question wording both help to assure a good response rate (Zikmund 2000). The cover letter must succeed in convincing the respondents to complete the questionnaire and mail it back. It should therefore identify the sponsor of the study, explain its purpose, the method of sampling used and how the respondents are chosen, and should tell the respondents the importance of completing the questionnaire (Frankfort-Nachmias and Nachmias 1992; Oppenheim 1992). Questionnaires could be accompanied by a self-addressed, freepost return envelop (Neuman 2000; Sarantakos 2005). In addition, the respondents' motivation for returning a questionnaire may be increased - in certain cases - by offering monetary incentives or by offering them the chance to win a major prize if the questionnaire is returned (Oppenheim 1992; Zikmund 2000). Follow-up reminder letters could be sent to those who have not returned the questionnaire (Neuman 2000; Zikmund 2000). Finally, and most importantly, is the length of the questionnaire. Hussey and Hussey (1997) argued that response rates could be increased by keeping the questionnaire as short as possible.

3.5.2 Interviews

Interviewing is one of the most common methods of data collection in social research. Interviews have become increasingly utilised in recent years in IS research in general and AIS security in particular, either as the sole data collection method (Keller *et al.* 2005) or combined with other methods (Mitchell *et al.* 1999; Straub and Welke 1998;

Tryfonas *et al.* 2001). An interview is a conversation or purposeful discussion between two or more people (Robson 1993, p.228). It is a method of collecting data in which selected participants are asked questions in order to find out what they do, think or feel (Hussey and Hussey 1997, p.156).

Figure 3.3 Types of interviews



(Based on Saunders *et al.* 2007, p.313)

Interviewing is employed as a data collection method in most research designs regardless of the underlying methodology (Sarantakos 2005). Interviews are associated with both positivistic and phenomenological methodologies. Under a positivistic approach they are highly formalised and structured, whereas a phenomenological approach suggests informal and unstructured conversations. In between, there are intermediate positions (Hussey and Hussey 1997; Saunders *et al.* 2007). Interviews could be conducted either face-to-face or by telephone or online, and these forms of interview are summarised in Figure 3.3.

Broadly speaking, there are three types of interviews used in social research: structured interviews, semi-structured interviews, and unstructured interviews.

Structured interviews: These are the least flexible type of interviews. Structured interviews employ a structured questionnaire, which is verbally presented to

respondents, with the answers recorded in the questionnaire by the interviewer (Frankfort-Nachmias and Nachmias 1992; Sarantakos 2005). Every respondent is asked the same questions with the same wording and in the same order (Wilson 1996). There is very little flexibility in the way questions are asked or answered in the structured interview setting (Fontana and Frey 2000). The interviewer is expected to act in a neutral manner, keeping the same tone of voice across the interviews, offering a consistent impression to the respondents, using the same style, appearance, prompts, probes, etc. (Sarantakos 2005). Thus, the highest degree of objectivity and uniformity in procedures can be achieved and the opportunities for interviewer bias can be restricted (Smith 2003). All or nearly all of the questions are closed-ended and the respondents are forced to select their answers from a limited set of previously established responses (Burns 2000). The use of closed-ended questions makes coding of answers easier and has advantages for the subsequent analysis. Closed-ended questions also eliminate the opportunities for error associated with open-ended questions. However, they sacrifice the comparative advantage of the interview method by failing to include the flexibility and richness of responses offered by open-ended questions (Smith 2003). In addition, this detachment and impersonal approach can prevent trust and rapport building up between the interviewer and respondents (Burns 2000). This form of interview can be employed in quantitative research.

Semi-structured interviews: In semi-structured interviews, the interviewer has a list of questions on specific topics to be covered, often referred to as an interview guide, but he has greater freedom in the sequencing of questions, in the exact wording and in the amount of time and attention given to different topics (Bryman and Bell 2003; Robson 1993). Some questions can be omitted in particular interviews and additional questions can be asked, as the interviewer sees fit, to examine associated issues that arise in the interview (Saunders *et al.* 2007; Smith 2003). This form of interview allows respondents to answer more on their own terms than the standardised interview permits. The interviewer can seek both clarification and elaboration on the answers given, can have more latitude to probe beyond the answers and thus can enter into a dialogue with the interviewee (May 1997). This permits greater flexibility than the structured interview; however, the comparability of the information between respondents is difficult to assess and response-coding difficulties may arise (Burns

2000). This form of interview can be employed in quantitative or qualitative research (Sarantakos 2005).

Unstructured interviews: These are the most flexible type of interviews. They take the form of a conversation between the interviewer and the interviewee (Burns 2000). The interviewer does not enter the interview setting with a planned sequence of questions to be asked, but with a series of topics for discussion (Sekaran 2003; Smith 2003). The interviewee is then allowed to talk freely about events, behaviour and beliefs in relation to the topic area, so that this type of interaction is sometimes called non-directive (Saunders *et al.* 2007). The interviewer has a great deal of freedom to probe various areas and to raise specific queries during the interview (Frankfort-Nachmias and Nachmias 1992). The actual words and phrases used may therefore vary significantly between interviews (Smith 2003). This type of interview is a powerful research tool and can provide a greater breadth of data than other methods (Fontana and Frey 2000; Punch 1998). However, it demands a sensitive, skilled and cautious interviewer in order to understand the other person's views and, at times, to assist individuals to explore their own beliefs (Easterby-Smith *et al.* 1991). The unstructured interviews can take a long time, they can be difficult to interpret and analyse and the coding is a difficult task in spite of improved coding techniques and systems (Ghauri and Gronhaug 2002). This form of interview is mostly used in qualitative research.

Based on the above, it appears that these three types of interviews have different strengths and weaknesses and different purposes in research. The type of interview selected should be aligned with the strategy, purposes, and research questions. Accordingly, given the research objectives, as well as the resources and time constraints, semi-structured interviews were adopted in the present study and full details of the interview findings are presented in Chapter 5.

However, the researcher must be aware of the strengths and limitations of the interviews - despite their type - as a data collection method, in order to benefit from the strengths, minimise the limitations and maintain the quality of research.

Interviews allow greater flexibility in the questioning process and can be adjusted to meet many diverse situations (Frankfort-Nachmias and Nachmias 1992). They result in a high response rate that makes the data more representative than data solicited through a postal questionnaire (Burns 2000). They give the interviewer the opportunity to observe non-verbal cues that help in understanding the verbal response, that can change or even, in extreme cases, reverse its meaning (Robson 1993). The identity of the interviewee is known, and the interviewer has an opportunity to control the conditions under which the questions are answered (Sarantakos 2005). In addition, greater length is possible in interviewing than when other methods are used.

On the other hand, interviews are more expensive and time-consuming than other methods such as questionnaires (Zikmund 2000). They offer less anonymity since the interviewer knows the identity of the respondent (Sarantakos 2005). They are less convenient than other methods. The flexibility of interviews leaves room for the interviewer's personal influence and bias (Frankfort-Nachmias and Nachmias 1992), and may generate difficulties in categorising and evaluating responses (Burns 2000).

3.5.3 Case studies

Case studies have become quite common in accounting research, especially in management accounting (Ryan *et al.* 1992). In IS research, case studies are gaining acceptance as an appropriate research method and increasing numbers are appearing in the research literature (Dhillon and Moores 2001; Gercek and Saleem 2005; Kotulic and Clark 2004; Onions 2006; Shih and Wen 2005; Spurling 1995; Willison 2006).

Robson (1993, p.146) defines a case study as "a strategy for doing research which involves an empirical investigation of a particular contemporary phenomenon within its real life context using multiple sources of evidence". The basic idea is that one case (or perhaps a small number of cases) will be studied in detail using whatever methods seem appropriate (Punch 1998). A case can be a single company, a single location, a person, or a single event. However, in business research, the most common use of the term associates the case study with a location, such as a workplace or

company, and the emphasis tends to be upon an intensive examination of the setting (Bryman and Bell 2003).

The case study aims to understand the case in depth and in its natural setting, recognising its complexity and its context (Punch 1998). It involves gathering detailed information about the case, often over a very long period of time (Hussey and Hussey 1997). A case study often involves data collection through multiple sources such as observation (both participant and non-participant), interviews (unstructured and structured), and the use of documents and records (Burns 2000; Robson 1993; Smith 2003).

In business studies, case study research is particularly useful when the phenomenon under investigation is difficult to study outside its natural setting and when the concepts and variables under study are difficult to quantify (Ghauri and Gronhaug 2002). Case studies are intensive, generate rich subjective data, and they may bring to light variables, phenomena, processes and relationships that deserve more investigation (Burns 2000). They produce first-hand information, and employ methods that encourage familiarity and close contact with the informants (Sarantakos 2005). In addition, the in-depth case studies can provide an understanding of the important aspects of a new research area (Punch 1998).

However, case studies provide very little evidence for scientific generalisation (Burns 2000). Ryan *et al.* (1992) indicated that authors of accounting case studies frequently apologise for the fact that the size of their sample creates difficulties in generalising their findings. Findings entail personal impressions and biases, hence there can be no assurance of objectivity, validity and reliability, and the research cannot be replicated (Sarantakos 2005). Moreover, the process of the research can be very time-consuming and can result in an information overload that is sometimes difficult to analyse and to interpret (Blaxter *et al.* 2001; Bryman 1989).

Although this method has been used in previous studies of IS in general and AIS security in particular, it is not used in the current study due to the above disadvantages and because limited time and resources are available for the study.

3.6 Data collection methods of the current research

The aim of this section is to provide a detailed explanation of the research methods used in the current study. As mentioned earlier in Section 3.3.3, this study employed quantitative and qualitative approaches using a postal questionnaire and semi-structured interviews. Miles and Huberman (1994) indicated that qualitative data could help quantitative analysis by confirming and illustrating quantitative findings.

The first stage involved a postal questionnaire. This method was chosen because of its specific relevance to the nature of this study as well as the advantages it offers compared to other research methods. Moreover, it is the most popular method used in previous research on IS security.

The second stage involved semi-structured interviews with IT managers of large UK companies listed on the London Stock Exchange. As mentioned earlier, the use of qualitative interviews to triangulate data collected by questionnaire was increasingly advocated by many researchers. Thus, semi-structured interviews were conducted after completion of the questionnaire in order to understand and confirm the results obtained from the questionnaire analysis, to achieve a high degree of validity and reliability (Smith 2003), to enrich the quality of information collected, and to fill in any gaps in the data that might occur in the questionnaire's results. This section provides a detailed explanation of both methods, the strengths and weaknesses of each, the procedures followed, and the statistical tests used.

3.6.1 Postal questionnaire

As stated above, the primary and first data collection method was the postal questionnaire. There are many advantages and disadvantages of using a postal questionnaire. One of its main strengths is its ability to collect data from a large number of companies located in a wide geographical area (Abu-Musa 2006a and b; Mitchell *et al.* 1999). It is relatively less expensive and less time-consuming compared with personal interviews and a telephone questionnaire (Zikmund 2000). The postal questionnaire provides greater anonymity to encourage respondents to give their true opinion rather than an acceptable answer when dealing with sensitive issues (Bailey 1994; Frankfort-Nachmias and Nachmias 1992). Respondents can complete it at their convenience (Bryman 2001; Sekaran 2003), they can take time to think about

their responses and can consult personal documents or other people, if necessary (Zikmund 2000). Thus, the postal questionnaire was chosen as the primary and first data collection method for the following reasons:

- The sample is relatively large;
- The UK is a large country and the sample is distributed around the country;
- The time and resources are relatively limited; and
- The postal questionnaire enables a high degree of anonymity and confidentiality that is necessary particularly when dealing with very sensitive and intrusive security issues.

Despite these advantages, the postal questionnaire is not without limitations (Section 3.5.1). The first and most important problem of using a postal questionnaire is the poor response rate as identified and experienced by many IS security researchers. Table 3.3 gives examples of the response rates achieved by some IS security researchers.

Table 3.3 Examples of response rates achieved in some IS security research

Name of article	Author(s)	Journal & date of issue	Response rate
Information systems security issues and decisions for small business: an empirical examination	Atul Gupta and Rex Hammond	Information Management & Computer Security 2005, 13:4	13.8%
Controlling corporate e-mail, PC use and computer security	Gayle Webb White and Sheila Pearson	Information Management & Computer Security 2001, 9:2/3	13.8%
An assessment of accounting information security	Charles Davis	The CPA Journal 1997, 67:3	11.6%
Threats and countermeasures for information system security: a cross-industry study	Quey-Jen Yeh and Arthur Jung-Ting Chang	Information & Management 2007, 44:5	10.9%
Do information security policies reduce the incidence of security breaches: an exploratory analysis	Neil Doherty and Heather Fulford	Information Resources Management Journal 2005, 18:4	7.7%
The application of information security policies in large UK-based organisations: an exploratory analysis	Heather Fulford and Neil Doherty	Information Management & Computer Security 2003, 11:2/3	7.3%
Information security policy's impact on reporting security incidents	Terry Wiant	Computers & Security 2005, 24:6	5.6%
Why there aren't more information security research studies	Andrew Kotulic and Jan Guynes Clark	Information & Management 2004, 41:5	0.6%

However, the researcher considered the above limitations and the questionnaire was pilot-tested before sending it out to respondents (Section 3.6.1.2). In addition, every effort was made to maximise the expected response rate.

3.6.1.1 Questionnaire design and layout

According to Wass (1994), in order to generate the greatest number of high quality responses, researchers must pay careful attention to the design of the questionnaire including its length, wording, sequence of questions and layout.

The questionnaire of the current study was designed after an extensive review of the existing literature on IS security in general and AIS security in particular. In addition, many security reports (GAO 1998; 2004), surveys (BERR 2008; DTI 2004 c; 2006; DTT 2006a and b; 2007; Ernst &Young 2005; 2006; Gordon *et al.* 2005; 2006; KPMG 1998; 2006; Richardson 2007), standards (ISO/IEC 17799 2005; ISO/IEC 27001 2005), and guidelines (BSI 2000; CICA 1998; COBIT 2000; ISACA 2005; ISACF 2001; NIST 800-53 2005; OECD 2002) were examined.

Then, three main themes were identified, in addition to the background information, on which the main structure of the questionnaire was based. These themes are:

- The management framework of the AIS security;
- AIS security threats; and
- AIS security controls.

These themes cover the major issues highlighted in the literature review on the AIS security (see Chapter 2). A list of questions was developed under each theme and the questionnaire was organised into four sections covering these themes.

Section 1: The management framework of the AIS security

The questions in this section aimed at collecting the respondents' opinions concerning the management framework of AIS security within their companies. The questions were grouped under seven sections including the AIS security policy; security training and awareness programs; risk assessment; incident handling, disaster recovery and a business continuity plans; security budget; security standards and certification; and finally AIS security effectiveness.

The questions in Section 1.1 addressed the AIS security policy and were set to investigate the existence of a written AIS security policy within the company and the frequency of updating this security policy (if any).

The questions in Section 1.2 focused on the security training and awareness programs. Respondents were asked about the existence of a formal security training and awareness program for the managers, employees and other users and were asked to indicate their level of agreement with a list of statements concerning the security awareness practices within their companies, using a five-point Likert scale.

The questions in Section 1.3 aimed at evaluating the risk assessment practices within UK companies. Respondents were asked about the existence and frequency of undertaking the risk assessment within their companies, and were asked to indicate their level of agreement with some statements regarding their companies' risk assessment activities. Section 1.4 investigates the existence of incident handling procedures, disaster recovery and business continuity plans within UK companies, the frequency of updating these plans, and the actions taken to reduce future security incidents.

Section 1.5 addressed the security budget. Respondents were asked about the existence of a separate security budget within their companies. They were asked also to rank their companies top three areas of AIS security spending. Hussey and Hussey (1997) argued that after ranking the first three respondents might be unable to decide what their opinions are amongst the remainder and are likely to leave them blank.

Section 1.6 aimed to investigate the respondents' awareness of the British Standard BS 7799 (now ISO 27000) and its two parts ISO/IEC 17799 and ISO/IEC 27001, while Section 1.7 covered AIS security effectiveness. Respondents were asked to state the techniques used by their companies to evaluate AIS security effectiveness and to rank the top three critical success indicators of AIS security management within their companies.

Section 2: Security threats to the company's AIS

The questions in this section aimed to investigate the most common types of security threats facing the companies' AIS and the sources of those threats. In the first question, respondents were given a list of common sources of security threats and were asked to rank the top three, where one represents the most common source. The second question included 13 security threats identified from the literature review (Chapter 2) and respondents were asked to indicate the frequency of occurrence of each type of threat in their company in the last year by ticking the appropriate box on a given scale.

Section 3: Security controls of the company's AIS

This section was set to investigate the AIS security controls within UK companies that were implemented to reduce security threats. The respondents were given a list of security controls identified from the literature review (Chapter 2), that were grouped under the following sub-titles:

- Administrative/organisational security controls
- Personnel security controls
- Software security controls
- Hardware/physical security controls
- Input/data security controls
- Output security controls
- Network security controls

Respondents were asked to indicate whether their companies are using each control, are planning to use it, or there were no plans to use it.

Section 4: General and background information

This section focused on the respondents' and their companies' background. Respondents were asked eight questions related to their job title, number of years of experience in their current job, their most recent educational qualification and their academic field of study. Respondents were asked also about the number of employees in their companies and their companies' industry sector. The main objective of these questions was to obtain a profile of those who participated in the study. They are also useful for the statistical analysis and comparisons.

Toward the end of the questionnaire, the respondents were provided with sufficient space to provide any further comments or suggestions that they thought might have relevance to the issues addressed in the questionnaire, and which the researcher had overlooked.

Finally, the respondents were asked to provide their contact details (title, name, address, telephone number and e-mail address), if they were willing to be contacted, for arranging a follow-up face-to-face interview concerning their opinions on AIS security within their companies and if they wished to receive a copy of the study results.

According to Frankfort-Nachmias and Nachmias (1992), the major considerations involved in formulating the questions are as follows:

- Content of questions;
- Structure (type) of questions;
- Format of questions (response categories); and
- Sequence of questions.

Content of questions: The questions in the questionnaire can be classified into two general categories: questions about subjective experiences or opinions and factual questions. Questions about subjective experiences are designed to obtain the respondents' beliefs, perceptions, attitudes, feelings and opinions (Frankfort-Nachmias and Nachmias 1992; Sekaran 2003). Most questions in Sections 1, 2, and 3 are intended to obtain the respondents' opinions regarding the AIS security practices within their companies. On the other hand, factual questions are designed to obtain objective information from respondents regarding their background including their age, gender and level of education (Easterby-Smith *et al.* 1991). Section 4 of the questionnaire asked respondents to provide information about their background and their companies' characteristics.

Structure (type) of questions: The questionnaire contained both closed-ended and open-ended questions; however, the majority were closed-ended questions. In the closed-ended questions, the respondents are asked to select an answer from among a list provided by the researcher (Babbie 1998). They are sometimes called forced-

choice questions (De Vaus 2002) or fixed-alternative questions (Zikmund 2000). They are easy to ask and quick to answer. They require no writing by respondents (Frankfort-Nachmias and Nachmias 1992). They provide a greater uniformity of responses and therefore greater reliability and comparability of answers (Burns 2000; Zikmund 2000). In addition, less effort is required to code, analyse and interpret answers (Peterson 2000). Their major drawback is that they may introduce bias, either by forcing respondents to choose from given alternatives or by making respondents select alternatives that might not have otherwise come to mind (Frankfort-Nachmias and Nachmias 1992).

However, these weaknesses can be reduced by mixing open-ended and closed-ended questions in the questionnaire or by adding an "other (please specify)" category. This category allows respondents to fill in their answers, in their own words, in cases where the responses provided by the researcher are incomplete or inappropriate (De Vaus 2002; Hussey and Hussey 1997; Johnson and Turner 2003; Oppenheim 1992).

In contrast to the closed-ended questions, the open-ended questions are not followed by any kind of choice, and the answers have to be recorded in full (Oppenheim 1992). They are sometimes called free-answer questions (Zikmund 2000). They allow respondents to state their answers in the way they see appropriate, in their own way and in their own words (Sarantakos 2005). The chief advantage of the open-ended questions is the freedom they give to the respondents (Oppenheim 1992). They permit an unlimited number of possible answers. They permit creativity, self-expression, and richness of detail (Neuman 2000).

However, the open-ended questions take more time and effort to answer and produce large amounts of information that require extensive time and effort to code, analyse and interpret (Peterson 2000; Sarantakos 2005). They open the possibility of misunderstanding and researcher bias (Babbie 1998). They do not allow accurate comparisons. They may deter busy respondents from replying to the questionnaire and they tend to be more expensive than closed-ended questions (Hussey and Hussey 1997; Peterson 2000).

In the current study, the researcher attempted to overcome the limitations of the closed-ended and open-ended questions and to gain the best of both types, as follows:

- There were a limited number of open-ended questions in the questionnaire and the majority were closed-ended questions;
- The researcher tried to provide the respondents with a sufficient range of alternatives or categories from which to choose; and
- Whenever appropriate, the researcher added a category "other (please specify)" to allow respondents to create their own answer, in their own words, in the cases where the responses provided by the researcher were incomplete or inappropriate.

Format of questions (response categories): In structuring the response categories of the closed-ended questions, the researcher employed some of the most common techniques including the multiple-choice format, checklists, ranking and rating.

Multiple-choice format requires respondents to choose just one response from a list of alternatives (De Vaus 2002) such as asking respondents to select the industry sector that most closely corresponds to their companies' line of business (see Section 4 of the questionnaire).

Checklists involved listing a set of items and asking the respondents to select those that apply (De Vaus 2002) such as providing the respondents with a list of actions supposed to be undertaken after a security incident and asking them to select or tick all that apply (see Section 1.4 of the questionnaire).

The ranking format was used whenever we wanted to obtain information regarding the degree of importance or the priorities that respondents give to a set of items (Frankfort-Nachmias and Nachmias 1992). For example, the respondents were given a list of common sources of AIS security threats, and were asked to rank the top three sources (see Section 2 of the questionnaire).

Rating scales involve a set of responses where the alternative answers are ordered from low to high. Respondents need to indicate where between the low and high extremes their attitude lies (De Vaus 2002). One of the more frequently used types of scale is the Likert scale, where respondents are asked to indicate their level of

agreement with a statement by ticking a box. The Likert scale where a number of different statements can be provided in a list that does not take up much space has many advantages. It is simple for the respondents to complete and also simple for the researcher to code and analyse (Hussey and Hussey 1997). In Section 1 of the questionnaire, there are many questions in which the respondents were asked to indicate their level of agreement with a list of statements such as risk assessment activities.

Sequence of questions: This refers to the order in which questions are organised within the context of the questionnaire. A common requirement is that questions should be presented in a logical order, allowing for transition and flow, from one topic to the next, and avoiding distortions and problems (Hussey and Hussey 1997; Sarantakos 2005). In the current study, the researcher followed the funnel format, where the questioning moved from general to specific, from impersonal to personal, and from non-sensitive to sensitive questions (Sarantakos 2005). The questions related to each other logically and they moved from general to specific topics.

There is wide agreement among many authors that early questions should not address personal issues or background information like age, experience and educational level. Babbie (1998) stated that requests for demographic data (age, gender and the like) should generally be placed at the end of the questionnaire, since placing these items at the beginning gives the questionnaire the initial appearance of routine form, and the respondent may not be motivated to complete it. Dillman (2000) advised researchers not to begin by asking a series of demographic questions. Although they may be highly relevant to the study objectives and easy to answer, respondents will not see obvious relevance to the topic. Hussey and Hussey (1997) also indicated that it could be better to put classification questions at the end, so that the respondents are not deterred at the start. Moreover, Zikmund (2000) argued that it is not advisable to ask demographic questions at the beginning of the questionnaire because asking personal information may be embarrassing or threatening to respondents. In order to avoid these drawbacks, the demographic questions in this study were placed in the last section of the questionnaire (Section 4).

There is also an agreement among many authors regarding the importance of the wording of questions. Based on Bryman (1989), De Vaus (2002), Frankfort-Nachmias and Nachmias (1992), Saunders *et al.* (2007) and Zikmund (2000), considerable attention was given to developing clear, unambiguous and useful questions. Thus, the researcher tried to keep questions as simple as possible. The questions were short because the shorter the question, the less confusing and ambiguous it will be. The content of each question related to the research topic. Each question addressed one point only. The researcher avoided leading questions since they are a major source of bias, and finally the researcher avoided negative questions since they can be misunderstood.

Regarding the length of the questionnaire, there is a widespread view that long questionnaires should be avoided. De Vaus (2002) indicated that long questionnaires increase the burden on respondents and this leads to increased reluctance to participate and thus leads to non-response. However, a very short questionnaire may suggest that the research is insignificant and hence not worth bothering with (Saunders *et al.* 2007). The length of the questionnaire depends on many factors such as the research objective, respondents' characteristics, methods of analysis, availability of resources, and most importantly, on the number of variables considered in the study (Sarantakos 2005). Therefore, the questionnaire of the current study was only seven pages in length and was printed as a booklet with two staples in the spine which looks more professional (Dillman 2000), and did not take more than 30 minutes to be completed. However, it covered all the major aspects of the AIS security issue. A complete copy of the questionnaire with the covering letter is provided in Appendix 1.

3.6.1.2 Pilot test of the questionnaire

Once the questionnaire was developed, each question and the questionnaire as a whole must be pilot tested or pretested before final administration. A pilot test is a small-scale study to test the questionnaire, to minimise the likelihood of respondents having problems in answering the questions and to allow some assessment of the questions' validity and the reliability of the data that will be collected (Saunders *et al.* 2007). According to Hussey and Hussey (1997) and Sekaran (2003), it is important to pre-test the questionnaire as fully as possible before distributing it, to ensure that

respondents understand the questions, there are no problems with the wording or sequence of questions, and to improve the reliability and validity of individual questions.

Piloting is also essential to ensure the suitability of the questionnaire for achieving the research aims and objectives, to demonstrate that the questionnaire is capable of generating the required responses from the target respondents and to ensure that the questionnaire as a whole functions well (Bryman and Bell 2003; Smith 2003). Moreover, piloting is essential to ensure that the sampling frame is adequate and to estimate the response rate of the study. Piloting, therefore, can discover possible weaknesses, inadequacies, ambiguities and problems in all aspects of the research so they can be corrected before actual data collection takes place (Sarantakos 2005).

Consequently, in order to check the suitability of the questionnaire to the current study, to enrich its quality and to generate the maximum response rate, several development steps were taken before the final distribution.

First, after an extensive review of the existing literature on AIS security, and after several modifications and changes, the first draft of the questionnaire was completed and was submitted to the supervisors.

Second, after several discussions with the supervisors and after being satisfied with the content, wording and format of questions, the questionnaire was circulated for comments to several academics in the accounting and finance section and to some fellow research students within Cardiff Business School. The comments received were found to be very useful. Consequently, several modifications were made to the wording and scaling of certain questions, some questions were omitted and others were included.

Third, in order to improve the quality of the questionnaire and to ensure the questions were relevant and could be understood by the respondents, the questionnaire was sent for piloting to the finance directors of 15 UK listed companies. These companies were selected randomly from the list of companies found in the London Stock Exchange website. A copy of the questionnaire together with a covering letter and a

self-addressed freepost return envelope was mailed to each director. Three responses were received; however, none of the questionnaires had been completed either because of company policy or time constraints or because of the confidential nature of the information required. Consequently, the length of the questionnaire was considered and it was reduced from 16 pages to 7 pages and was printed as a booklet with two staples in the spine in order to look more professional (Dillman 2000). In addition, after several discussions with the supervisors it was decided to change the target respondents of the questionnaire. A full discussion of the questionnaire sampling is presented in the next section.

Finally, after taking into consideration all the comments and suggestions, and after making all the necessary modifications, the final copy of the questionnaire was ready for administration.

3.6.1.3 Questionnaire sampling

After developing and pilot testing the questionnaire, the next step was to select those elements from which the data would be collected. One option is complete coverage of the population in which all units of the target population will be studied. Another option, and the most common, is sampling in which the target population is investigated by studying a small part of it, namely a sample (Sarantakos 2005).

There are many reasons for sampling. Sampling enables the researcher to study a relatively small part of the target population and obtain data that are representative of the whole. Sampling is also economical; it saves time and produces quick results. In addition, if properly selected, samples can provide a high degree of accuracy (Sarantakos 2005; Saunders *et al.* 2007; Zikmund 2000).

The first step in sampling is to identify and to define precisely the population to be sampled (Burns 2000). The target population of the current study were the large UK listed companies. The decision to target only larger companies was based on the premise that large companies with greater human, technological and financial resources were generally expected to be more sophisticated and more successful in using IS (Yang *et al.* 2005). Kankanhalli *et al.* (2003) argued that large companies invested more in information security than small companies did in terms of systems

software and human resources. This population was chosen because it covers a wide range of businesses in the UK and because large companies tend to expend the most effort on security, and have well developed IS security strategies.

A sampling frame of approximately 1295 UK listed companies was drawn up from the London Stock Exchange website and the researcher made every effort to ensure that this sampling frame was unbiased, current and accurate. The target respondents were the IT managers of the large UK listed companies whose titles differ among different companies. These titles are chief information officer (CIO), chief security officer (CSO), chief information security officer (CISO), IS managers/executives and IT executives. These managers were chosen because, as the persons in charge of IS, they should be familiar with all AIS security practices in their companies including their companies' security policies, security controls, etc. They are assumed to have sufficient knowledge and relevant information regarding the issues under examination, which is important for achieving a high degree of reliability of the data collected and strengthening the validity of the results obtained.

The next step in sampling is to decide on a suitable sample size. Bryman and Bell (2003) argued that the decisions about sample size represent a compromise between the constraints of time and cost, and the need for precision. In addition, Sarantakos (2005) and Saunders *et al.* (2007) have indicated that the choice of sample size depends on the underlying methodology, the nature and purpose of the study, the nature of the data required and the types of analysis the researcher is going to undertake. Moreover, it depends on the degree of confidence needed in the data obtained, the degree of accuracy required, and the response rate expected for the study.

Based on the above, and after taking into consideration the limited time and resources and the expected low response rate for such types of studies, the sample size comprised 800 companies, which represented about 60 percent of the total population. This sample size was limited by the time and resources constraints; however, it was felt to be reasonable enough to allow the researcher to conduct the required tests of the research questions.

Having chosen a suitable sampling frame and estimated the actual sample size required, the next step is to select the most appropriate sampling technique that ensures the sample is representative of the population and, as far as possible, not biased in any way (Burns 2000).

In the current study, the researcher decided to use stratified random sampling. It is a probability sampling procedure in which the target population is divided into a number of strata, and a sample is drawn randomly (simple or systematic) from each stratum. The resulting sub-samples make up the final sample of the study (Sarantakos 2005). The ultimate function of stratification is to organise the population into homogeneous subsets and to select the appropriate number of elements from each (Babbie 1998). Accordingly, the companies that represent the population of the current study were stratified by sectors, and the researcher organised a list of companies for each sector or stratum. The decision to stratify the companies by sectors derived from the research objective that emphasised the differences between the industry sectors regarding the types of security threats and controls, and the existence of a management framework for AIS security. Within each sector, a simple random sample was taken. The researcher decided sometimes to use the disproportional stratified sampling when the number of companies in certain sectors was too small or too large, in order to ensure an adequate number of companies in every sector.

The strength of this procedure is that it allows all population groups (sectors) to be adequately represented in the final sample (Frankfort-Nachmias and Nachmias 1992). It can give greater precision with the same sample size or, alternatively, the same precision with a smaller sample. It reduces the probable sampling error. It can give separate results for each stratum (sector), and it simplifies data collection (Babbie 1998; Ghauri and Gronhaug 2002). However, complete, accurate, and updated stratum information is needed.

3.6.1.4 Administration of the questionnaire

Once the questionnaire was designed, pilot tested and the sample was selected, the questionnaire was ready for administration. The final version of the questionnaire was sent by mail to the IT managers of each of the 800 UK listed companies selected. The

addresses were obtained from the FAME Database and were confirmed through the website of each company, whenever available.

As mentioned in Section 3.6.1, the most serious problem with the postal questionnaire is the poor response rate particularly when dealing with a very sensitive and intrusive issue such as security. Consequently, in an attempt to deal with this problem and to improve the response rate, the following techniques were employed:

- First, the questionnaire was accompanied by a covering letter, introducing the researcher's status as a PhD student at Cardiff Business School, explaining the primary purpose and importance of the study, how the respondents were chosen to participate, assuring the anonymity of respondents and the confidentiality of information and finally thanking the respondents in advance for their participation.

- Second, the covering letter was addressed to the IT manager of each company; it was printed on the Cardiff Business School letterhead and was signed by the researcher.

- Third, the questionnaire was printed as a booklet with two staples in the spine that gave it a professional look.

- Fourth, the respondents were offered the opportunity to receive a copy of the study results.

- Fifth, a self-addressed freepost return envelope was provided with each copy of the questionnaire.

- Sixth, three weeks after sending the first mail, reminder letters were posted to those who had not responded (750 companies).

The number of questionnaires received in total was 65 resulting in a response rate of 8.1 percent.

3.6.1.5 Reliability and validity

In developing the questionnaire, the researcher paid special attention to two technical considerations: reliability and validity. According to Hunter and Brewer (2003) and Neuman (2000), both qualities are most central to the assessment of the goodness of a measurement and are important in establishing the truthfulness, credibility, or believability of findings. They are complementary concepts and are closely interrelated; however, in some situations they can conflict with each other. In addition, one cannot predict the other i.e. reliability is necessary for validity; however, it does not guarantee that a measure will be valid (Neuman 2000; Sarantakos 2005). Both terms have multiple meanings.

Reliability is "the degree to which measures are free from error and therefore yield consistent results" (Zikmund 2000, p.280). It applies to a measure when similar results are obtained over time and across situations. Reliability refers to the consistency of a measure. There are two main aspects of this consistency: stability (or external reliability) and internal consistency (or internal reliability) (Bryman 1989; Punch 1998).

External reliability refers to "the degree to which a measure is consistent and stable over time" (Bryman 1989, p.55). It is usually expressed in the question: does the measure deliver the same answer when applied in different times? (Neuman 2000). Internal reliability refers to the degree of internal consistency of a measure or whether indicators that make up the scale are consistent with each other (Bryman and Bell 2003), and all are working in the same direction (Punch 1998). It can be expressed in the question: does the measure yield consistent results across different indicators? (Neuman 2000).

There are four common ways of testing reliability: test-retest method; alternate (or parallel) form method; split-half method; and Cronbach's coefficient alpha (Burns 2000; Frankfort-Nachmias and Nachmias 1992; Punch 1998; Zikmund 2000).

The test-retest method involves administering the same measuring instrument to the same respondents at two separate times to test for stability and the correlation between the two sets of responses is computed. The obtained coefficient is the

reliability estimate. The high stability correlation indicates a high degree of reliability. However, this method has some limitations. It is difficult to persuade respondents to answer the same questionnaire twice, and if they do, they may think more deeply about the questions on the second occasion and give different answers, or may remember specific questions and answer the same way as on the first occasion, thus yielding a high but overstated reliability estimate. In addition, it is possible that change will occur in the measured variable during the measuring interval, thus lowering the estimate of reliability (De Vaus 2002; Frankfort-Nachmias and Nachmias 1992; Hussey and Hussey 1997; Saunders *et al.* 2007).

In the alternate (or parallel) form method, two alternative instruments are designed to be as equivalent as possible. Each of the two measuring instruments are then administered to a group of persons, and the two sets of measures (scores) are correlated to obtain an estimate of reliability. If there is high correlation between the two instruments, the researcher concludes that the measure is reliable. However, with this technique there is a problem of determining whether the two forms of an instrument are in fact parallel, in addition to the further time and effort involved in the construction of another form (Burns 2000; Frankfort-Nachmias and Nachmias 1992; Zikmund 2000).

In the split-half method, the questionnaire is divided into two equal halves or two equal sets of questions and each of the two sets is treated separately and scored accordingly. The two sets are then correlated and the correlation coefficient of the two sets is taken as an estimate of reliability. However, with this technique different types of items with different difficulty levels may occur in each half (Burns 2000; Frankfort-Nachmias and Nachmias 1992).

The most frequently used method for measuring the internal reliability or internal consistency among the academic researchers is Cronbach's coefficient alpha. This is used to assess the reliability of a measurement scale with multi-point items. It calculates the average of all possible split-half reliability coefficients (Bryman and Bell 2003). The value of this coefficient varies between 1 (denoting perfect internal reliability) and 0 (denoting no internal reliability); however, Bryman (1989) argued

that most researchers regard 0.80 as an acceptable level of internal reliability for any multiple-point scale.

Based on the above discussion and due to the limitations recognised in the first three methods, Cronbach's coefficient alpha was used in the current study to assess the reliability of the questionnaire. The scales attained a Cronbach's coefficient alpha of 0.667 to 0.766, which indicates a reasonable degree of consistency of the scales used.

As mentioned earlier, reliability is a necessary condition for validity, but a reliable instrument may not be valid. Thus, even though the responses to questions may turn out to be highly reliable, the results will be worthless if the questions do not measure what the researcher intended them to measure i.e. validity is low. Therefore, after testing the reliability of the questionnaire, the validity of the research findings must be well considered by the researcher.

Validity is concerned with the question "Is one measuring what one intends to measure?" (Frankfort-Nachmias and Nachmias 1992, p.158). Validity is a measure of precision, accuracy and relevance; it reflects the quality of indicators and instruments; and it refers to the ability to produce findings that are in agreement with theoretical or conceptual values (Sarantakos 2005). The researcher must provide supporting evidence that a measuring instrument in fact measures what it appears to measure. Among the various approaches to the validation of instrument, three of the main ones are: (1) content validity; (2) criterion-related validity; and (3) construct validity (De Vaus 2002; Neuman 2000; Punch 1998; Saunders *et al.* 2007; Zikmund 2000).

(1) Content validity refers to the extent to which the measurement device (questions in the questionnaire) provides adequate coverage of the investigative questions (Saunders *et al.* 2007, p.366).

(2) Criterion-related validity is an attempt by the researcher to answer the question "Does my measure correlate with other measures of the same construct?" (Zikmund 2000, p.282); therefore, an indicator is compared with another measure of the same construct in which the researcher has confidence. There are two types of criterion-related validity: concurrent validity, where the criterion variable exists in the present

and predictive validity, where the criterion variable will not exist until later (Punch 1998, p.101).

(3) Construct validity refers to the extent to which the measurement questions actually measure the presence of those constructs the researcher intended them to measure (Saunders *et al.* 2007, p.367). It involves relating a measuring instrument (questionnaire) to a general theoretical framework in order to determine whether the instrument is tied to the concepts and theoretical assumptions that are employed (Frankfort-Nachmias and Nachmias 1992, p.161).

According to Frankfort-Nachmias and Nachmias (1992) and Punch (1998), each of these three kinds of validity is concerned with a different aspect of the measurement situation, and each includes several kinds of evidence and has special value under certain conditions. In fact, there is no ideal way to establish validity and the validation methods used should depend on the situation.

Given the importance of the validity of the research findings, two approaches were followed in the current study in order to enhance validity. First, the questionnaire was subject to many modifications and amendments and had passed through several steps before its final distribution in order to enrich its quality and to improve the validity of individual questions (Section 3.6.1.2). Second, the current study employed a postal questionnaire and semi-structured interviews. As mentioned in Section 3.3.3, the findings from one method can be checked against the findings derived from the other method. Consistent findings among different data collection methods increase the credibility of findings, improve the trustworthiness of research, and thus maximise its validity.

3.6.1.6 Statistical tests used

Once the questionnaires were received, the data analysis started. The researcher followed a systematic process that began with preparing the data for computer entry, that is, by checking, editing and coding the data, followed by entering the data in the computer, and then by data processing and analysis. In analysing the data, the statistical package for social sciences (SPSS) version 12 was used. It is one of the most popular statistical packages, can perform highly complex data manipulation and

analysis with simple instructions, has a vast number of statistical and mathematical functions and a very flexible data handling capability, and it can read data in almost any format (Punch 1998).

However, before the analysis began, the type of data collected was well considered by the researcher. In general, data can be measured on four different scales: (1) nominal; (2) ordinal; (3) interval; and (4) ratio. Nominal data imply no more than a labelling of different categories for which there is no meaningful ordering or ranking (Bowerman and O'Connell 2007; Easterby-Smith *et al.* 1991). Ordinal data can be ordered or ranked but the distance between the categories is unknown. Interval data can not only be ordered or ranked but the distance between the categories is precisely defined as well; however, there is no inherently defined zero value i.e. the zero point is arbitrary. Finally, ratio data have all the characteristics of interval data, and in addition, they have a meaningful zero point (Bowerman and O'Connell 2007; Fielding and Gilbert 2000; Siegel and Castellan 1988). Saunders *et al.* (2007) argued that these different types of data dictate the range of the techniques available to the researcher for presentation, summary and analysis of the data collected.

In general, two main statistical techniques have been used in the current study, namely, descriptive statistics and inferential statistics. Descriptive statistics is the first step in the analysis of data. It entails the researcher in summarising and organising data in an effective and meaningful way. It keeps the researcher close to the data, at least in the initial stages of the analysis, and helps the researcher in understanding the distribution of each variable across the survey respondents (Frankfort-Nachmias and Nachmias 1992; Punch 1998). Accordingly, the frequency distribution table and cross-tabulation were used in the current study as the first step in the data analysis. These methods are discussed in details in Chapter 4.

As the analysis progressed beyond the descriptive stage, the researcher applied the tools of inferential statistics. The function of inferential statistics is to provide an idea about whether the patterns described in the sample are likely to apply in the population from which the sample is drawn (De Vaus 2002). It involves using data collected from a sample to draw conclusions about a complete population (Hussey and Hussey 1997). In general, there are two major groups of statistical tests:

parametric and nonparametric tests. The major distinction between these two groups lies in their power and the underlying assumptions about the data to be analysed (Burns 2000; Zikmund 2000).

In using parametric tests, a number of assumptions about the actual data need to be satisfied: first, the observations must be independent; second, the observations must be drawn from a normally distributed population (bell-shaped distribution); third, the populations must have the same variance. Finally, the variables must have been measured in at least an interval scale, so that it is possible to interpret the results (Siegel and Castellan 1988).

In contrast, a nonparametric test is based on a model that specifies only very general conditions; it neither specifies the normality condition nor requires an interval level of measurement. Certain assumptions are associated with most nonparametric tests for example the observations are independent and the variable under study has underlying continuity; however, these assumptions are weaker and fewer than those associated with the parametric tests (Frankfort-Nachmias and Nachmias 1992; Siegel and Castellan 1988).

Nonparametric tests have many advantages. They do not make numerous or stringent assumptions about the population from which the sample was drawn. The error caused by assuming a population is normally distributed, and when it is not, it is avoided. Thus, they are considered as distribution-free tests. Some nonparametric tests are appropriate for data measured in an ordinal scale, and others for data measured in a nominal scale. They often test different hypotheses rather than parametric tests. If the sample is small, there may be no alternative to using a nonparametric test unless the nature of the population distribution is known exactly. In addition, nonparametric tests are much easier to apply and their interpretation is often more direct than the interpretation of parametric tests (Siegel and Castellan 1988; Zikmund 2000).

In general, parametric tests are more powerful than nonparametric tests when all the assumptions are met. The meaningfulness of their results depends on the validity of these assumptions. If there is any doubt about the quality of data or the underlying

assumptions, then parametric tests may be unreliable and nonparametric tests should be adopted (Siegel and Castellan 1988; Smith 2003).

Based on the above discussion, and according to the hypotheses of the current study (Section 3.2.4) and the type of data collected (nominal and ordinal), nonparametric tests were employed. In particular, the Kruskal-Wallis One-Way Analysis of Variance, Chi-Square Test of Independence, and Spearman's Rank Correlation were used in the current study to analyse the data of the questionnaire. In addition to these non-parametric tests, multiple regression analysis and particularly stepwise regression were used to investigate the effect of AIS security controls on the different types of AIS security threats facing UK companies. A full discussion of these tests and the questionnaire findings is presented in Chapter 4.

3.6.2 Semi-structured interviews

In order to overcome the problems associated with the use of questionnaires (Section 3.5.1), semi-structured interviews were conducted in the current study as the second stage of data collection. The semi-structured interviews were chosen to triangulate data collected by questionnaires to derive the benefits of both quantitative and qualitative methods; to get a more detailed perspective on some of the issues raised; and to supplement, confirm, validate, explain, illuminate or reinterpret quantitative data gathered from questionnaires (Blaxter *et al.* 2001; Miles and Huberman 1994; Smith 2003).

The semi-structured interviews permit greater flexibility; however, the interviewer remains in control throughout the whole process (Burns 2000; Robson 1993). They allow interviewees to answer on their own terms but still provide a greater structure for comparability over that of the unstructured interviews (May 1997). They permit the interviewer to ask more complex questions. The interviewer is more free to probe beyond the answers that add significance and depth to the data collected. They can take account of non-verbal communications (Hussey and Hussey 1997; Saunders *et al.* 2007). They are also appropriate when the subject matter is highly confidential or commercially sensitive (Easterby-Smith *et al.* 1991) such as security practices in UK companies, which are defined as very intrusive, confidential and sensitive issues. However, semi-structured interviews are more time-consuming and expensive than

questionnaires, in terms of travel expenses, the time required to conduct the interviews, and to analyse the collected data. The flexibility of interviews leaves room for the interviewer's personal influence and bias, and interviews offer less anonymity than questionnaires (Frankfort-Nachmias and Nachmias 1992; Sarantakos 2005). However, every effort was made by the researcher to overcome these limitations and to maximise the benefits of using semi-structured interviews.

3.6.2.1 Interviews sampling

The sample of the interviews in the current study comprised a sample from large UK listed companies, namely, the IT managers of these companies.

At the end of the questionnaire, the respondents were asked to provide their contact details (title, name, address, telephone number and e-mail address), if they were willing to be contacted to arrange a follow-up face-to-face interview concerning their opinions on some AIS security issues within their companies.

The managers who agreed to participate and supplied their details were then contacted to arrange an appointment for the interview. In total 12 managers agreed to be interviewed and supplied their contact details in the returned questionnaire. An email was sent to these managers thanking them for completing the questionnaire and for their willingness to be interviewed and asking their permission to contact them again to arrange an appointment after analysing the questionnaire data. One month later, another e-mail was sent to these managers reminding them of the study and arranging an appointment for the interview. Some of them expected a telephone interview, but another email was sent to them clarifying the benefits of the face-to-face interviews for the current study. Most of the IT managers agreed and appointments were arranged to conduct the interviews. In total nine interviews were conducted with the IT managers of the UK listed companies in different industry sectors.

3.6.2.2 Administration of the interviews

Before conducting the interviews, an interview guide was sent to those who agreed to participate, along with a letter reminding them of the identity of the researcher, the

main objectives of the study, assuring their anonymity and confidentiality of information and thanking them in advance for their participation.

An interview guide is a list of issues to be addressed or questions to be asked in the semi-structured interview (Bryman and Bell 2003). According to Saunders *et al.* (2007), providing participants with a list of themes or questions before the interview should promote validity and reliability by enabling the interviewees to consider the information being requested and allowing them the opportunity to assemble supporting organisational documentation from their files. The interview guide of the current study evolved from the analysis of the questionnaire responses and the questions were divided into six sections as follows:

Section 1: Introductory discussion

The aim of this section was to introduce the researcher, to explain the aims of the research, to assure the anonymity of interviewees and the confidentiality of information and to thank the interviewees in advance for their participation.

Section 2: General and background information

This section aimed to ask general questions about the interviewees and their companies' background in order to obtain a profile of those who participated in the study.

Section 3: The management framework of the AIS security

This section aimed to collect the interviewees' opinions regarding the management framework of the AIS security within their companies, including security policy, training and awareness programs, risk assessment, incident handling, disaster recovery and a business continuity plans, security budget, security standards and certification and AIS security effectiveness.

Section 4: Security threats to the companies' AIS

This section aimed to investigate the most common types and frequency of occurrence of the AIS security threats facing the companies and the sources of those threats.

Section 5: Security controls of the companies' AIS

This section aimed to investigate the most recent AIS security controls implemented within UK companies, the gaps between security threats and the scope of controls employed, the new security controls they are planning to use, and the companies' security level.

Section 6: Uncovered issues

This section focused on adding any other issues the interviewees viewed as important for the current study which had been overlooked by the researcher, and finally, thanking the interviewees for their time and cooperation.

The interview guide used during the interviews with the covering letter is provided in Appendix 2.

After receiving the permission of the interviewees, all the interviews were audio-recorded. The audio recording is important for the detailed analysis required in qualitative research and to ensure that the interviewees' answers are captured in their own terms. It enables the interviewer to concentrate on the phrasing and order of questions rather than on note taking. It allows questions formulated at an interview to be accurately recorded for use in later interviews where appropriate. It provides an accurate and unbiased record and allows quotes to be used (Bryman and Bell 2003; Healey and Rawlinson 1994; Saunders *et al.* 2007).

However, audio recording might bias the interviewees' answers because they know that their anonymity is not preserved in full. It makes interviewees anxious and less likely to reveal confidential information. Transcribing and analysing the interviews can take a considerable time. In addition, there is a risk that during audio recording the interviewer might cease to listen carefully, believing that all the information is going onto the tape which will be listened to later in a more relaxed environment (Blaxter *et al.* 2001; Sekaran 2003). Therefore, many authors for example Burns (2000), Ghauri and Gronhaug (2002) and Saunders *et al.* (2007) recommended note taking as the interview progresses in order to supplement the audio recording and to overcome its limitations. Based on their suggestion, the researcher took some notes in

addition to audio recording the interviews in order to record non-verbal actions and to maintain concentration and focus.

3.6.2.3 Analysis of interview data

The analysis of the interview data is one of the most serious and central difficulties facing researchers. According to Robson (1993, p.370), "there is no clear and accepted set of conventions for analysis corresponding to those observed with quantitative data". However, in order to increase the transparency of research, the methods of data analysis need to be systematic, disciplined and able to be seen and described (Punch 1998). Accordingly, the analysis of the interview data in the current study was based on Miles and Huberman's approach for qualitative data analysis. Miles and Huberman (1994, pp.10-11) suggest the following main components for qualitative data analysis: data reduction, data display, and drawing and verifying conclusions. A full discussion of this approach is presented in Chapter 5.

Despite the small number of interviews conducted, and the lack of wide agreement among researchers regarding the use of computers in qualitative data analysis, the researcher used NVivo, which is one of the best known computer-assisted qualitative data analysis software, to support Miles and Huberman's (1994) approach in analysing the interview data. A full discussion of the advantages and limitations of NVivo, the interviewees' responses and the data analysis is presented in Chapter 5.

3.7 Research ethics

A number of ethical issues arose across the different stages and duration of the research that were carefully considered by the researcher. A copy of the research proposal, questionnaire and the interview guide with the covering letters were submitted to the Research Ethics Committee at Cardiff Business School. After permission was obtained to conduct the research, the researcher began to contact participants and to gain access.

According to Bryman and Bell (2003), participants should be given as much information as might be needed to make an informed decision about whether or not they wish to participate in the study. Consequently, the questionnaire was

accompanied by a covering letter introducing the researcher's status as a PhD student in Cardiff Business School, explaining the importance and objective of the study, how the respondents were chosen to participate, assuring the anonymity of respondents and the confidentiality of data and thanking them in advance for completing the questionnaire.

After receiving the responses, an e-mail was sent to the managers who agreed to be interviewed and supplied their contact details in the questionnaire, thanking them for completing the questionnaire and for their willingness to take part in a follow up interview and seeking their permission to contact them again for arranging an appointment after analysing the questionnaire's responses.

After analysing the responses of the questionnaire, another e-mail was sent to inform the participants about the expected duration of the interview and to arrange a convenient time for each participant. An interview guide was then mailed to participants, accompanied by a covering letter, reminding them of the researcher's status, explaining the objective of the study, assuring their anonymity, th e confidentiality of data and their right to decline to answer a question or set of questions.

According to Neuman (2000), participants should explicitly agree to participate. At the beginning of the interview, the participants signed two consent forms concerning the confidentiality and anonymity of data, and their right to withdraw from the interview at any time. However, De Vaus (2002) indicated that there are some problems with asking participants to sign consent forms; not only does it formalise the interview and lead to a loss of rapport, it can also make some participants more suspicious about the research. Despite De Vaus's opinion and despite the sensitive nature of the study, the researcher did not perceive any problem in asking participants to sign these forms. A copy of these forms is provided in Appendix 3. In addition, the researcher received the participants' permission to audio-record the interviews.

During the interview, the researcher avoided pressing the participants for a response. According to Cooper and Schindler (2006), the researcher should make clear to participants that they have the right to decline to respond to any question. In addition,

Saunders *et al.* (2007) indicated that it would be unethical to attempt to prolong the duration of an interview beyond that previously agreed unless the participant freely proposes this as an option. All the interviews conducted were, therefore, within the duration agreed upon, unless the participants were willing to complete the discussion. Furthermore, the researcher tried to collect the data accurately in this stage to fully maintain the validity and reliability of the research.

Saunders *et al.* (2007) and Zikmund (2000) indicated that the objectivity of the researcher is vital during the analysis stage. Lack of objectivity will clearly distort the conclusions. The researcher, therefore, avoided being selective in which data to report, and the data were analysed honestly.

During the reporting stage, the researcher maintained the anonymity of participants. In addition, De Vaus (2002) indicated that when reporting the study findings sufficient information should be provided so that the results will not be misleading. The researcher provided readers with all the details about data collection, sampling and the ways in which data were prepared for analysis, and finally represented the statistical significance of the data accurately and honestly.

It is most important, according to Bryman and Bell (2003), that the researcher take all reasonable precautions to ensure that participants are in no way directly harmed or adversely affected as a result of their participation in the study.

3.8 Summary of the chapter

This chapter has mainly been concerned with the methodology used in the current study. The chapter began by presenting the conceptual framework of the research, explaining the main variables of the current study, linking each variable to the literature and demonstrating the relationships between them. It proceeded with a general discussion on the research paradigms, emphasised the use of both positivistic and phenomenological paradigms, the main strengths and weaknesses of quantitative and qualitative approaches in research and explained the adoption of both approaches in the current study. The common types of triangulation were presented together with the reasons of employing data and methodological triangulation in the current study.

The chapter then discussed the research design, explaining the descriptive and explanatory nature of the current study and the main reasons for adopting the deductive approach and the cross-sectional design in the study.

The three methods recommended in the literature on IS security namely questionnaires, interviews and case studies, were then presented and the strengths and weaknesses of each method identified and considered. The chapter then provided the justification for the use of questionnaires and semi-structured interviews as the data collection methods of the current study. A detailed description of the questionnaire was provided, including questionnaire design and layout, and the major considerations involved in formulating the questions. How the questionnaire was piloted, the sampling frame, the sample size, the sampling technique and how the questionnaire was administered were then presented. Reliability and validity of the questionnaire were explained together with the reasons of using Cronbach's coefficient alpha to assess the reliability of the scales and the approaches followed to enhance its validity. The process used by the researcher to analyse the data was provided.

The chapter continued with a description of the semi-structured interviews, interviewees' selection, the procedures followed to contact the interviewees and to arrange appointments, how the interview guide was organised, how the interviews were conducted, and how the data were analysed. Finally, the chapter emphasised the ethical issues that arose across the different stages and duration of the research.

The following two chapters present and discuss the main findings of both questionnaire and the semi-structured interviews. Chapter 4 presents a full discussion of the statistical methods used to analyse data of the questionnaire, reasons of selecting these methods and the main findings of the questionnaire. Chapter 5 presents a full discussion of the interviewees' responses and the methods used to analyse the interview data.

Chapter 4

Analysis of questionnaire results

4.1 Introduction

Chapter 3 was concerned with the methodology used in the current study. It provided the justification of using questionnaire and semi-structured interviews as the data collection methods of the current study. This chapter provides a full discussion of the statistical methods employed to analyse the data from the questionnaire and the reasons for selecting these methods. It also sets out the opinions of the IT managers of the UK listed companies on the AIS security in their companies and the main findings of the questionnaire.

This chapter is organised as follows. Section 4.2 presents the sample size and response rate. Section 4.3 discusses the statistical methods employed in the current study to analyse data of the questionnaire. Section 4.4 focuses on the respondents and their companies' background. Section 4.5 analyses the questions of Section 1 of the questionnaire concerning the management framework of AIS security within UK companies. This is followed by Section 4.6 which presents the results on the most common sources and types of AIS security threats facing UK companies and the frequency of occurrence of each type of threat. Section 4.7 investigates the AIS security controls employed by UK companies to reduce security threats. Finally, Section 4.8 concludes the chapter with a summary of the questionnaire's findings.

4.2 Sample size and response rate

It was mentioned in Chapter 3 that the final version of the questionnaire was sent by post to the IT managers of 800 randomly selected UK listed companies. A total of 104 responses were received, of which 30 completed questionnaires were returned after posting reminder letters to those who had not responded. However, 39 incomplete responses were received which were unusable for statistical analysis. Different reasons were provided for not completing the questionnaire. Some respondents mentioned that it was against their companies' policy to complete or to participate in any research studies or surveys. Others refused to participate for confidentiality reasons. Some explicitly stated that the information requested was either security

sensitive or commercially sensitive, not only for them, but for their customers as well, and although they were provided with confidentiality assurances by the researcher, they did not want to take the risk that the information could become visible to a wider audience. The others believed that it was inappropriate to complete the questionnaire as third parties currently outsource the IT functions in their companies. Consequently, 65 questionnaires were usable for statistical analysis purposes, resulting in a usable response rate of 8.1 percent (Table 4.1).

Table 4.1 Responses to the questionnaire

Responses	Initial mail		Follow-up		Total	
	no	%	no	%	no	%
Usable responses	35	58.3	30	68.2	65	62.5
Unusable responses						
Blank questionnaire	15	25	9	20.4	24	23.1
E-mail	10	16.7	5	11.4	15	14.4
Total	60	100	44	100	104	100

Out of the 800 questionnaires mailed to the IT managers, 696 managers, did not respond at all. As was mentioned in Chapter 3 (Section 3.5.1), one of the major problems associated with a questionnaire is the low response rate, particularly with the postal questionnaire. According to Collis and Hussey (2003), this low response rate introduces the problem of non-response bias that is the data collected may be biased and thus may not be representative of the population. In addition, De Vaus (1996) argued that those who did respond might be significantly different from those who did not, and consequently, the results were biased in some way. However, Oppenheim (1966, p.34) stated, "Respondents who send in their questionnaire very late are roughly similar to non-respondents". Consequently, in order to examine whether non-response bias was a major problem for the results of the questionnaire in the current study, statistical tests were conducted to compare early respondents with late respondents in terms of their answers to the questionnaire. The results of the responses from the initial mailing (35 responses) were compared with the results of the responses from the follow-up mailing (30 responses) using the Kruskal-Wallis test. The results revealed that no significant differences were found between the early and late responses. The two groups did not differ significantly in their opinions regarding the common sources and types of AIS security threats in UK companies.

Consequently, non-response bias does not appear to be a major problem in the current study.

4.3 Statistical methods used

As was mentioned in Chapter 3 (Section 3.6.1.6), in analysing the questionnaire data, two main statistical techniques were used in the current study, namely, descriptive statistics (exploratory data analysis) and inferential statistics (confirmatory data analysis). Descriptive statistics is the first step in data analysis. This refers to the transformation of the raw data into a form that will make them easy to understand and interpret (Zikmund 2000). The calculation of averages, frequency distributions, and percentage distributions is the most common form of summarising data. Accordingly, the frequency distribution table and cross-tabulation were used in the current study as the first step in the data analysis. These methods are discussed in detail in Sections 4.3.1 and 4.3.2 respectively.

As the analysis progressed beyond the descriptive stage, the researcher applied the tools of inferential statistics. Inferential statistics give an idea of whether the patterns described in the sample are likely to apply in the population from which the sample is drawn (De Vaus 2002). This involves using data collected from a sample to draw conclusions about a complete population (Hussey and Hussey 1997).

In general, there are two major groups of statistical tests: parametric and non-parametric tests. As was mentioned in Chapter 3 (Section 3.6.1.6), non-parametric tests were mainly employed in the current study for many reasons. First, the sample size in the current study is small (65 usable responses). According to Siegel and Castellan (1988, p.35), if the sample size is small, there may be no alternative to using a non-parametric statistical test. Second, the data collected are nominal and ordinal. Pallant (2007) indicated that non-parametric techniques are ideal for use when data are measured on nominal (categorical) and ordinal (ranked) scales. Moreover, Anderson *et al.* (2007, p.720) stated that with nominal or ordinal data, it is inappropriate to compute means, variances, and standard deviations, and therefore, parametric methods cannot be used.

Third, non-parametric techniques require no assumptions about the shapes of the sampled populations. They, therefore, can be more efficient than parametric tests when the underlying populations are not normally distributed (Bowerman and O'Connell 2007; Hollander and Wolfe 1999). Fourth, non-parametric methods often test different hypotheses about the population than do parametric procedures (Siegel and Castellan 1988, p.34). Fifth, the sample in the current study was made up of observations from seven industry sectors. According to Siegel and Castellan (1988), there are suitable non-parametric statistical tests for treating samples made up of observations from several different populations. Finally, non-parametric tests are often easier to apply and quite easy to understand.

Based on the above, the Kruskal-Wallis One-Way Analysis of Variance, Chi-Square Test of Independence, and Spearman's Rank Correlation were used in the current study to analyse the data of the questionnaire. These tests are discussed in Sections 4.3.3, 4.3.4, and 4.3.5 below. In addition to these non-parametric tests, multiple regression analysis, in particular stepwise regression, was used in the current study to investigate the effect of AIS security controls used in UK companies on the different types of AIS security threats facing the companies.

According to Allison (1999), in practice, ordinal variables are often used in regression analysis. Moreover, Sprent (1989) indicated that by using the techniques of dummy variables, the researcher could include qualitative factors in the multiple regression analysis. In addition, Labovitz (1970) has suggested that almost all ordinal variables can and should be treated as interval variables. He argues that the amount of error that can happen is minimal, especially in relation to the considerable advantages to the researcher as a result of using techniques of analysis like regression analysis which is powerful and relatively easy to interpret. Multiple regression analysis, particularly stepwise multiple regression, is discussed in detail in Section 4.3.6 below.

4.3.1 Frequency distribution

The starting point in descriptive analysis is the construction of a frequency distribution for each variable of interest. The idea of the frequency distribution is to tell the researcher the number of cases in each category. The tabular form of representing frequency distributions can be used with any variable irrespective of its

level of measurement (Diamantopoulos and Schlegelmilch 1997, p.74). In addition, De Vaus (2002) stated that the frequency table provides a first look at some of the characteristics of the sample and the sorts of responses that have been given. The researcher can get an idea of the shape of the distributions on key variables and can investigate which variables have very little variation and which categories have almost no cases. Sekaran (2003) indicated that the frequency distribution could be obtained for all the personal data or classification variables.

Based on the above, frequency distribution tables were constructed for the responses concerning the general and background information (Section 4 of the questionnaire) in order to obtain a profile of the respondents and their companies. Consequently, a frequency distribution table was constructed for the respondents' job title, number of years of experience in their current job, their most recent educational qualification, their academic field of study, and security qualifications. In addition, a frequency distribution table was constructed for the companies' industry sector, age, and number of employees. These frequency distributions are discussed in more detail in Section 4.4.

4.3.2 Cross-tabulation

A cross-tabulation is a tabular summary of data for two variables. It is widely used for examining the relationship between two variables (Anderson *et al.* 2007) and for allowing the inspection of differences among groups (Zikmund 2000). It can be constructed using one qualitative variable and one quantitative variable, when both variables are qualitative, or when both variables are quantitative. The primary advantage of the cross-tabulation is its simplicity and understandability.

However, analysing either a few variables with many categories or many variables leads to a large number of cells. Consequently, the tables become difficult both to display and to interpret. Small cell sizes reduce the reliability of the estimated behaviour for a given characteristic and make comparison among cells difficult and risky. In addition, while cross-tabulation and related statistical tests may be used to analyse the degree of association between variables, they do not provide information about the magnitude of any effect or the strength of any relationship (Hanushek and Jackson 1977).

Consequently, in order to investigate the differences among UK companies in different industry sectors concerning the management framework of AIS security, types of AIS security threats facing the companies, and security controls used, cross-tabulations were constructed for variables in Sections 1, 2 and 3 of the questionnaire and the industry sectors of the companies that responded. The cross-tabulations of these variables are discussed in Sections 4.5, 4.6, and 4.7.

4.3.3 Kruskal-Wallis one-way analysis of variance

The Kruskal-Wallis test is the non-parametric equivalent of the one-way ANOVA, and is a generalisation of the Mann-Whitney test; however, it is used when there are more than two groups in the analysis (Dancey and Reidy 2004). The Kruskal-Wallis test can be used with ordinal data and it is not based on any assumptions about population shape. It is based on the assumption that the groups are independent and that individual items are selected randomly (Black 1994, p.764). The Kruskal-Wallis test is an extremely useful test for deciding whether K independent samples are from different populations.

In the computation of the Kruskal-Wallis test, each of the observations is replaced by ranks. That is, all the scores from all of the K samples are combined and ranked in a single series. The smallest score is replaced by rank 1 and the largest score is replaced by rank N, where N is the total number of independent observations in the K samples. The sum of the ranks in each sample is then found. From these sums, the mean rank for each sample or group is computed. If the samples are from identical populations, the mean ranks will tend to be similar, while if the samples are from different populations, then the mean ranks should differ (Siegel and Castellan 1988).

The hypotheses for the Kruskal-Wallis test with $K \geq 3$ populations can be written as follows:

Ho: All K populations are identical

H1: Not all K populations are identical

The Kruskal-Wallis statistic can be computed as follows (Siegel and Castellan 1988):

$$KW = \quad 12 / N (N + 1) \sum_{j=1}^{K} nj (\overline{R} j - \overline{R})^2$$

Where: K = number of samples or groups

n_j = number of cases in the j_{th} sample

N = number of cases in the combined sample

Rj = sum of the ranks in the j_{th} sample or group

$\overline{R}$ j = average of the ranks in the j_{th} sample or group

$\overline{R}$ = (N + 1) / 2 = the average of the ranks in the combined sample

When the obtained value of KW is significant i.e. if p-value < 0.05, it indicates that there is a statistically significant difference in the variable across the groups. However, it does not tell the researcher which ones are different nor does it tell the researcher how many of the groups are different from each other. According to Bowerman and O'Connell (2007), for this test to be valid, there should be five or more observations in each sample.

Based on the above, the Kruskal-Wallis test was used in the current study to test whether there are significant differences between the industry sectors in the UK concerning the most common sources and types of AIS security threats. In addition, it was used to test whether there are significant differences between the industry sectors regarding security training and awareness programs, risk assessment practices, top areas of spending on AIS security, awareness level of the British Standard BS 7799, and the common success indicators of AIS security management within UK companies. The analysis of the above variables using the Kruskal-Wallis test is discussed in Sections 4.5 and 4.6.

4.3.4 The Chi-Square test of independence

The chi-square test of independence is used to explore the relationship between two categorical variables. Each of these variables can have two or more categories (Pallant 2007, p.214). It is used when more than two groups need to be compared on a nominal variable (Diamantopoulos and Schlegelmilch 1997). The chi-square test is based on a contingency table (cross-tabulation) with cases classified according to the categories in each variable. This test compares the observed frequencies or proportions of cases that occur in each of the categories with the values that would be expected if there

were no association between the two variables being measured. The chi-square test statistic can be computed as follows:

$$\chi^2 = \sum (O - E)^2 / E$$

Where: O = observed frequencies

E = expected frequencies

If the observed frequencies equal the expected frequencies (no deviation), then the chi-square is zero which indicates that there is no association between the two variables. As observed frequencies begin to deviate from their expected frequencies, the chi-square begins to increase. The larger the deviation the larger the chi-square gets which indicates that there is an association between the two variables. The hypotheses for the chi-square test of independence can be written as follows:

Ho: The two variables are independent

H1: The two variables are dependent

If the value of the chi-square statistic χ^2 is large, this indicates that the observed cell frequencies differ substantially from the expected cell frequencies. The null hypothesis (*Ho*) is rejected where χ^2 exceeds a critical value for a given level of significance (if p-value < 0.05), and for a given number of degrees of freedom f. It can be concluded, therefore, that the two variables are dependent. The number of degrees of freedom can be computed as follows:

$$f = (r - 1)(c - 1)$$

Where: r = the number of rows in the cross-tabulation

c = the number of columns in the cross-tabulation

However, the chi-square test only tells us that the association between variables is likely to exist, but it does not tell us anything about the strength of the association or the relationship (Bryman and Cramer 2001). In addition, Siegel and Castellan (1988, p.199) indicated that the proper application of the chi-square test requires that the expected frequencies in each cell are not small. The chi-square should not be used when any expected frequency is smaller than one or when more than 20 percent of the

expected frequencies are smaller than five. However, if these requirements are not met by the data in the form in which they were originally collected and a large sample cannot be obtained, the researcher should combine categories, whenever possible and whenever to do so makes sense. Consequently, fewer than 20 percent of the cells have expected frequencies of less than five and no cell has an expected frequency of less than one.

Based on the above, the chi-square test of independence was used in the current study to test the association between the industry sectors and the nominal (categorical) variables in the data collected. For example, the existence of security policy, training and awareness programs, risk assessment programs, security budget, certification under ISO/IEC 27001, and the different types of AIS security controls used in UK companies. However, in order to avoid violating the above requirements and to ensure the validity of the results, the industry sectors were combined. Originally, seven industry sectors responded; however, in order to use the chi-square test, they were combined into four sectors: insurance & financial services, manufacturing & merchandising, technology, media & entertainment, and construction, energy & utilities. The results of the chi-square test are discussed in Sections 4.5, 4.6, and 4.7.

4.3.5 Spearman's rank correlation coefficient

Correlation is one of the most widely used measures of association between two or more variables. The measures of correlation are employed to explore the presence or absence of a correlation. The correlation coefficient describes the direction of the correlation (whether it is positive or negative) and the strength of the correlation (whether an existing correlation is strong or weak) (Singh 2007, p.146).

Spearman's rank correlation is designed for use with ordinal or ranked data and is particularly useful when the data do not meet the criteria for Pearson's correlation[2] (Pallant 2007). Spearman's rank correlation is used to analyse the degree of association of two variables. Spearman's rank correlation coefficient (r_s) is computed as follows (Anderson *et al.* 2007):

$$r_s = 1 - 6 \sum d_i^2 / n (n^2 - 1)$$

[2] Pearson's correlation is the most common measure of association between two or more variables scaled on an interval level.

Where: n = number of items or individuals being ranked

$d_i = x_i - y_i$

x_i = the rank of items i with respect to one variable

y_i = the rank of items i with respect to the second variable

Spearman's rank correlation coefficient (r_s) can take values from -1 to +1, so that the sign indicates whether there is a positive correlation or a negative correlation. The size of the absolute value provides an indication of the strength of the relationship. A perfect correlation of +1 or -1 indicates that the value of one variable can be determined exactly by knowing the value of the other variable. On the other hand, a correlation of zero indicates no relationship between the two variables. According to Singh (2007), a correlation is considered very low if the coefficient has a value under 0.20, and is considered low if the value ranges between 0.21 and 0.40, whereas a coefficient value above 0.70 is considered high. The hypotheses for Spearman's rank correlation can be written as follows:

Ho: There is no correlation in the ranked data of the population i.e. there is no association between the two variables.

H1: There is a correlation in the ranked data of the population i.e. there is an association between the two variables.

The significance level obtained does not indicate how strongly the two variables are associated, but it indicates how much confidence the researcher should have in the results obtained that is whether a value produced by a measure of association does in fact reflect the existence of a true relationship in the population. Therefore, if p-value < 0.05, the null hypothesis can be rejected which indicates that the two variables are associated.

Based on the above, Spearman's rank correlation is used in the current study to analyse the degree of association between the different types of AIS security threats and the different types of controls used in UK companies to reduce these threats. In addition, Spearman's rank correlation is used also to analyse the degree of correlation between the AIS security effectiveness level in UK companies and the types of

security threats facing these companies. The results of Spearman's rank correlation are discussed in Section 4.7.

4.3.6 Multiple regression analysis

Multiple regression analysis is the most commonly utilised multivariate technique. It examines the relationship between a single dependent variable and two or more independent variables (Singh 2007, p.178). There are two major uses of multiple regressions: prediction and causal analysis. According to Allison (1999), in a prediction study, the goal is to develop a formula for making predictions about the dependent variable, based on the observed values of the independent variables. On the other hand, in a causal analysis, the aim of the study is to determine whether a particular independent variable really affects the dependent variable, and to estimate the magnitude of that effect, if any, which is our concern in the current study.

The multiple regression technique relies upon determining the linear relationship with the lowest sum of squared variances (Singh 2007). The general equation for the multiple regression models takes the following form (Black 1994, p.562):

$$Y = \beta o + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \ldots\ldots\ldots\ldots\ldots\ldots + \beta_k X_k + \varepsilon$$

Where: Y = the dependent variable

X_k = the independent variable k

βo = the regression constant

β_1 = the regression coefficient for independent variable X_1

β_2 = the regression coefficient for independent variable X_2

β_k = the regression coefficient for independent variable X_k

ε = the error of prediction

In multiple regression, the dependent and independent variables should preferably be measured on an interval scales, though ordinal scale measurements are also acceptable (Singh 2007). Allison (1999) also indicated that, in practice, ordinal variables are often used in regression analysis. In addition, by using the technique of "dummy variables", the researcher can even include qualitative factors in the regression

analysis (Levin and Rubin 1994, p.646). Moreover, Allison (1999) stated that dummy variables are perfect as independent variables in regression analysis.

According to Anderson *et al.* (2007), there are four variable selection procedures: stepwise regression, forward selection, backward elimination, and best-subsets regression. These procedures are used to identify which independent variables provide the best model. Stepwise regression is the most widely known and used by researchers. In stepwise regression, the researcher provides the computer program for example SPSS with a list of independent variables. The stepwise regression procedure begins each step by determining whether any of the variables already in the model should be removed. If none of the independent variables can be removed from the model, the procedure checks to see whether any of the independent variables that are not currently in the model can be entered. In stepwise regression, an independent variable can enter the model at one step, be removed at a subsequent step, and then enter the model at a later step. This procedure then stops when no independent variables can be removed from or entered into the model. However, because the stepwise procedure is based on statistical considerations alone and requires no theoretical justification for the independent variable it includes or excludes from entry, the researcher knows what was and was not included but not why.

One problem that can arise in multiple regression analysis is multicollinearity. This problem arises when the independent variables are too highly correlated with one another. Allison (1999) indicated that a common way to judge the seriousness of the multicollinearity problem is to examine all the bivariate correlations among the independent variables. In addition, the tolerance value that appears in the output of regression analysis is very effective in diagnosing multicollinearity. Tolerance value ranges between 0 and 1, so that high tolerance values indicate low multicollinearity, whereas low tolerance values indicate high multicollinearity. Allison (1999) suggested that the researcher starts to get concerned if the tolerance falls below 0.40. In the current study, the tolerance values range between 0.7 and 0.9, which indicates that multicollinearity is low and that there is a low level of correlation between independent variables. In addition, Black (1994) stated that stepwise regression is a way to prevent the problem of multicollinearity.

In the current study, a series of stepwise regressions was run in an attempt to identify the significant effect of the different types of security controls implemented by UK companies and AIS security effectiveness level on the reduction of AIS security threats facing the companies. Consequently, 13 regressions were run and the dependent variable in each regression was one type of security threat and the independent variables were the different types of security controls and the security effectiveness level within UK companies. The results of the regression analysis are discussed in Section 4.7.

4.4 General and background information

Section 4 of the questionnaire (Appendix 1) focused on the respondents and their companies' background. Respondents were asked eight questions concerning their position, experience, qualifications, and their companies' characteristics. The main objective of these questions was to obtain a profile of those who participated in the study and were useful for statistical analysis and comparisons. The background information requested from respondents includes their job titles, years of experience in the current job, most recent educational qualification obtained, academic field of study, and their security qualification, if obtained. In addition, respondents were asked about their companies' industry sector, age, and number of employees.

Respondents' job title

In Question 4.1 of the questionnaire, respondents were asked to state their job title. It was disclosed in Chapter 3 that the questionnaire was mailed to the IT managers of the UK listed companies. Table 4.2 below shows that 39 percent of respondents are IT managers, and 10 respondents (15.6 percent) are security managers, whereas other titles such as risk manager, information security analyst, etc. represent small percentages of the respondents. It can also be seen that among the respondents, there are eight finance directors (12.5 percent). This could be because some companies depend mainly on outside service providers in most of their IT functions that is outsourcing most IT functions; consequently, they do not have an internal IT manager to complete the questionnaire. On the other hand, because of the nature of the current study and its focus on AIS, the IT managers could take the view that finance directors are more knowledgeable of the security of these accounting systems and they are able

to provide the required data. This issue is further investigated in the next chapter using data collected in the interviews.

Table 4.2 Job title of respondents

Job title	no	%
Chief information officer	4	6.3
Information technology manager	25	39
Security manager	10	15.6
Head of information systems	3	4.7
Information security analyst	1	1.6
Risk manager	2	3
Information security architecture manager	1	1.6
Infrastructure director	3	4.7
Finance director	8	12.5
Others	7	11
Total	64	100

Years of experience in the current job

Question 4.2 of the questionnaire asked respondents about the number of years of experience in their current job. From Table 4.3, it can be seen that just over one third of respondents (35.4 percent) have less than 5 years of experience in their current job, 27 respondents (41.5 percent) have from 5 to 10 years of experience, whereas only one respondent has more than 20 years of experience in the current job. Regarding the managers who have less than 5 years of experience in their current job, they still have the experience and knowledge, which qualify them to complete the questionnaire, because according to the interviews' data, most of these managers had more years of experience in the same position or in equivalent positions in other companies.

Table 4.3 Years of experience of respondents in the current job

Years of experience in current job	no	%
Less than 5 years	23	35.4
5 -10	27	41.5
11-15	5	7.7
16-20	9	13.9
More than 20 years	1	1.5
Total	65	100

The most recent educational qualification

Question 4.3 of the questionnaire asked respondents about the most recent educational qualification they have obtained. Out of the 65 respondents, 11 respondents did not mention their most recent educational qualification. Table 4.4 shows the most recent educational qualification of those who responded. The results reveal that 35.2 percent

of respondents had obtained a bachelors degree, three respondents (5.5 percent) a masters degree, whereas another three respondents had obtained a PhD degree.

Table 4.4 The most recent educational qualification of respondents

Most recent educational qualification	no	%
Bachelors degree	19	35.2
Diploma	3	5.5
Masters degree	3	5.5
PhD degree	3	5.5
MBA	5	9.3
Others	21	39
Total	54	100

The academic field of study

Question 4.4 of the questionnaire asked respondents to state the academic field of study of their most recent educational qualification. It can be seen from Table 4.5 that 32 percent of respondents have a computer science degree, eight respondents have a business/management degree, 10 percent of respondents have an accounting/finance degree, while the academic field of study of the other respondents includes economics, mathematics/statistics, information security, risk management, engineering/electronics, and biochemistry/physics.

Table 4.5 The academic field of study of respondents

Academic field of study	no	%
Business/management	8	16
Accounting/finance	5	10
Economics	2	4
Mathematics/statistics	4	8
Computer science	16	32
Information security	2	4
Risk management	1	2
Engineering/electronics	4	8
Biochemistry/physics	2	4
Others	6	12
Total	50	100

Professional security qualification

Question 4.5 of the questionnaire asked respondents to specify their professional security qualification if obtained. The BERR Information Security Breaches Survey (BERR 2008) stated that there has been an increased emphasis on security qualifications in the UK following the formation of the Institute of the Information Security Professionals, and that nearly 98 percent of large businesses now have qualified staff. However, nearly 90 percent of respondents in the current study do not have any professional security qualification. Out of the 65 respondents, only seven

respondents (10.8 percent) have professional security qualification. Among these seven respondents, three respondents are Certified Information Systems Security Professionals (CISSP). In addition, one respondent has a Certificate in Information Security Management Principles (CISMP), another respondent is a Certified Information Security Manager (CISM), another respondent has the Information Systems Security Professionals (ISSP) qualification, while the other has a qualification obtained from the British Computer Society (BCS).

Table 4.6 The number of respondents having professional security qualification

Professional security qualification	no	%
Yes	7	10.8
No	58	89.2
Total	65	100

Industry sector

It was mentioned in Section 3.2.1.4 (Chapter 3) that there is an agreement that a company's approach to information security depends on its industry sector. Companies in different industry sectors tend to have different security requirements. Based on the importance of the industry sector in the current study, Question 4.6 of the questionnaire asked respondents to select the industry sector, which most closely corresponds to their companies' line of business. Table 4.7 demonstrates that 20 percent of respondents are from the property & construction sector, followed by insurance & financial services (16.9 percent), manufacturing (15.4 percent), energy & utilities (13.9 percent), technology & telecommunications (12.3 percent), retail merchandising (10.8 percent) and media & entertainment (9.2 percent). However, only one respondent is from the pharmaceuticals sector, which was eliminated from further analysis due to statistical considerations.

Table 4.7 Distribution of respondents by industry sector

Industry sector	no	%
Insurance & financial services	11	16.9
Manufacturing	10	15.4
Media & entertainment	6	9.2
Property & construction	13	20
Retail merchandising	7	10.8
Technology & telecommunications	8	12.3
Energy & utilities	9	13.9
Pharmaceuticals	1	1.5
Total	65	100

Age of company

Question 4.7 of the questionnaire asked respondents about their companies' age. It is clear from Table 4.8 below that the majority of companies have been established for more than 20 years (89.2 percent), 9.2 percent of companies for 11 to 20 years, with only one company for 5 to 10 years. The results reveal that nearly all the companies participating in the current study have been established for at least 10 years.

Table 4.8 The age of the companies participating in the study

Age of company	no	%
5-10	1	1.5
11-20	6	9.2
More than 20 years	58	89.2
Total	65	100

Number of employees

Question 4.8 of the questionnaire asked respondents to state the approximate number of employees in their companies. It can be seen from Table 4.9 that 83 percent of companies participating in the study have at least 100 employees. The results also show that 15 companies (23.1 percent) have from 1001 to 5000 employees, another 23.1 percent of companies have from 100 to 500 employees, 11 companies have more than 10000 employees, and another 16.9 percent have fewer than 100 employees. Table 4.9 also shows that 10.8 percent of companies have from 501 to 1000 employees, while 9.2 percent have from 5001 to 10000 employees. The results indicate that the size of the companies participating in the study ranges from medium (less than 100 employees), to large (100-1000) to very large (1001 - more than 10000 employees). This is important since companies in different sizes tend to handle information security differently, given that they have different levels of resources and expertise (Chang and Ho 2006).

Table 4.9 The number of employees in the companies participating in the study

Number of employees	no	%
Less than 100	11	16.9
100-500	15	23.1
501-1000	7	10.8
1001-5000	15	23.1
5001-10000	6	9.2
More than 10000	11	16.9
Total	65	100

The subsequent analysis of the questionnaire findings is presented on the following three sections (4.5 – 4.7) based on the same sequence of the questionnaire (Appendix 1).

4.5 The management framework of AIS security

Companies now are faced with contradictory requirements to deal with open systems on the one hand and to assure high protection standards on the other hand (Trcek 2003). Consequently, management of IS requires a structured and disciplined process (Vermeulen and Von Solms 2002). In addition, an IS security management framework must exist not only to protect IS and information, but to ensure the continuity of the company (Karyda *et al.* 2005). Section 1 of the questionnaires collected respondents' opinions concerning the management framework of AIS security within their companies. Consequently, this section presents and analyses respondents' opinions regarding this framework and it is divided into the following sections:

4.5.1 AIS security policy
4.5.2 Security training and awareness program
4.5.3 Risk assessment
4.5.4 Incident response, disaster recovery and business continuity plan
4.5.5 Security budget
4.5.6 Security standards and certification
4.5.7 AIS security effectiveness

4.5.1 AIS security policy

There is wide agreement in the literature that the security policy is the starting point of security management. Whitman (2003) argued that the security policy is a company's first and most important layer of security. In addition, Wiant (2005) stated that the first step towards achieving good information security within a company is to ensure that the security policy at hand is followed, maintained, and updated. David (2002) also indicated that only through the implementation and enforcement of policy could proper security be realised. Moreover, Fulford and Doherty (2003) argued that effective information security management is predicated on the formulation and utilisation of a security policy. While Poore (1999) stated that the lack of a security policy could result in the company subjecting IS and information to undue risks and

increasing the potential for unacceptable loss, liability or harm to the company and to other relevant parties.

Due to the importance of the AIS security policy, this section presents the questionnaire results on the existence and the frequency by which this security policy is updated. This section is concerned with testing Hypothesis 1.1 (Section 3.2.4 in Chapter 3). This hypothesis can be expressed as follows:

H1.1: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security policy and the frequency of updating this policy.

In order to test this hypothesis, respondents were asked two questions (Section 1.1 of the questionnaire). Question 1.1.1 addressed the existence of an AIS security policy within the respondents' companies, whereas Question 1.1.2 focused on the frequency of updating this policy. Table 4.10 demonstrates that the majority of companies (77.4 percent) revealed that they have a security policy. This result is consistent with results of earlier surveys. In their study, Fulford and Doherty (2003) revealed that 76 percent of UK companies have a documented security policy. The results of the BERR Information Security Breaches Survey (BERR 2008) also indicated that nearly 87.5 percent of large UK businesses have a security policy.

Table 4.10 Cross-tabulation of existence of an AIS security policy by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	8		5		6		9		5		7		8		48
%		16.7		10.4		12.5		18.8		10.4		14.6		16.7	
Industry %		72.2		55.6		100		69.2		83.3		87.5		88.9	
No	3		4		0		4		1		1		1		14
%		21.4		28.6		0		28.6		7.1		7.1		7.1	
Industry %		27.3		44.4		0		30.8		16.7		12.5		11.1	
Total	11		9		6		13		6		8		9		62

Q 1.1.1 Does your company have a written security policy covering its AIS?

In addition, the analysis by industry sector reveals that 72.7 percent of the insurance & financial services have an AIS security policy, while only 55.6 percent of manufacturing companies have a security policy in place. These results are again consistent with the results of the BERR Information Security Breaches Survey (BERR

2008) which revealed that over three quarters of financial services companies have a security policy, while the manufacturing companies are less likely to have a security policy in place. The results in Table 4.10 also show that all respondents from media & entertainment reported that their companies have a security policy; however, this result is not consistent with the result of the BERR survey, which indicated that entertainment companies are the least likely to have a security policy.

Regarding the frequency of updating the security policy, Table 4.11 demonstrates that 58.7 percent of companies believed that they updated their AIS security policy every year, 12 companies updated their security policy every two years or less frequently, while the other companies (15.2 percent) updated their security policy every six months or as required. This result is consistent with the result of Fulford and Doherty (2003) in which nearly 46 percent of respondents updated their policy on an annual basis, 38 percent updated their policy every two years or less frequently, while the remainder updated the policy every six months or more frequently.

Table 4.11Cross-tabulation of frequency of updating AIS security policy by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Less frequently than every 3 years	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		11.1		0		0		0	
Every 2 years	1		2		2		2		0		2		2		11
%		9.1		18.2		18.2		18.2		0		18.2		18.2	
Industry %		14.3		40		33.3		22.2		0		28.6		25	
Every year	4		3		2		5		4		4		5		27
%		14.8		11.1		7.4		18.5		14.8		14.8		18.5	
Industry %		57.1		60		33.3		55.6		100		57.1		62.5	
Every 6 months	2		0		1		0		0		0		0		3
%		66.7		0		33.3		0		0		0		0	
Industry %		28.6		0		16.7		0		0		0		0	
As required	0		0		1		1		0		1		1		4
%		0		0		25		25		0		25		25	
Industry %		0		0		16.7		11.1		0		14.3		12.5	
Total	7		5		6		9		4		7		8		46

Q 1.1.2 If yes, approximately how often is this policy updated?

In addition, in order to test the hypothesis and to investigate the differences among industry sectors regarding the existence and frequency of updating their AIS security policies, the chi-square test of independence, and the Kruskal-Wallis tests were

conducted. However, in order to meet the requirements of the chi-square test, the seven industry sectors in Table 4.10 were combined in Table 4.12.

Table 4.12 Cross-tabulation of existence of an AIS security policy by industry sector

	Insurance & financial services		Manufacturing & merchandising		Technology, media & telecommunications		Construction, energy & utilities		Total
	no	%	no	%	no	%	no	%	no
Yes	8		10		13		17		48
%		16.7		20.8		27.1		35.4	
Industry %		72.7		66.7		92.9		77.3	
No	3		5		1		5		14
%		21.4		35.7		7.1		35.7	
Industry %		27.3		33.3		7.1		22.7	
Total	11		15		14		22		62
Chi-square value (χ^2) = 3.039, df = 3, and p-value = 0.386									

Note: Industry sectors are combined for some statistical considerations in using the chi-square test (Section 4.3.4)

The results of the chi-square test (Table 4.12), given that the chi-square value χ^2 = 3.039, df = 3, and the p-value = 0.386 ($p > 0.05$), reveal that there is no significant association between the different industry sectors that responded and the existence of an AIS security policy. In addition, regarding the frequency of updating AIS security policy, the results of the Kruskal-Wallis test (Table 4.13) do not provide any evidence of the existence of statistically significant differences, at the 0.05 level of significance, among the seven industry sectors, given that p-value = 0.876 ($p > 0.05$).

Table 4.13 Results of Kruskal-Wallis test regarding the frequency of updating AIS security policy

Industry sectors	N	Mean Rank
Insurance & financial services	7	27.57
Manufacturing	5	18.40
Media & entertainment	6	25.25
Property & construction	9	21.06
Retail merchandising	4	26
Technology & telecommunications	7	23.21
Energy & utilities	8	23.56
Chi-square value (χ^2) = 2.436, df = 6, and p-value = 0.876		

The above results, therefore, do not provide any evidence to suggest that the existence and the frequency of updating AIS security policies are in any way related to the industry sectors that responded. Consequently, $H_{1.1}$ cannot be rejected.

Overall, the results indicate that an AIS security policy has now been adopted in the majority of companies that responded regardless of the industry sector. However, the term "security policy" has different meanings to different companies. The BERR Information Security Breaches Survey (BERR 2008) indicated that a security policy could vary from a one-page policy to hundreds of pages of detailed standards. This

issue is further investigated in more details in the follow-up interviews (Chapter 5). However, having a security policy alone cannot improve security awareness among employees. The companies, therefore, should take some steps to raise employees' security awareness.

4.5.2 Security training and awareness program

Employee training and awareness is the most important of all information security measures (Eveloff 2005). Bowen *et al.* (2007) argued that security training and awareness is a critical component of the information security program and the vehicle for disseminating the security information that employees need to do their jobs. It will ensure that employees at all levels understand their security responsibilities to properly use and protect information resources entrusted to them. Security training and awareness are also requisites for several international standards such as ISO 27001 and COBIT.

Due to the importance noticed in the literature regarding security training and awareness, this section presents the questionnaire results on the existence of a formal security training and awareness program for managers, employees and other users in UK companies. This section is concerned with testing Hypothesis 1.2 (Section 3.2.4 in Chapter 3). This hypothesis can be expressed as follows:

H1.2: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security training and awareness program and the security awareness level.

In order to test the hypothesis, respondents were asked two questions (Section 1.2 of the questionnaire). Question 1.2.1 was concerned with the existence of a formal security training and awareness program for managers, employees, and other users in UK companies, while Question 1.2.2 addressed the security awareness practices in the companies.

The results in Tables 4.14, 4.15, and 4.16 indicate that the majority of companies that responded do not provide enough security training for their managers, employees and the other users. Table 4.14 demonstrates that only 18 companies (29 percent) provide

security training for managers. In addition, Table 4.15 shows that 25.8 percent of companies provide security training for employees, while Table 4.16 shows that only 10 companies provide security training for other users such as third parties and contractors.

Table 4.14 Cross-tabulation of existence of an AIS security training for managers by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	6		2		2		2		3		1		2		18
%		33.3		11.1		11.1		11.1		16.7		5.6		11.1	
Industry %		60		20		33.3		15.4		50		12.5		22.2	
No	4		8		4		11		3		7		7		44
%		9.1		18.2		9.1		25		6.8		15.9		15.9	
Industry %		40		80		66.7		84.6		50		87.5		77.8	
Total	10		10		6		13		6		8		9		62

Q 1.2.1 Does your company have a formal AIS security awareness and training program for its managers?

Table 4.15 Cross-tabulation of existence of an AIS security training for employees by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	5		2		2		1		2		2		2		16
%		31.3		12.5		12.5		6.3		12.5		12.5		12.5	
Industry %		50		20		33.3		7.7		33.3		25		22.2	
No	5		8		4		12		4		6		7		46
%		10.9		17.4		8.7		26.1		8.7		13		15.2	
Industry %		50		80		66.7		92.3		66.7		75		77.8	
Total	10		10		6		13		6		8		9		62

Q 1.2.1 Does your company have a formal AIS security awareness and training program for its employees?

Table 4.16 Cross-tabulation of existence of an AIS security training for other users by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	3		1		2		1		1		1		1		10
%		30		10		20		10		10		10		10	
Industry %		33.3		10		33.3		7.7		20		16.7		11.1	
No	6		9		4		12		4		5		8		48
%		12.5		18.8		8.3		25		8.3		10.4		16.7	
Industry %		66.7		90		66.7		92.3		80		83.3		88.9	
Total	9		10		6		13		5		6		9		58

Q 1.2.1 Does your company have a formal AIS security awareness and training program for the other users?

These results are, to some extent, consistent with the results of the DTT Global Security Survey (DTT 2005) which indicated that only 37 percent of companies had provided security training for their employees. However, the results are not consistent with the results of the DTI Information Security Breaches Survey (DTI 2006) in which nearly one in eight companies did nothing to educate their staff about their security responsibilities. The results are not consistent either with the results of the

CSI Survey (Richardson 2007) which revealed that 80 percent of respondents are training their employees about security risks and appropriate handling of sensitive data.

The low level of security training and awareness presented in Tables 4.14, 4.15, and 4.16 could be because the majority of companies find it difficult to justify their spending on security training programs. Further verification was found in the follow-up interviews, which is discussed in Chapter 5.

Further analysis reveals that more than half of the insurance & financial services companies that responded (60 percent) provide security training for their managers (Table 4.14), 50 percent provide security training for their employees (Table 4.15), whereas only one third provide security training for the other users (Table 4.16). Table 4.14 shows that only one in eight technology & telecommunications companies (12.5 percent) provide security training for their managers. Moreover, the property & construction companies are the least likely to provide their managers, employees and other users with the relevant security training. Table 4.14 shows that 15.4 percent of the property & construction companies provide their managers with security training, while only 7.7 percent provide their employees with security training (Table 4.15), and another 7.7 percent provide other users with security training (Table 4.16). According to expectations, 80 percent of manufacturing companies do nothing to train their managers and employees on their security responsibilities, and only 10 percent provide security training to other users.

These results are consistent with the literature. There is wide agreement that some industry sectors such as financial services companies are more concerned with information security, and therefore, devote more efforts to raising the security awareness of their staff. Kankanhalli *et al.* (2003) indicated that financial services companies tend to invest more resources in IS and obtain more benefits from IS than other companies. Goodhue and Straub (1991) argued that financial services companies are more likely than other companies to rely extensively on IS for their business operations. In addition, IS generally plays a more strategic and critical role in finance than in other sectors (Jarnvenpaa and Ives 1990), and therefore, they are more concerned about giving their managers, employees and other users the relevant

security training. By contrast, manufacturing companies have more internal operations and transaction processes and thus may require fewer strategic IS applications (King 1994), and therefore, these companies do not devote much effort or resources to giving their staff and other users the appropriate security training.

Table 4.17 Results of chi-square test for the existence of security training

Existence of AIS security training	χ^2	df	p-value
Managers	6.343	3	0.096
Employees	4.820	3	0.185
Other users	3.324	3	0.344

Although some differences are noticed between industry sectors, the results of the chi-square test (Table 4.17) provide no evidence for any statistically significant association between the different industry sectors in the UK and the existence of AIS security training programs for managers, employees and the other users, given that, χ^2 = 6.343, 4.820, and 3.324, and the p-values = 0.096, 0.185, and 0.344 respectively.

Table 4.18 Cross-tabulation of regular communication of security awareness issues by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Strongly disagree	0		0		0		1		0		1		0		2
%		0		0		0		50		0		50		0	
Industry %		0		0		0		7.7		0		12.5		0	
Disagree	2		5		0		3		2		2		4		18
%		11.1		27.8		0		16.7		11.1		11.1		22.2	
Industry %		18.2		50		0		23.1		28.6		25		44.4	
Neither agree nor disagree	1		1		3		4		2		0		1		12
%		8.3		8.3		25		33.3		16.7		0		8.3	
Industry %		9.1		10		50		30.8		28.6		0		11.1	
Agree	7		4		1		4		2		4		4		26
%		26.9		15.4		3.8		15.4		7.7		15.4		15.4	
Industry %		63.6		40		16.7		30.8		28.6		50		44.4	
Strongly agree	1		0		2		1		1		1		0		6
%		16.7		0		33.3		16.7		16.7		16.7		0	
Industry %		9.1		0		33.3		7.7		14.3		12.5		0	
Total	11		10		6		13		7		8		9		64

Q 1.2.2 Please indicate your level of agreement with the following statement: Your company communicates security awareness issues to its managers and employees regularly.

Furthermore, in order to assess the security awareness level among UK companies, respondents were given four statements regarding security awareness practices within their companies and were asked to indicate their level of agreement with each of the four statements on a scale ranging from strongly disagree to strongly agree.

The first statement asked respondents whether their companies communicate security awareness issues to the employees regularly. The results in Table 4.18 show that 32 respondents (50 percent) agreed or strongly agreed, whereas, 31.2 percent disagreed or strongly disagreed. Further analysis reveals that 72.7 percent of the insurance & financial services companies agreed or strongly agreed that there is a regular communication of security awareness issues to employees, followed by technology & telecommunications companies (62.5 percent), whereas 50 percent of the manufacturing companies disagreed with the first statement. This result reflects the fact that financial companies are more concerned about security than the other sectors.

Table 4.19 Cross-tabulation of communication of security awareness issues in response to specific incidents by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Strongly disagree	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		7.7		0		0		0	
Disagree	0		3		0		1		0		0		2		6
%		0		50		0		16.7		0		0		33.3	
Industry %		0		30		0		7.7		0		0		22.2	
Neither agree nor disagree	3		0		1		0		1		0		2		7
%		42.9		0		14.3		0		14.3		0		28.6	
Industry %		27.3		0		16.7		0		14.3		0		22.2	
Agree	6		5		3		8		4		2		5		33
%		18.2		15.2		9.1		24.2		12.1		6.1		15.2	
Industry %		54.5		50		50		61.5		57.1		25		55.6	
Strongly agree	2		2		2		3		2		6		0		17
%		11.8		11.8		11.8		17.6		11.8		35.3		0	
Industry %		18.2		20		33.3		23.1		28.6		75		0	
Total	11		10		6		13		7		8		9		64

Q 1.2.2 Please indicate your level of agreement with the following statement: Your company communicates security awareness issues to its managers and employees in response to specific incidents.

The second statement asked respondents whether their companies communicate security awareness issues to their employees in response to specific incidents. Table 4.19 shows that the majority of the respondents (78.1 percent) agreed or strongly agreed. Further analysis reveals that all technology & telecommunications companies agreed or strongly agreed that security awareness issues are communicated in response to specific incidents, followed by retail merchandising (85.7 percent), property & construction (84.6 percent), and media & entertainment (83.3 percent), while only 55.6 percent of the energy & utilities companies agreed on the second statement.

Regarding the third statement, respondents were asked to indicate whether their companies supply employees with security awareness materials such as staff handbook, brochures, and intranet pages. It can be seen from Table 4.20 that the majority of respondents (70.3 percent) agreed or strongly agreed, while only 20.3 percent disagreed or strongly disagreed. In addition, the analysis by industry sector revealed that eight out of nine respondents from energy & utilities companies (88.9 percent) agreed or strongly agreed that their companies are supplying employees with security awareness materials, although only 44.4 percent from the same sector agreed with the first statement and 55.6 percent agreed with the second statement.

Table 4.20 Cross-tabulation of frequency of supplying employees with security awareness materials by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Strongly disagree	2		0		0		0		1		0		0		3
%		66.7		0		0		0		33.3		0		0	
Industry %		18.2		0		0		0		14.3		0		0	
Disagree	1		5		0		2		1		1		0		10
%		10		50		0		20		10		10		0	
Industry %		9.1		50		0		15.4		14.3		12.5		0	
Neither agree nor disagree	0		0		1		4		0		0		1		6
%		0		0		16.7		66.7		0		0		16.7	
Industry %		0		0		16.7		30.8		0		0		11.1	
Agree	5		5		4		6		3		4		6		33
%		15.2		15.2		12.1		18.2		9.1		12.1		18.2	
Industry %		45.5		50		66.7		46.2		42.9		50		66.7	
Strongly agree	3		0		1		1		2		3		2		12
%		25		0		8.3		8.3		16.7		25		16.7	
Industry %		27.3		0		16.7		7.7		28.6		37.5		22.2	
Total	11		10		6		13		7		8		9		64

Q 1.2.2 Please indicate your level of agreement with the following statement: Your company supplies its managers and employees with security awareness materials e.g. staff handbook, brochures, posters, intranet pages.

In addition, it can be seen from Table 4.20 that 87.5 percent of technology & telecommunications companies agreed or strongly agreed, followed by media & entertainment (83.3 percent), whereas only half of the respondents from manufacturing companies agreed with the third statement. The results imply that energy & utilities and technology & telecommunications companies are more concerned with supplying their employees with security awareness materials than the other sectors.

Table 4.21 Cross-tabulation of the regular testing of security awareness by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Strongly disagree	0		0		0		1		1		0		1		3
%		0		0		0		33.3		33.3		0		33.3	
Industry %		0		0		0		8.3		14.3		0		11.1	
Disagree	4		8		1		4		1		3		4		25
%		16		32		4		16		4		12		16	
Industry %		36.4		80		16.7		33.3		14.3		37.5		44.4	
Neither agree nor disagree	4		0		4		3		3		1		2		17
%		23.5		0		23..5		17.6		17.6		5.9		11.8	
Industry %		36.4		0		66.7		25		42.9		12.5		22.2	
Agree	0		1		0		3		1		4		2		11
%		0		9.1		0		27.3		9.1		36.4		18.2	
Industry %		0		10		0		25		14.3		50		22.2	
Strongly agree	3		1		1		1		1		0		0		7
%		42.9		14.3		14.3		14.3		14.3		0		0	
Industry %		27.3		10		16.7		8.3		14.3		0		0	
Total	11		10		6		12		7		8		9		63

Q 1.2.2 Please indicate your level of agreement with the following statement: Your company conducts regular testing of security awareness.

The fourth statement asked respondents whether their companies conduct regular testing of security awareness. Although there is a wide agreement on the importance of testing security awareness, Table 4.21 shows that only 28.6 percent of respondents agreed or strongly agreed that their companies conduct regular testing of security awareness, while 44.4 percent disagreed or strongly disagreed. This result is consistent with the CSI Survey (Richardson 2007) in which 35 percent of respondents made no effort to test security awareness or to measure the effect of security training on the company.

It can be seen from Table 4.21 that four fifths of respondents from manufacturing companies disagreed, 55.6 percent of energy & utilities companies disagreed or strongly disagreed, and 37.5 percent of technology & telecommunications companies disagreed. This level of disagreement among all industry sectors that responded might be due to the limited time and resources devoted to security training and awareness. These results are consistent with the interviews' results, which are investigated in more detail in Chapter 5.

Moreover, in order to test the hypothesis and to examine whether the security awareness level differs among industry sectors, the Kruskal-Wallis test was conducted. The results (Table 4.22) do not indicate any statistically significant differences, at the 0.05 level, in the distribution of responses between industry sectors

except for the second statement. The results imply that there are significant differences, at the 0.05 level, among UK companies in different industry sectors regarding the communication of security awareness issues in response to specific incidents, given that p-value = 0.032 ($p < 0.05$). On the other hand, there are no significant differences, at the 0.05 level, in the distribution of responses between industry sectors regarding the first, third, and fourth statements, given that their p-values are 0.546, 0.222, and 0.607 respectively.

Table 4.22 Results of Kruskal-Wallis test regarding the security awareness practices in companies

Security awareness practices	Industry sectors	N	Mean Rank
Regular communication of security awareness issues	Insurance & financial services	11	39.05
	Manufacturing	10	26.60
	Media & entertainment	6	41.33
	Property & construction	13	29.65
	Retail merchandising	7	32.64
	Technology & telecommunications	8	33.50
	Energy & utilities	9	28.28
Chi-square value (χ^2) = 4.985, df = 6, and p-value = 0.546			
Communication of security awareness issues in response to specific incidents	Insurance & financial services	11	30.09
	Manufacturing	10	28.05
	Media & entertainment	6	36
	Property & construction	13	32.42
	Retail merchandising	7	35.29
	Technology & telecommunications	8	49.75
	Energy & utilities	9	20.67
Chi-square value (χ^2) = 13.804, df = 6, and p-value = 0.032			
Supplying employees with security awareness materials	Insurance & financial services	11	33.45
	Manufacturing	10	22.25
	Media & entertainment	6	36.50
	Property & construction	13	27.50
	Retail merchandising	7	33.64
	Technology & telecommunications	8	41
	Energy & utilities	9	38.83
Chi-square value (χ^2) = 8.229, df = 6, and p-value = 0.222			
Regular testing of security awareness	Insurance & financial services	11	35.64
	Manufacturing	10	23.90
	Media & entertainment	6	37.33
	Property & construction	12	32.50
	Retail merchandising	7	34.29
	Technology & telecommunications	8	36.13
	Energy & utilities	9	26.89
Chi-square value (χ^2) = 4.517, df = 6, and p-value = 0.607			

In short, from the responses to the questions in this section, it was found that some sectors are taking more steps to provide their employees with security training and to raise their awareness such as the insurance & financial services sector, whereas the manufacturing sector does not devote enough effort to training their employees or raising their security awareness.

4.5.3 Risk assessment

Risk assessment is often the basis for an information security program (Wiant 2005). Since the nature and degree of threats facing companies vary there needs to be a risk

assessment of the likelihood that security will be compromised (Dutta and McCrohan 2002). In addition, companies are requested today to perform a risk assessment for their financial risks (Gomez and Paxmann 2006). Furthermore, to comply with the security standards such as ISO 27001, companies must demonstrate the use of a risk assessment methodology suited to their business, considering information security, legal and regulatory requirements (Kouns 2007).

Due to the importance of risk assessment, this section presents the questionnaire results on the existence of an AIS risk assessment program, the frequency of undertaking this program, and the risk assessment activities in UK companies. This section is concerned with testing Hypothesis 1.3 (Section 3.2.4 in Chapter 3). The hypothesis can be expressed as follows:

H1.3: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS risk assessment program and the frequency of undertaking this program.

In order to test this hypothesis, respondents were asked three questions (Section 1.3 of the questionnaire). Question 1.3.1 was concerned with the existence of security risk assessment programs in UK companies, Question 1.3.2 focused on the frequency of undertaking this risk assessment, while Question 1.3.3 addressed the risk assessment activities in the companies.

Table 4.23 Cross-tabulation of existence of an AIS risk assessment program by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	7		3		6		7		4		5		6		38
%		18.4		7.2		15.8		18.4		10.5		13.2		15.8	
Industry %		70		42.9		100		53.8		66.7		62.5		66.7	
No	3		4		0		6		2		3		3		21
%		14.3		19		0		28.6		9.5		14.3		14.3	
Industry %		30		57.1		0		46.2		33.3		37.5		33.3	
Total	10		7		6		13		6		8		9		59

Q 1.3.1 Does your company have an AIS risk assessment program?

Regarding the first question, Table 4.23 demonstrates that 38 respondents (64.4 percent) have security risk assessment programs, whereas 35.6 percent of respondents do not undertake any risk assessment for their AIS security. These results are

consistent, to some extent, with the results of the BERR Information Security Breaches Survey (BERR 2008) in which 77 percent of large UK companies have a security risk assessment process.

It is clear from Table 4.23 that 35.6 percent of the companies do not undertake any AIS security risk assessment. This result could be because some companies do not have a risk assessment program especially for AIS security, but they undertake a security risk assessment for their companies' IS in general. This issue is investigated in more detail in Chapter 5.

In addition, further analysis (Table 4.23) reveals that 70 percent of the insurance & financial services companies have an AIS security risk assessment program in place. This result is again consistent with the results of the BERR Information Security Breaches Survey (BERR 2008) which stated that nearly three quarters of financial services companies carry out a formal assessment of their security risks. On the other hand, the results show that all respondents from media & entertainment companies have an AIS risk assessment program, which is not consistent with the results of the BERR survey in which entertainment companies are the least likely to have any risk assessment procedures. These results are encouraging and indicate that the media & entertainment sector is beginning to be more concerned with security and is taking some steps in identifying threats and in assessing security risks.

Moreover, in order to test whether the existence of a risk assessment program is related to the companies' industry sector, a chi-square test was conducted. The results provide no evidence of any statistically significant association between the different sectors that responded and the existence of a risk assessment program, given that $\chi^2 = 2.265$, df = 3, and p-value = 0.519 ($p > 0.05$).

The second question in this section (Question 1.3.2) addressed the frequency by which UK companies undertake risk assessment for their AIS security. Table 4.24 shows that the majority of companies that responded (86.1 percent) undertake risk assessment for their AIS security every year or more frequently, while only 13.9 percent undertake risk assessment every two years or less frequently. This result is consistent with the Global State of Information Security Survey (Berinato 2007) in

which nearly four out of five companies conducted risk assessment at least periodically.

Table 4.24 Cross-tabulation of frequency of undertaking an AIS risk assessment by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Less frequently than every 3 years	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		14.3		0		0		0	
Every 2 years	1		1		1		1		0		0		0		4
%		25		25		25		25		0		0		0	
Industry %		16.7		33.3		16.7		14.3		0		0		0	
Every year	3		2		4		2		3		4		5		23
%		13		8.7		17.4		8.7		13		17.4		21.7	
Industry %		50		66.7		66.7		28.6		100		80		83.3	
Every 6 months	2		0		1		3		0		1		1		8
%		25		0		12.5		37.5		0		12.5		12.5	
Industry %		33.3		0		16.7		42.9		0		20		16.7	
Total	6		3		6		7		3		5		6		36

Q 1.3.2 If yes, approximately how often does your company undertake this risk assessment for its AIS security?

Interestingly, further analysis reveals that all retail merchandising, technology & telecommunications, and energy & utilities companies undertake risk assessment for their AIS security every year or more frequently, followed by insurance & financial services, and media & entertainment (83.3 percent).

Table 4.25 Results of Kruskal-Wallis test regarding the frequency of undertaking AIS risk assessment

Industry sectors	N	Mean Rank
Insurance & financial services	6	19.92
Manufacturing	3	12.50
Media & entertainment	6	17.33
Property & construction	7	19.43
Retail merchandising	3	17
Technology & telecommunications	5	20.10
Energy & utilities	6	19.58
Chi-square value (χ^2) = 1.992, df = 6, and p-value = 0.920		

In order to test whether the frequency with which companies undertake risk assessment is related to industry sector, a Kruskal-Wallis test was conducted. The results (Table 4.25) do not indicate any statistically significant differences, at the 0.05 level, in the distribution of responses between sectors regarding the frequency of undertaking an AIS security risk assessment. This result indicates that since threats vary over time, companies are more concerned with assessing their security risks periodically and with reassessing the effectiveness of their security controls.

Furthermore, in order to investigate the risk assessment activities within UK companies, respondents were given four statements in Question 1.3.3 of the questionnaire and were asked to indicate their level of agreement with each of the four statements on a scale ranging from "strongly disagree" to "strongly agree". The first statement asked respondents whether their companies assess risks and identify AIS security threats regularly. The results in Table 4.26 demonstrate that 57.4 percent of respondents agreed or strongly agreed that their companies assess risks and identify security threats regularly, while 19.7 percent disagreed.

Table 4.26 Cross-tabulation of the regular assessment of AIS security risks by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Disagree	1		3		0		2		2		2		2		12
%		8.3		25		0		16.7		16.7		16.7		16.7	
Industry %		10		33.3		0		15.4		28.8		28.6		22.2	
Neither agree nor disagree	4		2		2		3		1		1		1		14
%		28.6		14.3		14.3		21.4		7.1		7.1		7.1	
Industry %		40		22.2		33.3		23.1		14.3		14.3		11.1	
Agree	4		4		2		7		3		3		6		29
%		13.8		13.8		6.9		24.1		10.3		10.3		20.7	
Industry %		40		44.4		33.3		53.8		42.9		42.9		66.7	
Strongly agree	1		0		2		1		1		1		0		6
%		16.7		0		33.3		16.7		16.7		16.7		0	
Industry %		10		0		33.3		7.7		14.3		14.3		0	
Total	10		9		6		13		7		7		9		61

Q 1.3.3 Please indicate the extent to which you agree or disagree with the following statement: Risks are assessed and threats to the AIS security are identified regularly.

Interestingly, further analysis reveals that two thirds of media & entertainment and energy & utilities companies (66.7 percent) agreed or strongly agreed that risks are assessed and security threats are identified regularly, while 50 percent of insurance & financial services companies agreed or strongly agreed. These results are consistent with the results of Question 1.3.1 in which all the media & entertainment companies have an AIS risk assessment program. These results suggest that media & entertainment companies are beginning to be more concerned with assessing their risks and with identifying their security threats.

In the second statement, respondents were asked whether security controls identified within the risk assessment process provide sufficient protection against threats. It can be seen from Table 4.27 that 83.6 percent of respondents agreed or strongly agreed, while only 6.6 percent disagreed. These results, therefore, imply that nearly four fifths

of the companies that responded believe that they have sufficient security controls in place. These results are further investigated in Section 4.7.

Table 4.27 Cross-tabulation of defining controls and providing sufficient protection against threats by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Disagree	0		2		0		1		0		0		1		4
%		0		50		0		25		0		0		25	
Industry %		0		22.2		0		7.7		0		0		11.1	
Neither agree nor disagree	1		2		0		1		0		1		1		6
%		16.7		33.3		0		16.7		0		16.7		16.7	
Industry %		10		22.2		0		7.7		0		14.3		11.1	
Agree	8		5		4		8		3		4		5		37
%		21.6		13.5		10.8		21.6		8.1		10.8		13.5	
Industry %		80		55.6		66.7		61.5		42.9		57.1		55.6	
Strongly agree	1		0		2		3		4		2		2		14
%		7.1		0		14.3		21.4		28.6		14.3		14.3	
Industry %		10		0		33.3		23.1		57.1		28.6		22.2	
Total	10		9		6		13		7		7		9		61

Q 1.3.3 Please indicate the extent to which you agree or disagree with the following statement: Controls are defined and provide sufficient protection against threats

Interestingly, further analysis reveals again that all respondents from media & entertainment companies agreed or strongly agreed that security controls identified within risk assessment process provide sufficient protection against threats. There are also high levels of agreement among retail merchandising (100 percent), and insurance & financial services (90 percent), while only 55.6 percent of manufacturing companies agreed that they have sufficient protection against security threats.

Table 4.28 Cross-tabulation of ranking assets by their sensitivity and criticality by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Strongly disagree	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		14.3		0	
Disagree	3		2		1		2		1		1		2		12
%		25		16.7		8.3		16.7		8.3		8.3		16.7	
Industry %		30		22.2		16.7		15.4		14.3		14.3		22.2	
Neither agree nor disagree	2		2		0		5		1		2		1		13
%		15.4		15.4		0		38.5		7.7		15.4		7.7	
Industry %		20		22.2		0		38.5		14.3		28.6		11.1	
Agree	4		3		3		5		3		3		5		26
%		15.4		11.5		11.5		19.2		11.5		11.5		19.2	
Industry %		40		33.3		50		38.5		42.9		42.9		55.6	
Strongly agree	1		2		2		1		2		0		1		9
%		11.1		22.2		22.2		11.1		22.2		0		11.1	
Industry %		10		22.2		33.3		7.7		28.6		0		11.1	
Total	10		9		6		13		7		7		9		61

Q 1.3.3 Please indicate the extent to which you agree or disagree with the following statement: Assets are identified and ranked by their value, sensitivity and criticality to the company.

Regarding the third statement, respondents were asked whether assets are identified and ranked by their value, sensitivity, and criticality to their companies. Table 4.28 shows that 57.4 percent of the respondents agreed or strongly agreed, which is the same percentage of respondents who agreed or strongly agreed with the first statement. These results, therefore, imply that the companies that assess and identify AIS security threats regularly identify and rank assets by their sensitivity and criticality to the company as well.

Further analysis reveals that again there are high levels of agreement among media & entertainment companies (83.3 percent) that assets are identified and ranked by their sensitivity and criticality, while only half of the respondents from insurance & financial services and 42.9 percent of technology & telecommunications companies agreed or strongly agreed. These results are unexpected given the nature of the technology & telecommunications companies. Consequently, these results are investigated in more detail in the interview findings.

Table 4.29 Cross-tabulation of undertaking risk assessment after significant changes by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Disagree	0		3		0		1		1		0		2		7
%		0		42.9		0		14.3		14.3		0		28.6	
Industry %		0		33.3		0		7.7		14.3		0		22.2	
Neither agree nor disagree	2		2		2		2		2		1		2		13
%		15.4		15.4		15.4		15.4		15.4		7.7		15.4	
Industry %		20		22.2		33.3		15.4		28.6		14.3		22.2	
Agree	6		4		2		8		2		5		5		32
%		18.8		12.5		6.3		25		6.3		15.6		15.6	
Industry %		60		44.4		33.3		61.5		28.6		71.4		55.6	
Strongly agree	2		0		2		2		2		1		0		9
%		22.2		0		22.2		22.2		22.2		11.1		0	
Industry %		20		0		33.3		15.4		28.6		14.3		0	
Total	10		9		6		13		7		7		9		61

Q 1.3.3 Please indicate the extent to which you agree or disagree with the following statement: The company undertakes risk assessment when a significant change in the company's environment occurs.

The fourth statement asked respondents whether their companies undertake risk assessment if a significant change in the companies' environment occurs. The results in Table 4.29 reveal that nearly two thirds of companies (67.2 percent) agreed or strongly agreed, while only 11.5 percent disagreed. A detailed analysis by industry sector reveals that 85.7 percent of technology & telecommunications companies agreed or strongly agreed, whereas 44.4 percent of the respondents from manufacturing companies agreed. It is clear from Tables 4.27 and 4.29 that the

technology & telecommunications companies who agreed with the second statement (85.7 percent) agreed with the fourth statement (85.7 percent). These results imply that the companies that undertake risk assessment in response to any significant change in companies' environment also believe that security controls identified within the risk assessment process provide sufficient protection against threats.

Moreover, in order to test whether risk assessment activities mentioned in the four statements differ among the industry sectors that responded, a Kruskal-Wallis test was conducted. The analysis of responses (Table 4.30) does not indicate any significant differences, at the 0.05 level, in the distribution of responses between the seven industry sectors for any of the four statements, given that their p-values are 0.809, 0.062, 0.591, and 0.258 for statements 1, 2, 3 and 4 respectively.

Table 4.30 Results of Kruskal-Wallis test regarding the risk assessment activities in companies

Risk assessment activities	Industry sectors	N	Mean Rank
Regular assessment of AIS security risks	Insurance & financial services	10	30.70
	Manufacturing	9	24.72
	Media & entertainment	6	39.67
	Property & construction	13	32.08
	Retail merchandising	7	30.57
	Technology & telecommunications	7	30.57
	Energy & utilities	9	30.94
Chi-square value (χ^2) = 2.998, df = 6, and p-value = 0.809			
Defining controls and providing sufficient protection against threats	Insurance & financial services	10	29.40
	Manufacturing	9	18.33
	Media & entertainment	6	37.50
	Property & construction	13	31.19
	Retail merchandising	7	43.57
	Technology & telecommunications	7	33.21
	Energy & utilities	9	29.33
Chi-square value (χ^2) = 12.003, df = 6, and p-value = 0.062			
Ranking assets by their sensitivity and criticality to the company	Insurance & financial services	10	27.75
	Manufacturing	9	31.94
	Media & entertainment	6	40
	Property & construction	13	28.42
	Retail merchandising	7	37.14
	Technology & telecommunications	7	23.86
	Energy & utilities	9	32.17
Chi-square value (χ^2) = 4.640, df = 6, and p-value = 0.591			
Undertaking risk assessment in case of significant changes	Insurance & financial services	10	36.10
	Manufacturing	9	20.67
	Media & entertainment	6	35.83
	Property & construction	13	33.69
	Retail merchandising	7	31.29
	Technology & telecommunications	7	36.21
	Energy & utilities	9	24.28
Chi-square value (χ^2) = 7.742, df = 6, and p-value = 0.258			

There is no evidence from the above results to indicate that significant differences exist among UK companies in different industry sectors concerning the existence of an AIS risk assessment program and the frequency of undertaking this program. These results provide strong support for Hypothesis 1.3 and, therefore, the hypothesis can be

accepted. These results were followed up in the interviews and further explanations are offered in Chapter 5.

4.5.4 Incident handling, disaster recovery and business continuity plan

Recent surveys for instance the BERR Information Security Breaches Survey (BERR 2008) have revealed that fewer companies had security incidents in the last year than two years previously; however, the average seriousness of incidents had increased. It is, therefore, vital for all types of companies to have security incident handling procedures in place in order to deal with these incidents. Incident handling procedures can provide the ability to react quickly and efficiently to any disruption in normal business processes (Grance *et al.* 2003). In addition, a business continuity plan is a critical component of the security management system (Smith and Jamieson 2006). This plan defines how the continuity of the businesses processes is to be maintained in the event of a disaster (Nosworthy 2000). The business continuity plan assures the IS availability in the case of a crisis or other serious disruption in services. This continuity plan must be a living document (Rodetis 1999) and must be maintained up-to-date with the state of the company (Landry 2006).

Due to the importance of the incident handling procedures and business continuity plans in today's business environment, this section presents the questionnaire results on the numbers and types of security incidents facing UK companies. It also presents the results regarding the existence of security incident handling procedures, length of time to restore normal business operations after a serious security incident, and the actions undertaken by companies to reduce future incidents. In addition, this section presents the results regarding the existence of a formal business continuity plan and the frequency of testing and reviewing this plan. This section is concerned with testing Hypothesis 1.4 (Section 3.2.4 in Chapter 3). This hypothesis can be presented as follows:

H1.4: There are no significant differences among UK companies in different industry sectors concerning the existence of security incident handling procedures, disaster recovery and business continuity plans and the frequency of testing and updating these plans.

In order to test the hypothesis, respondents were asked seven questions (Section 1.4 of the questionnaire). The first three questions addressed the numbers and types of security incidents that UK companies had faced in the previous year. Respondents were asked first if their companies had experienced any AIS security incidents.

Table 4.31 demonstrates that only 11 respondents (17.2 percent) stated that their companies had experienced AIS security incidents in the previous year, whereas 82.8 percent of the companies claimed that they had not experienced any security incidents.

Table 4.31 Cross-tabulation of occurrence of AIS security incidents in the last year by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	2		2		1		1		2		2		1		11
%		18.2		18.2		9.1		9.1		18.2		18.2		9.1	
Industry %		18.2		20		16.7		7.7		28.6		25		11.1	
No	9		8		5		12		5		6		8		53
%		17		15.1		9.4		22.6		9.4		11.3		15.1	
Industry %		81.8		80		83.3		92.3		71.4		75		88.9	
Total	11		10		6		13		7		8		9		64

Q 1.4.1 Has your company experienced any AIS security incidents in the last year?

This result is consistent, to some extent, with the result of the BERR Information Security Breaches Survey (BERR 2008) in which under half of UK businesses had experienced security incidents in 2007. However, it stated that these figures could be under-estimated for several reasons. Some security incidents such as system failure and virus infection are no longer regarded by management as security breaches. In addition, many companies still lack the controls that would enable them to detect all incidents in certain areas such as staff misuse and system penetration. Some companies are also under-estimating risks posed by new technologies such as USB sticks, and therefore are not aware enough of the security breaches involving them. Moreover, many companies are under-reporting the exact number of security incidents. This result is further investigated in the next chapter using data collected in the interviews.

In addition, further analysis (Table 4.31) reveals that there are no significant differences between the industry sectors regarding the occurrence of security incidents in the previous year. The majority of property & construction companies (92.3

percent) claimed that they had no security incidents in the previous year, followed by energy & utilities (88.9 percent), media & entertainment (83.3 percent), insurance & financial services (81.8 percent), and manufacturing (80 percent).

This question was followed-up by asking respondents about the average number of security incidents their companies experienced in the last year (Question 1.4.2). It can be seen from Table 4.32 that 9 respondents (81.8 percent) out of the 11 respondents who reported that they had had security incidents in the previous year, stated that their companies experienced from one to five security incidents, while only two companies (18.2 percent) had had more than 15 incidents.

Table 4.32 Cross-tabulation of number of security incidents in the last year by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
1 - 5	0		2		1		1		2		2		1		9
%		0		22.2		11.1		11.1		22.2		22.2		11.1	
Industry %		0		100		100		100		100		100		100	
More than 15	2		0		0		0		0		0		0		2
%		100		0		0		0		0		0		0	
Industry %		100		0		0		0		0		0		0	
Total	2		2		1		1		2		2		1		11

Q 1.4.2 What is the average number of security incidents your company experienced in the last year?

Interestingly, further analysis reveals that the only respondents who stated that their companies had more than 15 security incidents in the previous year are from the insurance & financial services sector, while the other sectors had from one to five security incidents. This result is consistent with the Global State of Information Security Survey (Berinato 2007) which stated that over the years, respondents in the financial services sector have reported more security incidents without a significant increase in losses or downtime as a result. Consequently, financial services companies are attacked more but suffer less than other sectors.

The respondents were then asked about the worst security incidents their companies had faced in the previous year. Table 4.33 reveals that four companies had suffered from financial fraud, two companies suffered from unauthorised access to data or systems by current employees, while 10 percent suffered from unauthorised access to data or systems by former employees, virus attacks, data loss or internet misuse. These results are consistent with the results of the CSI Survey (Richardson 2007) in

which financial fraud was the source of the greatest financial losses to the companies. The CSI Survey also stated that financial fraud together with data loss account for nearly half of the overall reported losses.

Table 4.33 Cross-tabulation of the worst security incident in the last year by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Financial fraud	1		1		1		0		1		0		0		4
%		25		25		25		0		25		0		0	
Industry %		100		50		100		0		50		0		0	
Unauthorised access to data/systems by former employees	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		50		0	
Unauthorised access to data/systems by current employees	0		0		0		0		0		1		1		2
%		0		0		0		0		0		50		50	
Industry %		0		0		0		0		0		50		100	
Virus attacks	0		0		0		0		1		0		0		1
%		0		0		0		0		100		0		0	
Industry %		0		0		0		0		50		0		0	
Data Loss	0		1		0		0		0		0		0		1
%		0		100		0		0		0		0		0	
Industry %		0		50		0		0		0		0		0	
Internet misuse	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		100		0		0		0	
Total	1		2		1		1		2		2		1		10

Q 1.4.3 What was the worst security incident faced by your company in the last year?

In addition, further analysis (Table 4.33) reveals that insurance & financial services, manufacturing, media & entertainment, and retail merchandising are the most likely sectors to suffer from financial fraud. Manufacturing companies also suffer from data loss, while retail merchandising also suffers from virus attacks.

The results also reveal that technology & telecommunications and energy & utilities companies suffer from unauthorised access to data or systems by employees, while property & construction companies suffer from internet misuse. However, these results are not consistent with the BERR Information Security Breaches Survey (BERR 2008) in which the companies that suffer most from unauthorised access to data and systems are in the financial services and manufacturing sectors. These results are further investigated in Section 4.6.

This question was followed up by asking respondents whether their companies have any formal security incident handling procedures to deal with the security incidents they could face. The results in Table 4.34 show that 68.3 percent of companies have security incident handling procedures in place, while 31.7 percent have no procedures. The results indicate that most of UK companies now have formal procedures to respond to security incidents when they arise. This result is consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that nearly 56 percent of businesses have procedures to respond to incidents.

Table 4.34 Cross-tabulation of the existence of security incident handling procedures by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	8		3		5		7		6		5		7		41
%		19.5		7.3		12.2		17.1		14.6		12.2		17.1	
Industry %		80		33.3		83.3		58.3		100		62.5		77.8	
No	2		6		1		5		0		3		2		19
%		10.5		31.6		5.3		26.3		0		15.8		10.5	
Industry %		20		66.7		16.7		41.7		0		37.5		22.2	
Total	10		9		6		12		6		8		9		60

Q 1.4.4 Does your company have formal security incident handling procedures?

Further analysis reveals that the majority of companies in most of the sectors have procedures to deal with security incidents. All retail merchandising companies have formal procedures, followed by media & entertainment (83.3 percent), insurance & financial services (80 percent), energy & utilities (77.8 percent), technology & telecommunications (62.5 percent) and property & construction (58.3 percent). On the other hand, the results reveal that only 33.3 percent of manufacturing companies have formal procedures to deal with security incidents. These results are consistent with the results in Sections 4.5.1 and 4.5.2, which revealed that nearly half of the manufacturing companies have a security policy yet 80 percent do nothing to train their managers and employees on their security responsibilities. These results indicate that the manufacturing sector is the least concerned with AIS security.

Moreover, in order to test whether the existence of security incident handling procedures is related to the companies' industry sector, a chi-square test was conducted. The results provide no evidence that there are significant association between the different sectors that responded and the existence of security incident handling procedures given that $\chi^2 = 1.199$, df = 3, and p-value = 0.753 ($p > 0.05$).

The respondents were then asked about the length of time taken by their companies to restore normal business operations after the worst security incident (Question 1.4.5). It can be seen from Table 4.35 that 68.2 percent of companies took just one day to restore normal operations after the worst security incident and 22.7 percent needed between a day and a week. On the other hand, only 9.1 percent of companies took between a week and a month to restore normal business operations.

Table 4.35 Cross-tabulation of length of time to restore normal business operations after the worst incident by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
A day	1		2		1		4		3		2		2		15
%		6.7		13.3		6.7		26.7		20		13.3		13.3	
Industry %		33.3		66.7		100		80		75		100		50	
Between a day and a week	1		1		0		1		1		0		1		5
%		20		20		0		20		20		0		20	
Industry %		33.3		33.3		0		20		25		0		25	
Between a week and a month	1		0		0		0		0		0		1		2
%		50		0		0		0		0		0		50	
Industry %		33.3		0		0		0		0		0		25	
Total	3		3		1		5		4		2		4		22

Q 1.4.5 How long did it take to restore normal business operations after the worst security incident?

Analysis by industry sector reveals that the only companies that took between a week and a month to restore normal business operations after the worst security incident are from insurance & financial services and the energy & utilities sectors. This could be because these two sectors are dealing with thousands of customers' data, and therefore, if any security incident arises, it takes them weeks to restore normal business operations. On the other hand, media & entertainment and technology & telecommunications companies took only one day to restore normal operations after the worst incident.

In order to investigate whether the actions undertaken by UK companies after a security incident vary by industry sector, respondents were given a list of actions (Question 1.4.6) and were asked to select the actions undertaken by their companies. Table 4.36 shows that the majority of companies (69.4 percent) improve their disaster recovery and business continuity plan to reduce future incidents. In addition, half of the companies update their security policy, less than half (47.2 percent) undertake a security audit after suffering from a security incident, 44.4 percent improve their

back-up systems and 41.7 percent improve security awareness and training. On the other hand, only 33.3 percent of companies update their detection software or allocate sufficient budget to security to reduce future incidents, whereas nearly one tenth of companies do not take any action after suffering from security incidents.

Table 4.36 Actions undertaken by companies after a security incident

Actions undertaken after a security incident	Action is undertaken		Action is not undertaken		Total
	no	%	no	%	
Updating the security policy	18	50	18	50	36
Improving security awareness and training at all levels	15	41.7	21	58.3	36
Improving the back-up system	16	44.4	20	55.6	36
Improving the disaster recovery and business continuity plan	25	69.4	11	30.6	36
Updating detection software	12	33.3	24	66.7	36
Undertaking security audit	17	47.2	19	52.8	36
Allocating sufficient budget and resources to security	12	33.3	24	66.7	36
No actions were undertaken	4	11.1	32	88.9	36

Q 1.4.6 After a security incident, what actions are undertaken by the company to reduce future incidents?

Further analysis (Table 4.37) reveals that property & construction companies undertake most of the actions to reduce future incidents. The results show that 85.7 percent of property & construction companies improve disaster recovery and their business continuity plan after security incidents, 71.4 percent stated that they update their security policy, improve security awareness and training, improve back-up systems, undertake a security audit and allocate sufficient budget to security. On the other hand, only 42.9 percent of property & construction companies update their detection software. The results also reveal that all technology & telecommunications companies improve security awareness and training after a security incident. This result in conjunction with the results in Section 4.5.2 suggest that technology & telecommunications companies are not providing their managers and employees with regular security training, but they are more concerned with providing them with the relevant security training and awareness in response to security incidents. The results also reveal that none of the retail merchandising companies update their detection software after a security incident, but 20 percent improve security training and awareness, and 40 percent update their security policy, improve their back-up system, undertake a security audit, or allocate sufficient budget to security. These results indicate that retail merchandising companies do not take sufficient action after security incidents, although the previous results showed that they had suffered from financial fraud and virus attacks in the last year. These results are further discussed in Chapter 5.

Table 4.37 Cross-tabulation of the actions undertaken by companies after a security incident by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	
Updating the security policy	4	3	2	4	2	1	5	2	2	3	2	2	1	3	36
Improving security awareness and training at all levels	3	4	0	6	1	2	5	2	1	4	4	0	1	3	36
Improving the back-up system	2	5	2	4	2	1	5	2	2	3	1	3	2	2	36
Improving the disaster recovery and business continuity plan	5	2	3	3	1	2	6	1	4	1	3	1	3	1	36
Updating detection software	3	4	1	5	1	2	3	4	0	5	2	2	2	2	36
Undertaking security audit	3	4	1	5	1	2	5	2	2	3	3	1	2	2	36
Allocating sufficient budget and resources to security	2	5	1	5	0	3	5	2	2	3	1	3	1	3	36
No actions were undertaken	1	6	1	5	0	3	1	6	0	5	0	4	1	3	36

Note: Yes = action was undertaken, and No = action was not undertaken

The respondents were then asked whether their companies have a formal business continuity plan in place. It is clear from Table 4.38 that the majority of companies that responded are now paying more attention to establishing a well-documented business continuity plan.

Table 4.38 Cross-tabulation of the existence of a business continuity plan by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	10		5		5		10		7		7		8		52
%		19.2		9.6		9.6		19.2		13.5		13.5		15.4	
Industry %		100		62.5		83.3		83.3		100		87.5		88.9	
No	0		3		1		2		0		1		1		8
%		0		37.5		12.5		25		0		12.5		12.5	
Industry %		0		37.5		16.7		16.7		0		12.5		11.1	
Total	10		8		6		12		7		8		9		60

Q 1.4.7 Does your company have a formal business continuity plan?

The results show that 86.7 percent of companies have a business continuity plan, whereas only 13.3 percent have no plan. This result reflects the desire of most of the

companies to be certified under the new British Standard BS 25999 (2008) that covers business continuity in companies. Further analysis reveals that a business continuity plan is most common in the insurance & financial services and retail merchandising sectors. All the respondents from both sectors stated that their companies have a business continuity plan. Table 4.38 shows that 88.9 percent of energy & utilities companies, 87.5 percent of technology & telecommunications, 83.3 percent of both media & entertainment and property & construction, and 62.5 percent of manufacturing have a business continuity plan.

In order to test whether the existence of a formal business continuity plan is related to the companies' industry sector, a chi-square test was conducted. There is no evidence from the results that there are significant association between the different industry sectors and the existence of a formal business continuity plan, given that $\chi^2 = 2.143$, df = 3, and p-value = 0.543 ($p > 0.05$).

Table 4.39 Cross-tabulation of the frequency of testing and reviewing business continuity plan by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Less frequently than every 3 years	0		0		0		1		0		1		1		3
%		0		0		0		33.3		0		33.3		33.3	
Industry %		0		0		0		10		0		16.7		12.5	
Every 3 years	1		0		0		0		1		0		0		2
%		50		0		0		0		50		0		0	
Industry %		11.1		0		0		0		14.3		0		0	
Every 2 years	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		10		0		0		0	
Every year	3		5		1		6		5		3		6		29
%		10.3		17.2		3.4		20.7		17.2		10.3		20.7	
Industry %		33.3		100		33.3		60		71.4		50		75	
Every 6 months	5		0		2		2		1		2		1		13
%		38.5		0		15.4		15.4		7.7		15.4		7.7	
Industry %		55.6		0		66.7		20		14.3		33.3		12.5	
Total	9		5		3		10		7		6		8		48

Q 1.4.8 If yes, approximately how often does your company test and review the business continuity plan?

The last question in this section (Question 1.4.8) asked respondents about the frequency with which their companies test and review their business continuity plan. Table 4.39 reveals that the majority of companies (87.5 percent) test and review their business continuity plan every year or more frequently, whereas 12.5 percent test their plan every two years or less frequently. This result is not consistent with the result of

the Global Security Survey (DTT 2007) which indicated that regular testing of business continuity plans is performed by only 40 percent of respondents. This result indicates that UK companies are now more concerned about the regular testing of their business continuity plan in order to be certified under the new Standard BS 25999.

Further analysis reveals that all manufacturing and media & entertainment companies that responded test and review their continuity plan every year or more frequently, followed by insurance & financial services (88.9 percent), energy & utilities (87.5 percent), retail merchandising (85.7 percent), technology & telecommunications (83.3 percent), and property & construction (80 percent). These results indicate that companies have become more aware of the importance of having a well-documented formal continuity plan and of checking it regularly and keeping it up-to-date.

Table 4.40 Results of Kruskal-Wallis test regarding the frequency of testing and reviewing the business continuity plan

Industry sectors	N	Mean Rank
Insurance & financial services	10	32.90
Manufacturing	5	21
Media & entertainment	5	41.20
Property & construction	10	21.80
Retail merchandising	7	21.64
Technology & telecommunications	7	28.36
Energy & utilities	8	21.25
Chi-square value (χ^2) = 12.200, df = 6, and p-value = 0.058		

Moreover, in order to examine whether the frequency by which companies test and review their business continuity plan differs among the seven industry sectors, a Kruskal-Wallis test was conducted. The results (Table 4.40) do not indicate any significant differences, at the 0.05 level, in the distribution of responses among industry sectors, given that p-value = 0.058 ($p > 0.05$).

Overall, the responses to the questions in this section suggest that there are no significant differences among companies in different industry sectors regarding the existence of security incident handling procedures, disaster recovery and business continuity plans and the frequency of testing and reviewing these plans. However, it is clear that companies have become more concerned with having formal procedures to deal with security incidents and with having a formal, up-to-date business continuity plan.

4.5.5 Security budget

According to the DTI Information Security Breaches Survey (DTI 2006), spending the right amount on security continues to challenge UK companies. Some of the IT managers still find it difficult to justify the extra security spending to the board of directors. However, the rise in the number of security incidents year after year can be a main driver for the board of directors to give the security budget a priority in business budgets. In addition, Gordon and Loeb (2006) stated that until now little is known about the budgeting process used in deciding how much companies have to spend on security.

In order to investigate the priority given to the security budget in general and to the AIS security budget in particular, this section presents the questionnaire results on the existence of a separate security budget in UK companies, the percentage of security budget spent on AIS security, and the top areas of spending on AIS security. This section is concerned with testing Hypothesis 1.5 (Section 3.2.4 in Chapter 3). The hypothesis can be expressed as follows:

H1.5: There are no significant differences among UK companies in different industry sectors concerning the existence of a security budget and areas of spending on AIS security.

In order to test the hypothesis, respondents were asked three questions (Section 1.5 of the questionnaire). Question 1.5.1 was concerned with the existence of a separate security budget within UK companies. The second question asked respondents about the percentage of companies' security budget allocated to AIS security. Question 1.5.3 addressed the top areas of spending on AIS security.

Respondents were first asked whether their companies have a separate security budget (Question 1.5.1). It can be seen from Table 4.41 that only 29 percent of companies have a separate security budget, while 44 companies (71 percent) do not have a separate budget for security. This is not a surprising result, since the literature revealed that information security is still perceived to be an IT issue. According to the Global Security Survey (DTT 2007), most companies still do not have a security

budget separate from their IT budget. This result is investigated in more detail in Chapter 5.

Table 4.41 Cross-tabulation of the existence of a separate budget for security by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	4		0		3		2		1		4		4		18
%		22.2		0		16.7		11.1		5.6		22.2		22.2	
Industry %		36.4		0		50		16.7		16.7		50		44.4	
No	7		10		3		10		5		4		5		44
%		15.9		22.7		6.8		22.7		11.4		9.1		11.4	
Industry %		63.6		100		50		83.3		83.3		50		55.6	
Total	11		10		6		12		6		8		9		62

Q 1.5.1 Does your company have a separate budget for security?

Further analysis reveals that 50 percent of technology & telecommunications and media & entertainment companies have a separate security budget, followed by energy & utilities (44.4 percent), insurance & financial services (36.4 percent), property & construction, and retail merchandising (16.7 percent). Table 4.41 also reveals that all the respondents from manufacturing companies stated that they do not have a separate security budget. This implies that the security budget is included in the IT budget or in other budgets for most of the manufacturing companies in the UK.

Moreover, in order to test whether the existence of a separate security budget is related to the companies' industry sector, a chi-square test was conducted. However, the results do not reveal any significant association between the different industry sectors that responded and the existence of a separate security budget, given that $\chi^2 = 7.307$, df = 3, and p-value = 0.063 ($p > 0.05$).

This question was followed up by asking respondents, who stated that they have a separate security budget, about the percentage of the budget spent on AIS security in the last year (Question 1.5.2). Interestingly, Table 4.42 shows that one third of respondents stated that they do not know this percentage. This could be because these companies do not allocate a certain percentage of their security budget especially for AIS security; however, a part of their security budget is allocated to IS security in general. This result is also consistent with the results of the interviews and is further discussed in Chapter 5. In addition, the results reveal that one respondent stated that no allocation was made last year to AIS security, however, 38.9 percent of the

companies allocated 5 percent or less of their security budget to AIS security, and 22.2 percent allocated 6 percent or more of their security budget to AIS security.

Table 4.42 Cross-tabulation of the percentage of security budget spent on AIS security by industry sector

	Insurance & financial services		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no
None	0		1		0		0		0		0		1
%		0		100		0		0		0		0	
Industry %		0		33.3		0		0		0		0	
Less than 1%	0		0		1		0		1		1		3
%		0		0		33.3		0		33.3		33.3	
Industry %		0		0		50		0		25		25	
1% - 5%	1		0		0		0		1		2		4
%		25		0		0		0		25		50	
Industry %		25		0		0		0		25		50	
6% - 10%	0		0		1		0		1		0		2
%		0		0		50		0		50		0	
Industry %		0		0		50		0		25		0	
More than 20%	0		1		0		1		0		0		2
%		0		50		0		50		0		0	
Industry %		0		33.3		0		100		0		0	
Don't know	3		1		0		0		1		1		6
%		50		16.7		0		0		16.7		16.7	
Industry %		75		33.3		0		0		25		25	
Total	4		3		2		1		4		4		18

Q 1.5.2 If yes, approximately what percentage of your company's overall security budget was spent on AIS security in the last year?

Table 4.42 also reveals that 75 percent of respondents from the insurance & financial services sector do not know the percentage of security budget spent on AIS security in the last year, while only 25 percent stated that their companies spent one to five percent on AIS security. This is a surprising result given the nature of the insurance & financial services companies and their greater concern with AIS security. The results also show that the only respondent from retail merchandising sector stated that more than 20 percent of the company's security budget was spent on AIS. On the other hand, respondents who reported that their companies spent less than one percent on AIS security are from property & construction (50 percent), technology & telecommunications and energy & utilities (25 percent).

The last question in this section (Question 1.5.3) provided respondents with a list of different areas of spending on AIS security and asked them to rank the top three areas of spending within their companies.

Regarding the first area of spending on AIS security, Table 4.43 shows that 39.3 percent of respondents considered software security controls their first area of

spending on AIS security, followed by hardware and physical security controls (23.2 percent). On the other hand, 14.3 percent of respondents considered audit activities, compliance, and certification their first area of spending, followed by security staffing (10.7 percent) and incident response and business continuity (8.9 percent), whereas only 1.8 percent of companies considered security consultants and outsourcing, and employees' awareness and training their first area of spending on security.

A detailed analysis by industry sector shows that technology & telecommunications was the only sector that considered employees' awareness and training the first area of spending on security. This could be because the majority of companies find it difficult to justify their spending on this area or because most of the companies now are using their intranet to provide their employees with the relevant security training and awareness, which is not expensive. Table 4.43 also shows that the only respondent who considered security consultants and outsourcing the first area of security spending was from the manufacturing sector; however, software security controls, hardware and physical security controls were considered the first area of security spending by all the industry sectors that responded. This result is not surprising given the expensive nature of software and hardware security controls.

Table 4.44 shows the respondents' opinions regarding the second area of AIS security spending within their companies. The results reveal that 20 respondents considered hardware and physical security controls as their second area of security spending, followed by software security controls (27.3 percent), incident response and business continuity (12.7 percent). The results also reveal that 9.1 percent of companies considered security staffing their second area of security spending, followed by employees' awareness and training (7.3 percent), audit activities, compliance and certification (5.5 percent), while security consultants and outsourcing was considered by only one company as a second area of security spending.

Further analysis reveals that the only company that considered security consultants and outsourcing a second area of security spending was from the property & construction sector. In addition, retail merchandising and technology & telecommunications were the only sectors that considered audit activities, compliance, and certification their second area of security spending.

Table 4.43 Cross-tabulation of the first area of spending on AIS security by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Security staffing	2		0		1		0		0		1		2		6
%		33.3		0		16.7		0		0		16.7		33.3	
Industry %		20		0		16.7		0		0		14.3		25	
Security consultants/outsourcing	0		1		0		0		0		0		0		1
%		0		100		0		0		0		0		0	
Industry %		0		11.1		0		0		0		0		0	
Employees' awareness/training	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		14.3		0	
Software security controls	3		4		2		5		1		2		5		22
%		13.6		18.2		9.1		22.7		4.5		9.1		22.7	
Industry %		30		44.4		33.3		50		16.7		28.6		62.5	
Hardware & physical security controls	2		1		2		1		4		2		1		13
%		15.4		7.7		15.4		7.7		30.8		15.4		7.7	
Industry %		20		11.1		33.3		10		66.7		28.6		12.5	
Incidence response & business continuity	1		1		0		3		0		0		0		5
%		20		20		0		60		0		0		0	
Industry %		10		11.1		0		30		0		0		0	
Audit activities, compliance, certification	2		2		1		1		1		1		0		8
%		25		25		12.5		12.5		12.5		12.5		0	
Industry %		20		22.2		16.7		10		16.7		14.3		0	
Total	10		9		6		10		6		7		8		56

Q 1.5.3 Please rank your company's top 3 areas of spending on AIS security where 1 represents the most important.

Table 4.44 Cross-tabulation of the second area of spending on AIS security by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Security staffing	2		0		0		0		2		0		1		5
%		40		0		0		0		40		0		20	
Industry %		20		0		0		0		33.3		0		12.5	
Security consultants/outsourcing	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		11.1		0		0		0	
Employees' awareness/training	1		1		0		1		0		0		1		4
%		25		25		0		25		0		0		25	
Industry %		10		11.1		0		11.1		0		0		12.5	
Software security controls	2		4		2		2		2		1		2		15
%		13.3		26.7		13.3		13.3		13.3		6.7		13.3	
Industry %		20		44.4		33.3		22.2		33.3		14.3		25	
Hardware & physical security controls	3		3		3		4		0		3		4		20
%		15		15		15		20		0		15		20	
Industry %		30		33.3		50		44.4		0		42.9		50	
Incidence response & business continuity	2		1		1		1		1		1		0		7
%		28.6		14.3		14.3		14.3		14.3		14.3		0	
Industry %		20		11.1		16.7		11.1		16.7		14.3		0	
Audit activities, compliance, certification	0		0		0		0		1		2		0		3
%		0		0		0		0		33.3		66.7		0	
Industry %		0		0		0		0		16.7		28.6		0	
Total	**10**		**9**		**6**		**9**		**6**		**7**		**8**		**55**

Q 1.5.3 Please rank your company's top 3 areas of spending on AIS security where 1 represents the most important

Table 4.45 Cross-tabulation of the third area of spending on AIS security by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Security staffing	0		0		1		0		1		0		1		3
%		0		0		33.3		0		33.3		0		33.3	
Industry %		0		0		16.7		0		16.7		0		12.5	
Security consultants/outsourcing	1		1		1		0		0		1		0		4
%		25		25		25		0		0		25		0	
Industry %		12.5		11.1		16.7		0		0		16.7		0	
Employees' awareness/training	1		2		1		0		2		0		1		7
%		14.3		28.6		14.3		0		28.6		0		14.3	
Industry %		12.5		22.2		16.7		0		33.3		0		12.5	
Software security controls	2		0		2		2		2		1		0		9
%		22.2		0		22.2		22.2		22.2		11.1		0	
Industry %		25		0		33.3		25		33.3		16.7		0	
Hardware & physical security controls	4		4		0		1		0		0		0		9
%		44.4		44.4		0		11.1		0		0		0	
Industry %		50		44.4		0		12.5		0		0		0	
Incidence response & business continuity	0		0		0		1		0		3		4		8
%		0		0		0		12.5		0		37.5		50	
Industry %		0		0		0		12.5		0		50		50	
Audit activities, compliance, certification	0		2		1		4		1		1		2		11
%		0		18.2		9.1		36.4		9.1		9.1		18.2	
Industry %		0		22.2		16.7		50		16.7		16.7		25	
Total	8		9		6		8		6		6		8		51

Q 1.5.3 Please rank your company's top 3 areas of spending on AIS security where 1 represents the most important.

Table 4.44 also shows that all sectors except retail merchandising saw hardware and physical security controls as their second area of spending. This could be because two thirds of respondents from this sector considered hardware and physical security controls their first area of spending. At the same time, all sectors considered software security controls as a second area of spending. This result again implies that software security controls, hardware and physical security controls are the most expensive controls for almost all industry sectors that responded.

Regarding the third area of spending on AIS security, Table 4.45 shows that 21.6 percent of respondents considered audit activities, compliance, and certification their third area of security spending, followed by software security controls, and hardware and physical security controls (17.6 percent). The results also reveal that 15.7 percent of respondents identified incident response and business continuity as their third area of security spending, followed by employees' awareness and training (13.7 percent), security consultants and outsourcing (7.8 percent), and security staffing (5.9 percent).

Further analysis shows that audit activities, compliance, and certification were considered by all sectors as their third area of security spending except by the insurance & financial services. This could be because 20 percent of insurance & financial services companies considered it as their first area of security spending; however, the other respondents from this sector did not consider it their second or third area of spending. The results also reveal that all sectors except manufacturing and energy & utilities identified software security controls as their third area of security spending. The reason could be because 50 percent of respondents from both sectors considered software security controls to be their first area of spending and the other 50 percent saw it as their second area of spending.

Table 4.45 also shows that all sectors except property & construction and technology & telecommunications considered employees' awareness and training their third area of security spending. The reason is that all technology & telecommunications companies considered it their first area of spending, while only 11.1 percent of property & construction put it in second place. This is not surprising since according to the results in Section 4.5.2, the property & construction companies are the least

likely to provide their managers, employees and other users with the relevant security training (Tables 4.14, 4.15, and 4.16).

It is clear from the above results that the majority of companies that responded considered software security controls, hardware and physical security controls, and audit activities, compliance and certification as their top areas of AIS security spending. This result is further verified by calculating the weighted score of each area of spending. This method was used in previous studies such as Loch *et al.* (1992) and Whitman (2003) to rank the top threats to information and IS security. The weighted scores were calculated by assigning 3 points for the first place ranking, 2 for the second place ranking, and 1 for the third. These ranks were then added for each area of spending.

Table 4.46 shows that software security controls took the highest weighted score (105) which indicate that it was considered as the first area of security spending within UK companies. The results also show that hardware and physical security controls took the next highest weighted score (88), followed by audit activities, compliance and certification with a weighted score of 41. On the other hand, security consultants and outsourcing took the lowest weighted score (9). This result suggests that most companies are not depending much on external security consultants or service providers. This issue is further investigated in Chapter 5.

Table 4.46 Weighted scores of the number of times areas of spending on AIS security were selected by respondents

Areas of spending on AIS security	Number of times selected			Weighted scores
	First area of spending	Second area of spending	Third area of spending	
Security staffing	6	5	3	31
Security consultants/outsourcing	1	1	4	9
Employees' awareness and training	1	4	7	18
Software security controls	22	15	9	105
Hardware and physical security controls	13	20	9	88
Incident response and business continuity	5	7	8	37
Audit activities, compliance and certification	8	3	11	41

In order to test Hypothesis 1.5 and to examine whether the top areas of spending differ among industry sectors, the Kruskal-Wallis test was conducted. The results

(Table 4.47) did not indicate any statistically significant differences, at 0.05 level, in the distribution of responses among the industry sectors except for the hardware and physical security controls.

Table 4.47 Results of Kruskal-Wallis test regarding the areas of spending on AIS security

Areas of spending on AIS security	Industry sectors	N	Mean Rank
Security staffing	Insurance & financial services	4	6.25
	Manufacturing	-	-
	Media & entertainment	2	8.25
	Property & construction	-	-
	Retail merchandising	3	10.33
	Technology & telecommunications	1	3.50
	Energy & utilities	4	7.25
Chi-square value (χ^2) = 3.132, df = 4, and p-value = 0.536			
Security consultants/outsourcing	Insurance & financial services	1	4.50
	Manufacturing	2	2.75
	Media & entertainment	1	4.50
	Property & construction	1	2
	Retail merchandising	-	-
	Technology & telecommunications	1	4.50
	Energy & utilities	-	-
Chi-square value (χ^2) = 2.550, df = 4 and p-value = 0.636			
Employees' awareness and training	Insurance & financial services	2	6.25
	Manufacturing	3	7.17
	Media & entertainment	1	9
	Property & construction	1	3.50
	Retail merchandising	2	9
	Technology & telecommunications	1	1
	Energy & utilities	2	6.25
Chi-square value (χ^2) = 5.958, df = 6, and p-value = 0.428			
Software security controls	Insurance & financial services	7	25.50
	Manufacturing	8	20.75
	Media & entertainment	6	27.83
	Property & construction	9	22.39
	Retail merchandising	5	31.10
	Technology & telecommunications	4	23.75
	Energy & utilities	7	16.79
Chi-square value (χ^2) = 5.342, df = 6, and p-value = 0.501			
Hardware and physical security controls	Insurance & financial services	9	26.28
	Manufacturing	8	28.69
	Media & entertainment	5	16.90
	Property & construction	6	23.17
	Retail merchandising	4	7
	Technology & telecommunications	5	16.90
	Energy & utilities	5	20.20
Chi-square value (χ^2) = 13.214, df = 6, and p-value = 0.040			
Incident response and business continuity	Insurance & financial services	3	7
	Manufacturing	2	6
	Media & entertainment	1	9
	Property & construction	5	6.90
	Retail merchandising	1	9
	Technology & telecommunications	4	14.63
	Energy & utilities	4	16.50
Chi-square value (χ^2) = 11.647, df = 6, and p-value = 0.070			
Audit activities, compliance and certification	Insurance & financial services	2	4.50
	Manufacturing	4	10.75
	Media & entertainment	2	10.75
	Property & construction	5	14.50
	Retail merchandising	3	10.50
	Technology & telecommunications	4	10.38
	Energy & utilities	2	17
Chi-square value (χ^2) = 6.170, df = 6, and p-value = 0.404			

This result implies that there are significant differences, at 0.05 level, in the distribution of responses among industry sectors regarding the hardware and physical security controls, given that p-value is 0.040 ($p < 0.05$). On the other hand, there are no significant differences, at the 0.05 level, in the distribution of responses among industry sectors regarding the other areas of security spending, given that their p-values are 0.536, 0.636, 0.428, 0.501, 0.070, and 0.404 respectively.

Overall, the responses to the questions in this section indicate that there are no significant differences among companies in different industry sectors regarding the existence of a separate budget for security, and the top areas of security spending except for the hardware and physical security controls. This indicates that some sectors that responded are depending on hardware and physical security controls and are spending more on them than the other sectors. This result is further investigated in Section 4.7.

4.5.6 Security standards and certification

The British Standard BS 7799 (ISO 27000) is now one of the most prominent international efforts on information security (Ma and Pearson 2005). Many authors claimed the importance of this standard. Dodds and Hague (2004) argued that ISO 17799 assists in formalising an information systems security framework, which enables companies to take an enterprise-wide, top-down approach to IS security, thus aligning security and its consequent investment to the company's needs. Saleh *et al.* (2007) stated that this standard provides a wide range of information security protection controls, and provides a safe environment to e-services at the internal intranet level, the business extranet level, and the public internet level.

In addition, the DTI Information Security Breaches Survey (DTI 2006) indicated that the majority of the businesses believe that BS 7799 can raise staff awareness and can push security higher up the management agenda. Most recently, the BERR Information Security Breaches Survey (BERR 2008) stated that the implementation of the standard tends to raise the security baseline by ensuring that a minimum level of control is adopted in all areas of security management. It also strengthens companies' processes in checking compliance with their security policies.

Due to the importance and popularity of the British Standard BS 7799, this section is concerned with the respondents' awareness level of its two parts, the awareness level of the other managers and employees in their companies of the standard, and the certification under ISO 27001. This section is concerned with testing Hypothesis 1.6 (Section 3.2.4 in Chapter 3). The hypothesis can be expressed as follows:

H1.6: There are no significant differences among UK companies in different industry sectors concerning the awareness level of the British Standard for Information Security Management BS 7799 and the certification under ISO 27001.

In order to test this hypothesis, respondents were asked three questions (Section 1.6 of the questionnaire). Question 1.6.1 asked respondents about their awareness level of the two parts of the British Standard BS 7799, while the second question asked respondents about the overall awareness level of the other managers and employees in their companies with the standard. In addition, Question 1.6.3 asked respondents whether their companies are certified under ISO 27001, are planning to be certified, or have no plans for certification.

Table 4.48 Cross-tabulation of respondents' awareness level of part 1 of BS 7799 by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Low	4		6		2		5		3		3		2		25
%		16		24		8		20		12		12		8	
Industry %		36.4		60		33.3		41.7		42.9		37.5		22.2	
Moderate	1		2		1		6		3		3		1		17
%		5.9		11.8		5.9		35.3		17.6		17.6		5.9	
Industry %		9.1		20		16.7		50		42.9		37.5		11.1	
High	6		2		3		1		1		2		6		21
%		28.6		9.5		14.3		4.8		4.8		9.5		28.6	
Industry %		54.5		20		50		8.3		14.3		25		66.7	
Total	11		10		6		12		7		8		9		63

Q 1.6.1 Please indicate your awareness level of the British Standard for Information Security Management BS 7799: Part 1: Code of Practice for Information Security Management.

Regarding the respondents' awareness of the two parts of the British Standard, the results in Tables 4.48 and 4.49 illustrate that the respondents are not sufficiently aware of the two parts of BS 7799. One third of respondents (33.3 percent) stated that their awareness level of part 1 of the standard is high, whereas only 23.8 percent had the same opinion regarding part 2. On the other hand, 39.7 percent of respondents reported that their awareness level is low for part 1 (Code of Practice) of the standard and 47.6 percent had the same opinion for part 2 (Certification). This is a surprising

result given that the respondents are IT managers and the people responsible for security in their companies. However, this result is consistent with the results of the follow-up interviews (Chapter 5).

Table 4.49 Cross-tabulation of respondents' awareness level of part 2 of BS 7799 by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Low	5		9		3		5		3		3		2		30
%		16.7		30		10		16.7		10		10		6.7	
Industry %		45.5		90		50		41.7		42.9		37.5		22.2	
Moderate	1		0		1		6		3		4		3		18
%		5.6		0		5.6		33.3		16.7		22.2		16.7	
Industry %		9.1		0		16.7		50		42.9		50		33.3	
High	5		1		2		1		1		1		4		15
%		33.3		6.7		13.3		6.7		6.7		6.7		26.7	
Industry %		45.5		10		33.3		8.3		14.3		12.5		44.4	
Total	11		10		6		12		7		8		9		63

Q 1.6.1 Please indicate your awareness level of the British Standard for Information Security Management BS 7799: Part 2: Security Techniques: Information Security Management Systems.

When the responses were analysed by industry sector, Table 4.48 shows that the highest percentage of respondents who have a high level of awareness of part 1 of the standard were from energy & utilities sector (66.7 percent), they were followed by insurance & financial services (54.5 percent), and media & entertainment (50 percent), whereas the other sectors expressed a low level of awareness. Three fifths of respondents from the manufacturing sector, 42.9 percent from retail merchandising, 41.7 percent from property & construction, and 37.5 percent from technology & telecommunications have low awareness of the first part of the standard.

Regarding part 2 of the standard, the results in Table 4.49 show that the highest percentage of respondents who expressed a high level of awareness of the second part of the standard were from the insurance & financial services sector (45.5 percent), followed by energy & utilities (44.4 percent), and media & entertainment (33.3 percent). On the other hand, the other sectors expressed a low level of awareness of the second part. The results show that 90 percent of respondents from the manufacturing sector stated that their awareness level of the second part of the standard is low, followed by retail merchandising (42.9 percent), property & construction (41.7 percent), and technology & telecommunications (37.5 percent).

The responses to this question, therefore, suggest that the awareness level is moderate in the insurance & financial services, energy & utilities, and media & entertainment sectors, whereas it is weak in technology & telecommunications and very weak in the manufacturing, retail merchandising, and property & construction sectors. These results are consistent with the results of the DTI Information Security Breaches Survey (DTI 2006) which indicated that the penetration of BS 7799 into UK companies remains disappointing, and that among people responsible for information security in their companies, only one in ten is aware of its contents.

Respondents were then asked about the overall awareness of the other managers and employees in their companies regarding the British Standard BS 7799. Interestingly, the majority of the other managers and employees had only low awareness of the British Standard.

Table 4.50 Cross-tabulation of managers' awareness level of the BS 7799 by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Low	6		10		4		9		5		7		5		46
%		13		21.7		8.7		19.6		10.9		15.2		10.9	
Industry %		54.5		100		66.7		75		71.4		87.5		55.6	
Moderate	5		0		1		3		1		0		4		14
%		35.7		0		7.1		21.4		7.1		0		28.6	
Industry %		45.5		0		16.7		25		14.3		0		44.4	
High	0		0		1		0		1		1		0		3
%		0		0		33.3		0		33.3		33.3		0	
Industry %		0		0		16.7		0		14.3		12.5		0	
Total	11		10		6		12		7		8		9		63

Q 1.6.2 In your opinion, what is the overall awareness level of your company's managers regarding the British Standard BS 7799?

Table 4.51 Cross-tabulation of employees' awareness level of the BS 7799 by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Low	11		10		5		12		6		7		8		59
%		18.6		16.9		8.5		20.3		10.2		11.9		13.6	
Industry %		100		100		83.3		100		85.7		87.5		88.9	
Moderate	0		0		1		0		1		1		1		4
%		0		0		25		0		25		25		25	
Industry %		0		0		16.7		0		14.3		12.5		11.1	
Total	11		10		6		12		7		8		9		63

Q 1.6.2 In your opinion, what is the overall awareness level of your company's employees regarding the British Standard BS 7799?

The results in Tables 4.50 and 4.51 show that 46 of the respondents (73 percent) indicated that managers' awareness level of the standard is low, while 93.7 percent

had the same opinion regarding employees in their companies. In addition, it is clear from Table 4.51 that no one stated that employees' awareness in their companies is high. This is not a surprising result, given that the people responsible for security have a low level of awareness of the standard.

Further analysis (Table 4.50) reveals that the majority of respondents stated that managers in their companies have low awareness of the British Standard. All respondents from the manufacturing sector confirmed their managers' low awareness of the standard, followed by technology & telecommunications (87.5 percent), property & construction (75 percent), retail merchandising (71.4 percent), media & entertainment (66.7 percent), energy & utilities (55.6 percent), and insurance & financial services (54.5 percent).

Regarding the employees, it is not surprising to see from Table 4.51 that out of the 63 respondents, no one indicated that the awareness level of the employees is high. In addition, all respondents from insurance & financial services, manufacturing, and property & construction indicated that employees' awareness level is low, followed by energy & utilities (88.9 percent), technology & telecommunications (87.5 percent), retail merchandising (85.7 percent), and media & entertainment (83.3 percent).

Furthermore, when these results were analysed in conjunction with the results in Table 4.6 (Section 4.4), given that only 10.8 percent of respondents have a professional security qualification, the results suggest that the awareness level of the British Standard is high among respondents who have a professional security qualification. These results are consistent with the results of the BERR Information Security Breaches Survey (BERR 2008).

In addition, in order to test the hypothesis and to examine whether the awareness level of the British Standard differs among industry sectors, the Kruskal-Wallis test was conducted. The results (Table 4.52) strongly support Hypothesis 1.6, given that p-values are 0.286 for respondents' awareness of part 1 of the standard, 0.177 for respondents' awareness of part 2, 0.323 for managers' awareness of the standard, and 0.566 for employees' awareness. The results, therefore, reveal that no statistically significant differences exist, at the 0.05 level, among different industry sectors

regarding the awareness level of the British Standard among managers and employees of the companies that responded. These results will be investigated in more detail when the interviews are analysed (Chapter 5).

Table 4.52 Results of Kruskal-Wallis test regarding the awareness level of the British Standard BS 7799

Awareness level of the British Standard BS 7799	Industry sectors	N	Mean Rank
Respondents' awareness level of part 1 of BS 7799	Insurance & financial services	11	36.73
	Manufacturing	10	25.20
	Media & entertainment	6	36.50
	Property & construction	12	26.83
	Retail merchandising	7	27.71
	Technology & telecommunications	8	30.88
	Energy & utilities	9	42
Chi-square value (χ^2) = 7.394, df = 6, and p-value = 0.286			
Respondents' awareness level of part 2 of BS 7799	Insurance & financial services	11	36.09
	Manufacturing	10	19.55
	Media & entertainment	6	33
	Property & construction	12	30.88
	Retail merchandising	7	31.57
	Technology & telecommunications	8	32.56
	Energy & utilities	9	41.50
Chi-square value (χ^2) = 8.946, df = 6, and p-value = 0.177			
Managers' awareness level of the British Standard BS 7799	Insurance & financial services	11	37.14
	Manufacturing	10	23.50
	Media & entertainment	6	34.92
	Property & construction	12	31
	Retail merchandising	7	33.29
	Technology & telecommunications	8	28.31
	Energy & utilities	9	36.83
Chi-square value (χ^2) = 6.978, df = 6, and p-value = 0.323			
Employees' awareness level of the British Standard BS 7799	Insurance & financial services	11	30
	Manufacturing	10	30
	Media & entertainment	6	35.25
	Property & construction	12	30
	Retail merchandising	7	34.50
	Technology & telecommunications	8	33.94
	Energy & utilities	9	33.50
Chi-square value (χ^2) = 4.827, df = 6, and p-value = 0.566			

The final question in this section asked respondents whether their companies are certified, are planning to be certified, or have no plans to be certified under ISO 27001. It is not surprising to see from Table 4.53 that only two companies (3.6 percent) are certified under ISO 27001. The results also show that 12.7 percent of companies are not certified, but they are planning to be so, while 83.6 percent of companies responding are not certified, and are not planning to be certified under ISO 27001. This is not a surprising result, given that 76.2 percent of respondents stated that their awareness level of part 2 of the standard, against which companies seek certification, is moderate or low (Table 4.49).

Table 4.53 Cross-tabulation of the certification under ISO/IEC 27001 by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & Utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	0		0		0		0		0		1		1		2
%		0		0		0		0		0		50		50	
Industry %		0		0		0		0		0		14.3		11.1	
No, but plans to	0		1		0		2		0		1		3		7
%		0		14.3		0		28.6		0		14.3		42.9	
Industry %		0		10		0		20		0		14.3		33.3	
No, and no plans to	10		9		4		8		5		5		5		46
%		21.7		19.6		8.7		17.4		10.9		10.9		10.9	
Industry %		100		90		100		80		100		71.4		55.6	
Total	10		10		4		10		5		7		9		55

Q 1.6.3 Has your company become certified under the ISO/IEC 27001 Information Security Management Systems Standard?

Further analysis reveals that the only two respondents who stated that their companies are certified under ISO 27001 are from technology & telecommunications, and energy & utilities, whereas all respondents from insurance & financial services, media & entertainment, and retail merchandising sectors stated that their companies are not certified, and are not planning to do so. Despite the benefits of being certified under ISO 27001 (Section 2.4.8.8 in Chapter 2), these results indicate that, in practice, many companies believe that preparing for this certification is a comprehensive and time-consuming effort. In addition, even some of the companies which are already certified under ISO 27001 cannot see sufficient benefit from this. These opinions are further investigated in the interviews' analysis.

Moreover, in order to test whether certification under ISO 27001 differs among different industry sectors, a chi-square test was conducted. The results do not indicate any significant association between the industry sectors that responded and the certification under ISO 27001, given that, $\chi^2 = 7.543$, df = 6, and p-value = 0.274 ($p > 0.05$).

Overall, the responses in this section provide strong support for Hypothesis 1.6. The results, therefore, indicate that there are no statistically significant differences among the different sectors concerning the awareness level of the British Standard and the certification under ISO 27001.

4.5.7 AIS security effectiveness

It was mentioned in Section 2.4.8.9 in Chapter 2 that measuring security effectiveness eases the process of monitoring the effectiveness of the security management system, reduces the number of security incidents, and provides tangible evidence to auditors and assurance to senior management that a company is in control (Wright 2006). On the other hand, information security practitioners are facing a major problem, in that nothing happens when they do their jobs well. It is, therefore, necessary to quantify the benefits provided to the company from doing their jobs efficiently.

In order to evaluate the effectiveness level of AIS security management, this section presents the questionnaire results on the different techniques used by UK companies to evaluate AIS security effectiveness, the top success indicators of AIS security management, and the IT managers' opinions regarding the effectiveness level of AIS security management in their companies. This section is concerned with testing Hypothesis 1.7 (Section 3.2.4 in Chapter 3). This hypothesis can be expressed as follows:

H1.7: There are no significant differences among UK companies in different industry sectors concerning the techniques used to evaluate AIS security effectiveness, the success indicators of AIS security management, and the effectiveness level of AIS security management.

In order to test this hypothesis, respondents were asked three questions (Section 1.7 of the questionnaire). Question 1.7.1 addressed the techniques used to evaluate AIS security effectiveness within UK companies. The second question provided respondents with a list of the success indicators of AIS security management, and asked them to rank the top three indicators, while in Question 1.7.3, respondents were asked to indicate the effectiveness level of AIS security management within their companies on a scale ranging from "not effective at all" to "extremely effective".

In Question 1.7.1, respondents were given a list of techniques used to evaluate AIS security effectiveness, and were asked to select all the techniques used within their companies. Table 4.54 shows that the majority of companies that responded (81.7 percent) are undertaking internal audits of security procedures to evaluate the

effectiveness of their AIS security. In addition, three fourths of companies are undertaking external security audits and network monitoring in evaluating AIS security effectiveness, followed by penetration testing (61.7 percent), and vulnerability scanning (33.3 percent).

Table 4.54 Techniques used by companies to evaluate AIS security effectiveness

Techniques used to evaluate effectiveness of AIS security	Technique used		Technique not used		Total
	no	%	no	%	
External security audits	45	75	15	25	60
Internal audits of security procedures	49	81.7	11	18.3	60
Penetration testing	37	61.7	23	38.3	60
Network monitoring software	45	75	15	25	60
Vulnerability scanners	20	33.3	40	66.7	60

Q 1.7.1 Please indicate the techniques used by your company to evaluate the effectiveness of AIS security.

The results, therefore, suggest that the majority of companies depend on external and internal security audits to evaluate AIS security effectiveness. These results are consistent with the CSI Survey (Richardson 2007), which indicated that "security audits" is the most popular technique in the evaluation of security effectiveness.

Further analysis reveals that the five techniques are used by nearly all the industry sectors that responded. Regarding external security audits, Table 4.55 shows that 87.5 percent of technology & telecommunications companies use this technique in evaluating AIS security effectiveness, followed by retail merchandising (85.7 percent), media & entertainment (83.3 percent), manufacturing (75 percent), insurance & financial services (70 percent), property & construction, and energy & utilities (66.7 percent).

Table 4.55 Cross-tabulation of the techniques used by companies to evaluate AIS security effectiveness by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	
External security audits	7	3	6	2	5	1	8	4	6	1	7	1	6	3	60
Internal audits of security procedures	8	2	6	2	5	1	7	5	7	0	8	0	8	1	60
Penetration testing	7	3	3	5	5	1	6	6	5	2	4	4	7	2	60
Network monitoring software	9	1	5	3	6	0	9	3	6	1	5	3	5	4	60
Vulnerability scanners	5	5	1	7	2	4	2	10	5	2	3	5	2	7	60

Note: Yes = Technique used, and No = Technique not used

Table 4.55 shows that all companies from retail merchandising and technology & telecommunications undertake internal audits of security procedures in evaluating AIS security effectiveness whereas only 58.3 percent from property & construction use the same technique. In addition, 83.3 percent of media & entertainment companies undertake penetration testing in evaluating AIS security effectiveness, followed by energy & utilities (77.8 percent), while only 37.5 percent of manufacturing companies use it.

Table 4.55 also reveals that all companies from the media & entertainment sector use network monitoring software to evaluate AIS security effectiveness, whereas only 55.6 percent of energy & utilities do the same. The results also reveal that "vulnerability scanners" is the least common technique used to evaluate AIS security effectiveness. Table 4.55 shows that 71.4 percent of respondents from retail merchandising companies use this technique, followed by insurance & financial services (50 percent), technology & telecommunications (37.5 percent), and media & entertainment (33.3 percent), with only 12.5 percent of manufacturing companies using this technique.

The results, therefore, suggest that the most common technique used is "internal audits of security procedures", while the least common technique used is "vulnerability scanners". Moreover, in order to test whether the techniques used to evaluate AIS security differ among industry sectors, a chi-square test was conducted. The results in Table 4.56 provide no evidence of any statistically significant association, at the 0.05 level, between the different industry sectors and the techniques used to evaluate AIS security effectiveness in UK companies, given that their p-values are 0.579, 0.406, 0.855, 0.553, and 0.319 respectively.

Table 4.56 Results of chi-square test for the techniques used to evaluate AIS security effectiveness

Techniques used to evaluate effectiveness of AIS security	χ^2	df	p-value
External security audits	1.968	3	0.579
Internal audits of security procedures	2.910	3	0.406
Penetration testing	0.776	3	0.855
Network monitoring software	2.095	3	0.553
Vulnerability scanners	3.514	3	0.319

Respondents were then given a list of success indicators of AIS security management and were asked to rank the top three indicators from their point of view. Regarding

the first success indicator, Table 4.57 shows that 41.8 percent of companies considered "successful defences against AIS security attacks" their first success indicator, followed by "information security assurance" (25.5 percent), and "increased ability to recover from disasters" (18.2 percent). On the other hand, 7.3 percent of companies considered "reduction in frequency of AIS security incidents" their first success indicator, followed by "reduction in internal policy breaking" (5.5 percent), and only one respondent chose "increased budget for AIS security". The results, therefore, indicate that the majority of companies considered "successful defences against AIS security attacks" their first success indicator of AIS security management, while almost no companies saw "increased budget for AIS security" as a success indicator.

Further analysis by industry sector (Table 4.57) reveals that the only two indicators that were selected by respondents from all industry sectors as their first success indicator of security management are "information security assurance" and "successful defences against AIS security attacks". On the other hand, the increased ability to recover from disasters was selected by respondents from all industry sectors except media & entertainment.

The results also reveal that respondents from only the property & construction, and energy & utilities sectors considered the reduction in internal policy breaking as the first success indicator, while the only respondent who selected the increased budget for AIS security as the first success indicator was from the property & construction sector.

The respondents' opinions regarding the second success indicator of AIS security management are presented in Table 4.58. The results reveal that "increased ability to recover from disasters" was selected by 29.6 percent of respondents as their second success indicator, followed by information security assurance (20.4 percent), reduction in internal policy breaking, and reduction in frequency of AIS security incidents (16.7 percent), and successful defences against security attacks (14.8 percent). On the other hand, only one respondent selected the increased budget for AIS security as the second success indicator. It is clear from the results that the

majority of companies that responded do not consider an increased budget for AIS security as a success indicator of security management.

In addition, analysis by industry sector (Table 4.58) reveals that the increased ability to recover from disasters was selected by respondents from all industry sectors, reduction in internal policy breaking was considered as the second success indicator by all sectors except energy & utilities, while all sectors except manufacturing selected successful defences against security attacks. The results also show that the only respondent who considered an increased budget for AIS security as a second success indicator was from the manufacturing sector.

Regarding the third success indicator of AIS security management, Table 4.59 shows that 24.1 percent of companies selected the reduction in frequency of AIS security incidents, followed by information security assurance and increased ability to recover from disasters (22.2 percent). On the other hand, 16.7 percent selected the reduction in internal policy breaking, followed by successful defences against security attacks (14.8 percent). Interestingly, it can be seen from Table 4.59 that the increased budget for AIS security was not selected by any respondent as a third success indicator.

Further analysis by industry sector (Table 4.59) reveals that again the increased ability to recover from disasters was selected by companies from all industry sectors as their third success indicator of AIS security management, which indicates its importance as a success indicator for most companies. In addition, information security assurance was selected by respondents from all sectors except media & entertainment, and the reduction in internal policy breaking was not selected by property & construction.

Table 4.57 Cross-tabulation of the first success indicator of AIS security management by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Information security assurance	3		2		2		1		1		2		3		14
%		21.4		14.3		14.3		7.1		7.1		14.3		21.4	
Industry %		30		25		33.3		12.5		16.7		25		33.3	
Reduction in internal policy breaking	0		0		0		2		0		0		1		3
%		0		0		0		66.7		0		0		33.3	
Industry %		0		0		0		25		0		0		11.1	
Reduction of frequency of security incidents	1		2		1		0		0		0		0		4
%		25		50		25		0		0		0		0	
Industry %		10		25		16.7		0		0		0		0	
Increased ability to recover from disasters	1		1		0		1		3		3		1		10
%		10		10		0		10		30		30		10	
Industry %		10		12.5		0		12.5		50		37.5		11.1	
Successful defences against security attacks	5		3		3		3		2		3		4		23
%		21.7		13		13		13		8.7		13		17.4	
Industry %		50		37.5		50		37.5		33.3		37.5		44.4	
Increased budget for AIS security	0		0		0		1		0		0		0		1
%		0		0		0		100		0		0		0	
Industry %		0		0		0		12.5		0		0		0	
Total	10		8		6		8		6		8		9		55

Q 1.7.2 Please rank the top 3 critical success indicators of the AIS security management within your company where 1 represents the most important.

Table 4.58 Cross-tabulation of the second success indicator of AIS security management by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Information security assurance	4		0		1		3		0		1		2		11
%		36.4		0		9.1		27.3		0		9.1		18.2	
Industry %		40		0		16.7		37.5		0		14.3		22.2	
Reduction in internal policy breaking	1		3		1		1		1		2		0		9
%		11.1		33.3		11.1		11.1		11.1		22.2		0	
Industry %		10		37.5		16.7		12.5		16.7		28.6		0	
Reduction of frequency of security incidents	0		1		2		0		3		1		2		9
%		0		11.1		22.2		0		33.3		11.1		22.2	
Industry %		0		12.5		33.3		0		50		14.3		22.2	
Increased ability to recover from disasters	4		3		1		3		1		1		3		16
%		25		18.8		6.3		18.8		6.3		6.3		18.8	
Industry %		40		37.5		16.7		37.5		16.7		14.3		33.3	
Successful defences against security attacks	1		0		1		1		1		2		2		8
%		12.5		0		12.5		12.5		12.5		25		25	
Industry %		10		0		16.7		12.5		16.7		28.6		22.2	
Increased budget for AIS security	0		1		0		0		0		0		0		1
%		0		100		0		0		0		0		0	
Industry %		0		12.5		0		0		0		0		0	
Total	10		8		6		8		6		7		9		54

Q 1.7.2 Please rank the top 3 critical success indicators of the AIS security management within your company where 1 represents the most important.

Table 4.59 Cross-tabulation of the third success indicator of AIS security management by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Information security assurance	1		2		0		2		2		2		3		12
%		8.3		16.7		0		16.7		16.7		16.7		25	
Industry %		10		25		0		25		33.3		28.6		33.3	
Reduction in internal policy breaking	2		1		1		0		2		1		2		9
%		22.2		11.1		11.1		0		22.2		11.1		22.2	
Industry %		20		12.5		16.7		0		33.3		14.3		22.2	
Reduction of frequency of security incidents	4		1		1		4		0		2		1		13
%		30.8		7.7		7.7		30.8		0		15.4		7.7	
Industry %		40		12.5		16.7		50		0		28.6		11.1	
Increased ability to recover from disasters	1		2		2		1		2		2		2		12
%		8.3		16.7		16.7		8.3		16.7		16.7		16.7	
Industry %		10		25		33.3		12.5		33.3		28.6		22.2	
Successful defences against security attacks	2		2		2		1		0		0		1		8
%		25		25		25		12.5		0		0		12.5	
Industry %		20		25		33.3		12.5		0		0		11.1	
Total	10		8		6		8		6		7		9		54

Q 1.7.2 Please rank the top 3 critical success indicators of the AIS security management within your company where 1 represents the most important.

It is clear from the results that the most common success indicators of AIS security management among companies that responded are the successful defences against security attacks, information security assurance, and the increased ability to recover from disasters, whereas an increased budget for AIS security is the least common success indicator. These results could be because 71 percent of companies (Table 4.41) do not have a separate security budget, and those who have, do not allocate a specific amount of this budget for AIS security.

Table 4.60 Weighted scores of the number of times success indicators of AIS security management were selected by respondents

Success indicators of AIS security management	Number of times selected			Weighted scores
	First success indicator	Second success indicator	Third success indicator	
Information security assurance	14	11	12	76
Reduction in internal policy breaking	3	9	9	36
Reduction in frequency of AIS security incidents	4	9	13	43
Increased ability to recover from disasters	10	16	12	74
Successful defences against AIS security attacks	23	8	8	93
Increased budget for AIS security	1	1	0	5

This result was further verified by calculating the weighted score for each success indicator of AIS security management. Table 4.60 shows that successful defences against AIS security attacks achieved the highest weighted score (93), which indicates its importance as the first success indicator within UK companies. The results also reveal that information security assurance achieved the next highest weighted score (76), followed by the increased ability to recover from disasters, which achieved a weighted score of 74, whereas the increased budget for AIS security achieved the lowest score (5). These results indicate that the majority of companies that responded do not consider an increased AIS security budget as a success indicator of their security management.

Furthermore, in order to examine whether the success indicators differ among the industry sectors that responded, a Kruskal-Wallis test was conducted. The results (Table 4.61) do not indicate any statistically significant differences, at the 0.05 level, in the distribution of responses among industry sectors for the six success indicators of AIS security management, given that their p-values are 0.806, 0.369, 0.164, 0.792, 0.991, and 0.317 respectively.

Table 4.61 Results of Kruskal-Wallis test regarding the success indicators of AIS security management

Success indicators of AIS security management	Industry sectors	N	Mean Rank
Information security assurance	Insurance & financial services	8	16.75
	Manufacturing	4	19.50
	Media & entertainment	3	11.67
	Property & construction	6	21.75
	Retail merchandising	3	23.50
	Technology & telecommunications	5	19.60
	Energy & utilities	8	19.63
Chi-square value (χ^2) = 3.023, df = 6, and p-value = 0.806			
Reduction in internal policy breaking	Insurance & financial services	3	14
	Manufacturing	4	10.25
	Media & entertainment	2	12.50
	Property & construction	3	4
	Retail merchandising	3	14
	Technology & telecommunications	3	11
	Energy & utilities	3	12
Chi-square value (χ^2) = 6.505, df = 6 and p-value = 0.369			
Reduction in frequency of AIS security incidents	Insurance & financial services	5	16.50
	Manufacturing	4	8.50
	Media & entertainment	4	10.13
	Property & construction	4	20
	Retail merchandising	3	9
	Technology & telecommunications	3	16.33
	Energy & utilities	3	12.67
Chi-square value (χ^2) = 9.183, df = 6, and p-value = 0.164			
Increased ability to recover from disasters	Insurance & financial services	6	18.67
	Manufacturing	6	21
	Media & entertainment	3	27.83
	Property & construction	5	18.70
	Retail merchandising	6	16.67
	Technology & telecommunications	6	16.67
	Energy & utilities	6	21
Chi-square value (χ^2) = 3.133, df = 6, and p-value = 0.792			
Successful defences against AIS security attacks	Insurance & financial services	8	19.81
	Manufacturing	5	21.40
	Media & entertainment	6	22.42
	Property & construction	5	19.80
	Retail merchandising	3	17.17
	Technology & telecommunications	5	18.20
	Energy & utilities	7	19.79
Chi-square value (χ^2) = 0.849, df = 6, and p-value = 0.991			
Increased budget for AIS security	Insurance & financial services	-	-
	Manufacturing	1	2
	Media & entertainment	-	-
	Property & construction	1	1
	Retail merchandising	-	-
	Technology & telecommunications	-	-
	Energy & utilities	-	-
Chi-square value (χ^2) = 1.000, df = 1, and p-value = 0.317			

The last question in this section asked respondents about their opinions regarding the effectiveness level of AIS security management within their companies. The results presented in Table 4.62 reveal that 60 percent of respondents believed that AIS security management is somewhat effective, while 23.3 percent believed that it is extremely effective. On the other hand, 5 percent of respondents believed that AIS security management is somewhat ineffective, but no respondent mentioned that it is not effective at all, which indicates that the AIS security level in companies is now improving.

Table 4.62 Cross-tabulation of the effectiveness level of AIS security management by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Somewhat ineffective	0		2		0		0		0		1		0		3
%		0		66.7		0		0		0		33.3		0	
Industry %		0		22.2		0		0		0		12.5		0	
Neither ineffective nor effective	1		1		0		2		2		1		0		7
%		14.3		14.3		0		28.6		28.6		14.3		0	
Industry %		9.1		11.1		0		18.2		33.3		12.5		0	
Somewhat effective	6		5		4		5		2		6		8		36
%		16.7		13.9		11.1		13.9		5.6		16.7		22.2	
Industry %		54.5		55.6		66.7		45.5		33.3		75		88.9	
Extremely effective	4		1		2		4		2		0		1		14
%		28.6		7.1		14.3		28.6		14.3		0		7.1	
Industry %		36.4		11.1		33.3		36.4		33.3		0		11.1	
Total	11		9		6		11		6		8		9		60

Q 1.7.3 In your opinion, how effective is the AIS security management in your company?

Further analysis by industry sector shows that respondents from all sectors except technology & telecommunications believed that AIS security management in their companies is extremely effective. Given that technology & telecommunications companies are more concerned with security awareness than the other sectors (Tables 4.18 - 4.21), these companies could be more aware of the different types of security threats facing their systems, and therefore they are not fully confident that they have an extremely effective security management.

The results also reveal that respondents from all sectors believed that AIS security management within their companies is somewhat effective. 88.9 percent of respondents from energy & utilities believed so, followed by technology & telecommunications (75 percent), media & entertainment (66.7 percent), manufacturing (55.6 percent), insurance & financial services (54.5 percent), property & construction (45.5 percent), and retail merchandising (33.3 percent). On the other hand, the three respondents who believed that AIS security management in their companies is somewhat ineffective are from the manufacturing, and technology & telecommunications sectors. The results, therefore, suggest that the majority of companies believed that their AIS security management is somewhat effective.

Furthermore, in order to test whether the effectiveness level of AIS security management differs among industry sectors, a Kruskal-Wallis test was conducted. However, the results (Table 4.63) do not provide any evidence that there are

significant differences among the industry sectors that responded. The results, therefore, reveal that there are no significant differences, at the 0.05 level, in the distribution of responses between the industry sectors that responded regarding the effectiveness level of the AIS security management, given that p-value is 0.311 ($p > 0.05$).

Table 4.63 Results of Kruskal-Wallis test regarding the effectiveness level of AIS security management

Industry sectors	N	Mean Rank
Insurance & financial services	11	35.64
Manufacturing	9	23
Media & entertainment	6	36.83
Property & construction	11	33.68
Retail merchandising	6	29.67
Technology & telecommunications	8	22.50
Energy & utilities	9	31.28
Chi-square value (χ^2) = 7.113, df = 6, and p-value = 0.311		

In short, the responses to the questions in this section provide a strong support to Hypothesis 1.7 that there are no significant differences among companies in different industry sectors concerning the techniques used to evaluate AIS security effectiveness, success indicators of security management, and the effectiveness level of AIS security management. These results are further investigated in the interviews' analysis.

4.6 AIS security threats

Companies today have become increasingly dependent on IS more than ever before. However, these IS have brought companies not only enormous benefits, but also different types of security threats (Chang and Yeh 2006). According to Lin (2006), due to resource constraints, companies cannot implement unlimited controls to protect their systems. Instead, they need to understand the major threats, and implement effective controls accordingly. In addition, Whitman (2003) argued that in order to strengthen the protection level of IS, those responsible for these systems must begin with the identification of the dominant threats facing their companies' IS security, and the ranking of those threats in order to allow their companies to direct priorities accordingly.

In order to investigate the sources and types of AIS security threats facing companies, this section presents the questionnaire results on the most common sources and types of security threats facing UK companies, and the frequency of occurrence of each

type of threat in the last year. This section is concerned with testing Hypothesis 2 (Section 3.2.4 in Chapter 3). This hypothesis can be expressed as follows:

H2: There are no significant differences among UK companies in different industry sectors concerning the sources and types of AIS security threats.

In order to test the hypothesis, respondents were asked two questions (Section 2 of the questionnaire). In the first question, respondents were provided with a list of sources of AIS security threats and were asked to rank the top three common sources of threats within their companies. Question 2.2 provided respondents with a list of AIS security threats and they were asked to indicate the frequency of occurrence of each type of these threats, by choosing one among six choices (none, once a year, once a month, once a week, once a day, and more than once a day).

Table 4.64 Cross-tabulation of the first common source of AIS security threats by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Authorised users / employees	8		9		4		10		5		8		3		47
%		17		19.1		8.5		21.3		10.6		17		6.4	
Industry %		72.7		100		66.7		90.9		71.4		100		33.3	
Former employees	1		0		1		0		0		0		1		3
%		33.3		0		33.3		0		0		0		33.3	
Industry %		9.1		0		16.7		0		0		0		11.1	
Suppliers of goods or services	1		0		0		0		1		0		2		4
%		25		0		0		0		25		0		50	
Industry %		9.1		0		0		0		14.3		0		22.2	
Competitors	0		0		0		0		0		0		1		1
%		0		0		0		0		0		0		100	
Industry %		0		0		0		0		0		0		11.1	
Computer hackers	1		0		1		1		1		0		2		6
%		16.7		0		16.7		16.7		16.7		0		33.3	
Industry %		9.1		0		16.7		9.1		14.3		0		22.2	
Total	11		9		6		11		7		8		9		61

Q 2.1 Please rank the top 3 users who in your opinion represent the common sources of security threats to your company's AIS where 1 represents the most common source.

Regarding the top three common sources of AIS security threats, the results in Table 4.64 show that the majority of companies (77 percent) believed that authorised users or employees are their first common source of security threats. This result is consistent with what was claimed in the literature. The Organisation for Economic Co-operation and Development (OECD 1992) stated that employees who have been granted authorised access to systems might pose a larger threat to IS. In addition,

Loch *et al.* (1992) argued that employees are a greater threat than competitors. Moreover, Vroom and Von Solms (2004) claimed that, despite the vital role of employees in the success of any company, they are the weakest link when it comes to IS security. Most recently, the BERR Information Security Breaches Survey (BERR 2008) indicated that UK companies increasingly realise that their people, while their greatest asset, can be their greatest vulnerability.

On the other hand, Table 4.64 shows that only 9.8 percent of companies believed that computer hackers are their first common source of security threats, followed by suppliers of goods and services (6.6 percent), former employees (4.9 percent), and competitors (1.6 percent). From these results, it is clear that the majority of companies considered their employees the first common source of security threats facing their systems, whereas customers are not considered by any respondent as a first common source of threats.

Further analysis reveals that respondents from all sectors selected authorised users or employees as the first common source of security threats. In addition, all the respondents from manufacturing and technology & telecommunications had the same opinion, followed by property & construction (90.9 percent), insurance & financial services (72.7 percent), retail merchandising (71.4 percent), and media & entertainment (66.7 percent). On the other hand, only one third of energy & utilities companies considered employees to be their first common source of security threats. This result is consistent with the BERR Information Security Breaches Survey (BERR 2008) which revealed that the sector least affected by staff misuse was energy & utilities.

The results also show that only one respondent, from an energy & utilities company, believed that competitors are the first common source of security threats to a company's AIS. Table 4.64 also shows that companies from all sectors except manufacturing and technology & telecommunications believed that computer hackers are their first common source of security threats.

Regarding the second common source of security threats, Table 4.65 shows that just over half of companies (52.6 percent) believed that former employees are their second

common source of security threats. This result indicates that employees, whether current or former, are the main source of security threats to UK companies. The results also show that 15.8 percent of companies considered computer hackers to be their second common source of security threats, followed by suppliers of goods and services (12.3 percent), authorised users or employees (10.5 percent), and competitors (7 percent). However, only one respondent believed that the company's customers are the second source of threats. This result is consistent with Loch *et al.* (1992).

Table 4.65 Cross-tabulation of the second common source of AIS security threats by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Authorised users / employees	1		0		2		0		1		0		2		6
%		16.7		0		33.3		0		16.7		0		33.3	
Industry %		10		0		33.3		0		16.7		0		22.2	
Former employees	4		6		3		6		3		4		4		30
%		13.3		20		10		20		10		13.3		13.3	
Industry %		40		66.7		50		60		50		57.1		44.4	
Suppliers of goods or services	1		1		1		0		1		1		2		7
%		14.3		14.3		14.3		0		14.3		14.3		28.6	
Industry %		10		11.1		16.7		0		16.7		14.3		22.2	
Customers	1		0		0		0		0		0		0		1
%		100		0		0		0		0		0		0	
Industry %		10		0		0		0		0		0		0	
Competitors	1		1		0		0		1		0		1		4
%		25		25		0		0		25		0		25	
Industry %		10		11.1		0		0		16.7		0		11.1	
Computer hackers	2		1		0		4		0		2		0		9
%		22.2		11.1		0		44.4		0		22.2		0	
Industry %		20		11.1		0		40		0		28.6		0	
Total	10		9		6		10		6		7		9		57

Q 2.1 Please rank the top 3 users who in your opinion represent the common sources of security threats to your company's AIS where 1 represents the most common source.

The analysis by industry sector (Table 4.65) reveals that 66.7 percent of respondents from manufacturing companies believed that former employees are their second common source of security threats. These results are consistent with the results in Table 4.64 in which all the respondents from the manufacturing sector believed that employees are their first source of threats.

It can also be seen from Table 4.65 that 60 percent of property & construction companies believed that former employees are their second common source of security threats, followed by technology & telecommunications (57.1 percent), media & entertainment, and retail merchandising (50 percent), energy & utilities (44.4

percent), and insurance & financial services (40 percent). On the other hand, only one respondent, who is from the insurance & financial services, selected the company's customers. This result suggests that the majority of companies except for insurance & financial service companies do not consider customers as a common source of security threats. According to the Global Security Survey (DTT 2007), financial institutions are particularly vulnerable given the nature of the information they hold. In addition, since most training and awareness programs are directed towards internal users only, this means that the customer risk category is sometimes ignored.

Table 4.66 Cross-tabulation of the third common source of AIS security threats by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Authorised users / employees	2		0		0		1		0		0		3		6
%		33.3		0		0		16.7		0		0		50	
Industry %		28.6		0		0		12.5		0		0		33.3	
Former employees	0		2		0		2		1		2		0		7
%		0		28.6		0		28.6		14.3		28.6		0	
Industry %		0		25		0		25		16.7		28.6		0	
Suppliers of goods or services	3		1		3		0		1		0		0		8
%		37.5		12.5		37.5		0		12.5		0		0	
Industry %		42.9		12.5		50		0		16.7		0		0	
Customers	0		1		1		0		0		1		1		4
%		0		25		25		0		0		25		25	
Industry %		0		12.5		16.7		0		0		14.3		11.1	
Competitors	0		1		0		1		1		1		3		7
%		0		14.3		0		14.3		14.3		14.3		42.9	
Industry %		0		12.5		0		12.5		16.7		14.3		33.3	
Computer hackers	2		3		2		4		3		3		2		19
%		10.5		15.8		10.5		21.1		15.8		15.8		10.5	
Industry %		28.6		37.5		33.3		50		50		42.9		22.2	
Total	7		8		6		8		6		7		9		51

Q 2.1 Please rank the top 3 users who in your opinion represent the common sources of security threats to your company's AIS where 1 represents the most common source.

It can be seen from Table 4.66 that 37.3 percent of companies believed that hackers are their third source of AIS security threats. This could be because only 9.8 percent of companies (Table 4.64) considered computer hackers to be their first source of security threats, while 15.8 percent (Table 4.65) believed that hackers are their second common source of security threats. Table 4.66 also shows that suppliers were selected by 15.7 percent of companies as their third common source of security threats, followed by former employees, and competitors (13.7 percent), authorised users or employees (11.8 percent), and customers (7.8 percent).

Further analysis reveals that half of the respondents from property & construction, and retail merchandising believed that computer hackers are their third common source of security threats; this is followed by technology & telecommunications (42.9 percent), manufacturing (37.5 percent), media & entertainment (33.3 percent), insurance & financial services (28.6 percent), and energy & utilities (22.2 percent). This result indicates that respondents from all sectors saw computer hackers as their third common source of threats. This result is consistent with the BERR Information Security Breaches Survey (BERR 2008) which stated that hackers appear more successful at breaking companies' networks than before, and that larger companies are more likely to be penetrated than smaller ones. The results also show that authorised users or employees are seen as the third common source of security threats by only six respondents from insurance & financial services, property & construction, and energy & utilities. This could be because 77 percent of companies believed that employees are their first common source of threats (Table 4.64), and 10.5 percent considered them their second common source of threats (Table 4.65).

It is clear from the above results that authorised users or employees, former employees and computer hackers are the most common sources of AIS security threats facing the companies that responded, whereas competitors and customers are the least common. This result is consistent with the Security and Information Risk Survey (NCC 2007) which indicated that competitors are the least of a company's worries when it comes to their security strategy. This result is further verified by calculating the weighted score of each source of AIS security threats.

Table 4.67 Weighted scores of the number of times sources of AIS security threats were selected by respondents

Common sources of AIS security threats	Number of times selected			Weighted scores
	First common source of security threats	Second common source of security threats	Third common source of security threats	
Authorised users/employees	47	6	6	159
Former employees	3	30	7	76
Suppliers of goods/services	4	7	8	34
Customers	0	1	4	6
Competitors	1	4	7	18
Computer hackers	6	9	19	55

Table 4.67 shows that the authorised users or employees achieved the highest weighted score (159), which indicates that authorised employees are believed to be the first common source of AIS security threats facing UK companies that responded, followed by former employees with a weighted score of 76, then computer hackers

with 55. On the other hand, competitors, and customers achieved the least weighted scores of 18 and 6 respectively. The results provide evidence that the common source of security threats are now believed to come more from inside companies than from outside.

Moreover, in order to examine whether the most common sources of AIS security threats vary among different sectors, a Kruskal-Wallis test was conducted. The results (Table 4.68) do not indicate any statistically significant differences, at the 0.05 level, in the distribution of responses among the different industry sectors except for the authorised users or employees. This result implies that there are significant differences, at the 0.05 level, in the distribution of responses among the different sectors regarding the authorised users or employees, given that p-value is 0.022 ($p < 0.05$). On the other hand, there are no significant differences among the different sectors regarding the other five sources of threats.

Table 4.68 Results of Kruskal-Wallis test regarding the common sources of AIS security threats

Common sources of AIS security threats	Industry sectors	N	Mean Rank
Authorised users/employees	Insurance & financial services	11	32.32
	Manufacturing	9	24
	Media & entertainment	6	32.83
	Property & construction	11	26.95
	Retail merchandising	6	28.42
	Technology & telecommunications	8	24
	Energy & utilities	8	42.81
Chi-square value (χ^2) = 14.795, df = 6, and p-value = 0.022			
Former employees	Insurance & financial services	5	15.20
	Manufacturing	8	23.13
	Media & entertainment	4	14.38
	Property & construction	8	23.13
	Retail merchandising	4	23.13
	Technology & telecommunications	6	24.67
	Energy & utilities	5	15.20
Chi-square value (χ^2) = 8.598, df = 6 and p-value = 0.197			
Suppliers of goods/services	Insurance & financial services	5	11.40
	Manufacturing	2	11.75
	Media & entertainment	4	13.63
	Property & construction	-	-
	Retail merchandising	3	8.67
	Technology & telecommunications	1	8
	Energy & utilities	4	5.25
Chi-square value (χ^2) = 6.112, df = 5, and p-value = 0.296			
Customers	Insurance & financial services	1	1
	Manufacturing	1	3.50
	Media & entertainment	1	3.50
	Property & construction	-	-
	Retail merchandising	-	-
	Technology & telecommunications	1	3.50
	Energy & utilities	1	3.50
Chi-square value (χ^2) = 4.000, df = 4, and p-value = 0.406			
Competitors	Insurance & financial services	1	3.50
	Manufacturing	2	6.25
	Media & entertainment	-	-
	Property & construction	1	9

	Retail merchandising	2	6.25
	Technology & telecommunications	1	9
	Energy & utilities	5	6.30
Chi-square value (χ^2) = 2.195, df = 5, and p-value = 0.822			
Computer hackers	Insurance & financial services	5	15.10
	Manufacturing	4	21.50
	Media & entertainment	3	17.83
	Property & construction	9	16.39
	Retail merchandising	4	19.63
	Technology & telecommunications	5	19.40
	Energy & utilities	4	14.25
Chi-square value (χ^2) = 2.296, df = 6, and p-value = 0.891			

As mentioned before, respondents were then given a list of security threats and were asked to indicate the frequency of occurrence of each type of these threats. Table 4.69 provides the frequency of occurrence reported by respondents. The results for each type of security threats are presented below.

Table 4.69 Frequency of occurrence of each type of AIS security threats

	None		Once a year		Once a month		Once a week		Once a day		More than once a day		Total
	no	%	no	%	no	%	no	%	no	%	no	%	
Unauthorised access to data/systems by disgruntled employees	48	76.2	14	22.2	0	0	1	1.6	0	0	0	0	63
Unauthorised access to data/systems by hackers	55	88.7	5	8.1	1	1.6	0	0	0	0	1	1.6	62
Unintentional destruction of data by employees	22	36.7	20	33.3	14	23.3	4	6.7	0	0	0	0	60
Intentional destruction of data by employees	49	80.3	11	18	0	0	1	1.6	0	0	0	0	61
Theft of physical information e.g. printed output, computer disks, etc.	50	83.3	7	11.7	2	3.3	1	1.7	0	0	0	0	60
Introduction of computer viruses, bombs or worms to the system	31	49.2	20	31.7	4	6.3	5	7.9	1	1.6	2	3.2	63
Spamming attacks	23	37.7	8	13.1	8	13.1	2	3.3	7	11.5	13	21.3	61
Malware (spyware, adware) programs	22	34.9	15	23.8	3	4.8	7	11.1	7	11.1	9	14.3	63
Sharing of passwords	16	27.1	7	11.9	20	33.9	6	10.2	7	11.9	3	5.1	59
Theft of software	50	80.6	5	8.1	4	6.5	2	3.2	0	0	1	1.6	62
Technical software failures or errors	10	16.1	25	40.3	19	30.6	4	6.5	2	3.2	2	3.2	62
Sabotage or intentional destruction of computer equipment e.g. PCs and laptops	57	90.5	5	7.9	1	1.6	0	0	0	0	0	0	63
Natural disasters e.g. fire, floods, earthquakes, etc.	44	69.8	19	30.2	0	0	0	0	0	0	0	0	63

Q 2.2 Please indicate the frequency with which your company has faced each type of the following threats in the last year.

Unauthorised access to the data or systems by disgruntled employees

Table 4.69 shows that 76.2 percent of respondents claimed that this threat had never occurred in their companies in the last year, and 22.2 percent believed that it occurred only once a year. On the other hand, only one respondent believed that unauthorised access to data or systems by disgruntled employees happened once per week.

Further analysis by industry sector (Table 4.70) reveals that all respondents from property & construction, and energy & utilities claimed that their companies did not face any unauthorised access to data or systems by disgruntled employees in the last year, followed by insurance & financial services (72.2 percent), retail merchandising (71.4 percent), and manufacturing (70 percent). On the other hand, only two fifths of media & entertainment companies believed this. In addition, the only respondent who believed that this threat occurred once per week in the last year was from the media & entertainment sector, while respondents from all industry sectors except property & construction and energy & utilities believed that their companies suffered from unauthorised access to data or systems by disgruntled employees once in the last year.

Table 4.70 Cross-tabulation of unauthorised access to data/systems by disgruntled employees by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	8		7		2		13		5		4		9		48
%		16.7		14.6		4.2		27.1		10.4		8.3		18.8	
Industry %		72.7		70		40		100		71.4		50		100	
Once a year	3		3		2		0		2		4		0		14
%		21.4		21.4		14.3		0		14.3		28.6		0	
Industry %		27.3		30		40		0		28.6		50		0	
Once a week	0		0		1		0		0		0		0		1
%		0		0		100		0		0		0		0	
Industry %		0		0		20		0		0		0		0	
Total	11		10		5		13		7		8		9		63

From these results, it seems that this threat rarely occurred in the property & construction and energy & utilities sectors, but was more likely to happen in the other sectors that responded. In order to avoid this threat, companies should allow their employees to access only the data required to perform their jobs.

Unauthorised access to the data or systems by hackers

Despite being the third common source of AIS security threats facing UK companies, 88.7 percent of companies claimed that they did not face this threat in the last year, while five companies (8.1 percent) believed that it had happened once in the last year. On the other hand, only one company suffered from unauthorised access to data or its systems by hackers once per month in the last year, and another respondent believed that it happened more than once a day.

Further analysis (Table 4.71) reveals that all respondents from property & construction claimed that their companies did not face any unauthorised access to data or systems by hackers. This is followed by insurance & financial services (90.9 percent), manufacturing (90 percent), energy & utilities (88.9 percent), retail merchandising (85.7 percent), media & entertainment (80 percent), and technology & telecommunications (71.4 percent). The results also show that only one respondent, from the insurance & financial services sector, believed that their company's AIS was faced by this threat once a month in the last year, while another respondent from the manufacturing sector claimed that it happened more than once a day.

Table 4.71 Cross-tabulation of unauthorised access to data/systems by hackers by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	10		9		4		13		6		5		8		55
%		18.2		16.4		7.3		23.6		10.9		9.1		14.5	
Industry %		90.9		90		80		100		85.7		71.4		88.9	
Once a year	0		0		1		0		1		2		1		5
%		0		0		20		0		20		40		20	
Industry %		0		0		20		0		14.3		28.6		11.1	
Once a month	1		0		0		0		0		0		0		1
%		100		0		0		0		0		0		0	
Industry %		9.1		0		0		0		0		0		0	
More than once a day	0		1		0		0		0		0		0		1
%		0		100		0		0		0		0		0	
Industry %		0		10		0		0		0		0		0	
Total	11		10		5		13		7		7		9		62

From these results, it seems that property & construction companies that responded are rarely faced with unauthorised access to data or systems by hackers, whereas the sector most likely to suffer from this threat is the manufacturing sector. This is a surprising result, given that the manufacturing sector has a lower level of computerisation, and is less reliant on IT than other sectors (Yeh and Chang 2007).

Unintentional destruction of data by employees

In contrast to the two previous threats, the results reveal that 36.7 percent of companies claimed that they did not suffer last year from any unintentional destruction of data by their employees (Table 4.69). The results also show that one third of companies believed that they had suffered from this threat once in the last year, 23.3 percent believed that it happened once per month, while only four respondents believed that it occurred once per week.

It is not surprising that the unintentional destruction of data by employees occurred in more than three fifths of companies that responded, given that employees' accidental actions were ranked among the top IS threats in the study conducted by Loch *et al.* (1992) and Davis (1997). In addition, Wood and Banks (1993) argued that human error is one of the most serious information security threats. The CSI Survey (Richardson 2007) also indicated that there have been too many data breaches driven by simple human error and carelessness.

Table 4.72 Cross-tabulation of unintentional destruction of data by employees by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	5		2		2		7		1		2		3		22
%		22.7		9.1		9.1		31.8		4.5		9.1		13.6	
Industry %		50		22.2		40		53.8		14.3		28.6		33.3	
Once a year	3		3		0		5		3		3		3		20
%		15		15		0		25		15		15		15	
Industry %		30		33.3		0		38.5		42.9		42.9		33.3	
Once a month	2		4		2		1		2		2		1		14
%		14.3		28.6		14.3		7.1		14.3		14.3		7.1	
Industry %		20		44.4		40		7.7		28.6		28.6		11.1	
Once a week	0		0		1		0		1		0		2		4
%		0		0		25		0		25		0		50	
Industry %		0		0		20		0		14.3		0		22.2	
Total	10		9		5		13		7		7		9		60

Further analysis reveals that companies from all industry sectors claimed that no unintentional destruction of data by employees occurred last year. Table 4.72 reveals that 53.8 percent of the respondents from the property & construction sector reported the non-occurrence of this threat in the last year, followed by insurance & financial services (50 percent), media & entertainment (40 percent), energy & utilities (33.3 percent). On the other hand, only 14.3 percent from retail merchandising sector held the same opinion. In addition, it was claimed by respondents from all the industry sectors except media & entertainment that unintentional destruction of data by employees occurred once in the last year, while respondents from all sectors believed that it happened once per month. On the other hand, only four respondents from media & entertainment, retail merchandising, and energy & utilities sectors reported the occurrence of this threat once per week in the last year.

From the above results, it seems that the unintentional destruction of data by employees had occurred in most companies responded in the last year. This result is

consistent with what was claimed by Im and Baskerville (2005) that the major source of unmanaged risks to IS continues to be accidental in nature.

Intentional destruction of data by employees

The results concerning this threat (Table 4.69) reveal that the majority of companies responded (80.3 percent) reported the non-occurrence of any intentional destruction of data by their employees in the last year, and 18 percent reported the occurrence of this threat once in the last year. Only one company believed that it happened once per week. This suggests that intentional destruction of data by employees is an infrequent security threat in UK companies that responded. This result is consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that intentional destruction by employees remains rare, even in large businesses.

Table 4.73 Cross-tabulation of intentional destruction of data by employees by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	10		9		3		12		4		5		6		49
%		20.4		18.4		6.1		24.5		8.2		10.2		12.2	
Industry %		90.9		90		60		100		66.7		62.5		66.7	
Once a year	1		1		2		0		2		2		3		11
%		9.1		9.1		18.2		0		18.2		18.2		27.3	
Industry %		9.1		10		40		0		33.3		25		33.3	
Once a week	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		12.5		0	
Total	11		10		5		12		6		8		9		61

It can be seen from Table 4.73 that all the respondents from the property & construction sector claimed that no intentional acts by employees occurred in the last year, followed by insurance & financial services (90.9), manufacturing (90 percent), retail merchandising, and energy & utilities (66.7 percent), technology & telecommunications (62.5 percent), and media & entertainment (60 percent). In addition, respondents from all industry sectors except property & construction reported the occurrence of this threat once in the last year, while only one company from the technology & telecommunications sector believed that intentional destruction of data by employees occurred once per week. The results, therefore, suggest the infrequent occurrence of the intentional destruction of data by employees in UK companies that responded.

Theft of physical information e.g. printed output, computer disks, tapes, etc.

It can be observed from Table 4.69 that the majority of companies (83.3 percent) reported the non-occurrence of any theft of physical information in the last year. On the other hand, 11.7 percent of respondents stated that this had happened once in the last year, only two companies claimed its occurrence once per month, and one company reported its occurrence once per week. This result again suggests the infrequent occurrence of theft of physical information within UK companies that responded, which indicates that companies are beginning to implement sufficient access controls in place to reduce these threats. According to Lin (2006), data and information theft is more common when access controls are not implemented.

Table 4.74 Cross-tabulation of theft of physical information by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	9		8		4		12		3		6		8		50
%		18		16		8		24		6		12		16	
Industry %		81.8		80		80		100		50		85.7		88.9	
Once a year	1		2		0		0		2		1		1		7
%		14.3		28.6		0		0		28.6		14.3		14.3	
Industry %		9.1		20		0		0		33.3		14.3		11.1	
Once a month	1		0		0		0		1		0		0		2
%		50		0		0		0		50		0		0	
Industry %		9.1		0		0		0		16.7		0		0	
Once a week	0		0		1		0		0		0		0		1
%		0		0		100		0		0		0		0	
Industry %		0		0		20		0		0		0		0	
Total	11		10		5		12		6		7		9		60

Further analysis (Table 4.74) reveals that all respondents from the property & construction sector reported the non-occurrence of any theft of physical information during the last year, followed by energy & utilities (88.9 percent), technology & telecommunications (85.7 percent), insurance & financial services (81.8 percent), manufacturing and media & entertainment (80 percent). On the other hand, half of the retail merchandising companies believed there had been no theft of physical information in the last year.

Table 4.74 also reveals that respondents from all sectors except media & entertainment and property & construction reported that their companies suffered from theft of information once in the last year. At the same time, two respondents from insurance & financial services and retail merchandising companies believed that it had happened once per month. On the other hand, only one respondent, from media

& entertainment believed it occurred once per week. These results again reflect the infrequent occurrence of this threat in UK companies that responded.

Introduction of computer viruses, bombs, or worms to the system

In the past few years, there has been extensive publicity about the damage viruses can cause, and a large number of viruses has been identified. However, it can be seen from Table 4.69 that 49.2 percent of the companies claimed that they did not suffer from any virus attacks in the last year. This is not a surprising result since almost all companies, regardless of their size or sector, are using anti-virus software. This result is further investigated in Section 4.7. The BERR Information Security Breaches Survey (BERR 2008) indicated that the fewer virus infections reported by companies could be because corporate anti-virus defences have significantly improved. In addition, according to the CSI Survey (Richardson 2007), anti-virus vendors have become faster at reacting to new virus threats.

Table 4.75 Cross-tabulation of the introduction of computer viruses to the system by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	7		5		2		6		3		4		4		31
%		22.6		16.1		6.5		19.4		9.7		12.9		12.9	
Industry %		63.6		50		40		46.2		42.9		50		44.4	
Once a year	3		5		1		5		1		4		1		20
%		15		25		5		25		5		20		5	
Industry %		27.3		50		20		38.5		14.3		50		11.1	
Once a month	1		0		0		0		2		0		1		4
%		25		0		0		0		50		0		25	
Industry %		9.1		0		0		0		28.6		0		11.1	
Once a week	0		0		0		1		1		0		3		5
%		0		0		0		20		20		0		60	
Industry %		0		0		0		7.7		14.3		0		33.3	
Once a day	0		0		1		0		0		0		0		1
%		0		0		100		0		0		0		0	
Industry %		0		0		20		0		0		0		0	
More than once a day	0		0		1		1		0		0		0		2
%		0		0		50		50		0		0		0	
Industry %		0		0		20		7.7		0		0		0	
Total	11		10		5		13		7		8		9		63

The results also show that 31.7 percent of companies believed that their systems were faced by virus infection once in the last year, while only four companies stated that it happened once a month and five companies indicated that the virus infection occurred one per week. On the other hand, one respondent believed that it happened once a day and another two respondents reported that their companies' systems suffered from virus attacks more than once per day.

Further analysis (Table 4.75) reveals that respondents from all industry sectors that responded reported the non-occurrence of any virus attacks on their companies' systems in the last year. It can be seen that 63.6 percent of insurance & financial services companies agreed, followed by manufacturing, and technology & telecommunications (50 percent), property & construction (46.2 percent), energy & utilities (44.4 percent), retail merchandising (42.9 percent), and media & entertainment (40 percent).

It can also be seen from Table 4.75 that respondents from all sectors claimed that their systems had a virus infection once in the last year. On the other hand, one respondent from media & entertainment believed that systems were infected once a day, and another two respondents from media & entertainment, and property & construction reported the occurrence of virus infection more than once a day. This result is consistent with the result of the BERR Information Security Breaches Survey (BERR 2008), which indicated that financial services, and technology & telecommunications providers are the most rigorous at keeping their anti-virus software up-to-date, however, property & construction and leisure companies appear more relaxed.

The above results, therefore, suggest that viruses are no longer a big issue for UK companies that responded. Perhaps the media attention given to viruses has increased the awareness level of this particular threat.

Spamming attacks

The new business environment is accompanied by new security threats like spamming or e-mail attacks. Hicks (2004) argued that, although spam is not harmful for systems, it is considered a prime cause of productivity losses for companies. The results in Table 4.69 reveal that 62.3 percent of companies reported the occurrence of these attacks in the last year, while only 37.7 percent of companies reported their non-occurrence. This result indicates the frequent occurrence of the spamming attacks on UK companies that responded compared to other threats. It can also be seen from Table 4.69 that 13.1 percent of companies believed that they suffered from spamming attacks only once in the last year, and another 13.1 percent believed this occurred once per month, while two respondents reported their occurrence once per week. However, in contrast to most of the previous threats, 11.5 percent of respondents

reported the daily occurrence of spamming attacks, and more than one fifth declared that their companies suffered from these attacks several times per day in the last year, which underlines their frequent occurrence.

Table 4.76 Cross-tabulation of spamming attacks by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	3		5		1		7		3		3		1		23
%		13		21.7		4.3		30.4		13		13		4.3	
Industry %		27.3		55.6		20		53.8		42.9		42.9		11.1	
Once a year	3		1		0		1		2		0		1		8
%		37.5		12.5		0		12.5		25		0		12.5	
Industry %		27.3		11.1		0		7.7		28.6		0		11.1	
Once a month	3		1		0		2		0		1		1		8
%		37.5		12.5		0		25		0		12.5		12.5	
Industry %		27.3		11.1		0		15.4		0		14.3		11.1	
Once a week	0		0		1		0		1		0		0		2
%		0		0		50		0		50		0		0	
Industry %		0		0		20		0		14.3		0		0	
Once a day	1		0		2		1		1		0		2		7
%		14.3		0		28.6		14.3		14.3		0		28.6	
Industry %		9.1		0		40		7.7		14.3		0		22.2	
More than once a day	1		2		1		2		0		3		4		13
%		7.7		15.4		7.7		15.4		0		23.1		30.8	
Industry %		9.1		22.2		20		15.4		0		42.9		44.4	
Total	11		9		5		13		7		7		9		61

Furthermore, the analysis by industry sector (Table 4.76) indicates that 55.6 percent of the manufacturing companies reported the non-occurrence of these attacks. This is not a surprising result, given the low level of computerisation of manufacturing companies (Yeh and Chang 2007). The results also reveal that 53.8 percent of property & construction companies claimed the non-occurrence of any spamming attacks in the last year, followed by retail merchandising, and technology & telecommunications (42.9 percent), and insurance & financial services (27.3 percent). However, only a single respondent from both media & entertainment, and energy & utilities claimed such attacks did not occur. In addition, it can be seen from Table 4.76 that respondents from all sectors except media & entertainment, and retail merchandising believed spamming attacks occurred once per month in the last year, whereas respondents from these two sectors reported an occurrence of once per week. Moreover, companies from all sectors except manufacturing, and technology & telecommunications reported the daily occurrence of such attacks to their systems, whereas companies from all sectors except retail merchandising revealed the frequent attacks each day.

The above results indicate the frequent occurrence of spamming or e-mail attacks within UK companies that responded. These results are consistent with the Global Security Survey (DTT 2007), which indicated that e-mail attacks are among the top security threats that were repeated the greatest number of times by respondents.

Malware (spyware, adware) programs

Malware attacks represent a clearly understood threat. It can be seen from Table 4.69 that 25.4 percent of respondents reported the frequent occurrence of these attacks, either once a day, or several times per day. The results also show that 34.9 percent of respondents reported the non-occurrence of any malware attacks in the last year, while 23.8 percent of respondents believed that malware attacks rarely happened within their companies, as they had occurred only once in the last year. On the other hand, three companies reported their occurrence once per month, while 11.1 percent reported their occurrence once per week.

Table 4.77 Cross-tabulation of malware programs by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	3		5		1		6		2		2		3		22
%		13.6		22.7		4.5		27.3		9.1		9.1		13.6	
Industry %		27.3		50		20		46.2		28.6		25		33.3	
Once a year	6		4		1		2		2		0		0		15
%		40		26.7		6.7		13.3		13.3		0		0	
Industry %		54.5		40		20		15.4		28.6		0		0	
Once a month	1		0		0		0		1		1		0		3
%		33.3		0		0		0		33.3		33.3		0	
Industry %		9.1		0		0		0		14.3		12.5		0	
Once a week	0		0		2		1		1		2		1		7
%		0		0		28.6		14.3		14.3		28.6		14.3	
Industry %		0		0		40		7.7		14.3		25		11.1	
Once a day	1		0		0		2		0		0		4		7
%		14.3		0		0		28.6		0		0		57.1	
Industry %		9.1		0		0		15.4		0		0		44.4	
More than once a day	0		1		1		2		1		3		1		9
%		0		11.1		11.1		22.2		11.1		33.3		11.1	
Industry %		0		10		20		15.4		14.3		37.5		11.1	
Total	11		10		5		13		7		8		9		63

These results suggest the frequent occurrence of malware attacks in UK companies that responded, although the majority of companies are now using malware detection tools (Section 4.7). This could be because new malware is emerging at a frightening rate (BERR 2008). In addition, the Global Security Survey (DTT 2007) indicated that spyware are at the top of the list of attacks, with more than half of the companies (52 percent) reporting them.

Further analysis (Table 4.77) reveals that half of the manufacturing companies claimed the non-occurrence of any malware attacks in the last year, followed by property & construction (46.2 percent), and energy & utilities (33.3 percent). In addition, 28.6 percent of retail merchandising agreed, followed by insurance & financial services (27.3 percent), technology & telecommunications (25 percent), and media & entertainment (20 percent). This result could be because manufacturing companies have a lower level of computerisation, compared to other sectors, and therefore they are the companies to be affected least by malware attacks. In contrast, 55.6 percent of energy & utilities companies reported the frequent occurrence of malware attacks either once a day or more. This result is again consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that energy companies are least likely to be protected against spyware.

Table 4.77 also reveals that 37.5 percent of technology & telecommunications companies believed malware attacks took place more than once per day, with none of the respondents from insurance & financial services reporting this. This could be because financial services providers are the most rigorous at keeping their anti-malware software up-to-date. The results, therefore, suggest that manufacturing companies are the least affected by malware attacks, whereas energy & utilities and technology & telecommunications are the most affected companies.

Sharing of passwords

There have been too many security breaches driven by simple human error and carelessness, especially the sharing of passwords. The results (Table 4.69) show that 72.9 percent of respondents reported that employees in their companies shared their passwords in the last year, with only 27.1 percent of respondents reporting the non-occurrence of this threat, which indicates its frequent occurrence in UK companies that responded. Table 4.69 also shows that 11.9 percent of companies claimed that sharing passwords happened only once in the last year, 33.9 percent reported its occurrence once per month, and 10.2 percent once per week. On the other hand, seven companies believed that the sharing of passwords took place once per day, and 5.1 percent reported its occurrence several times per day.

Table 4.78 Cross-tabulation of sharing of passwords by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	3		1		1		7		0		3		1		16
%		18.8		6.3		6.3		43.8		0		18.8		6.3	
Industry %		33.3		11.1		20		53.8		0		42.9		11.1	
Once a year	1		3		0		1		0		0		2		7
%		14.3		42.9		0		14.3		0		0		28.6	
Industry %		11.1		33.3		0		7.7		0		0		22.2	
Once a month	3		4		3		4		1		1		4		20
%		15		20		15		20		5		5		20	
Industry %		33.3		44.4		60		30.8		14.3		14.3		44.4	
Once a week	1		1		0		1		0		2		1		6
%		16.7		16.7		0		16.7		0		33.3		16.7	
Industry %		11.1		11.1		0		7.7		0		28.6		11.1	
Once a day	1		0		1		0		3		1		1		7
%		14.3		0		14.3		0		42.9		14.3		14.3	
Industry %		11.1		0		20		0		42.9		14.3		11.1	
More than once a day	0		0		0		0		3		0		0		3
%		0		0		0		0		100		0		0	
Industry %		0		0		0		0		42.9		0		0	
Total	9		9		5		13		7		7		9		59

Further analysis (Table 4.78) shows that respondents from all sectors except retail merchandising reported the non-occurrence of password sharing among employees in the last year. In addition, 53.8 percent of the property & construction companies held the same opinion, followed by technology & telecommunications (42.9 percent), insurance & financial services (33.3 percent), and media & entertainment (20 percent), with only 11.1 percent from manufacturing, and energy & utilities. It was also observed that companies from all sectors believed that employees' sharing of passwords happened once per month, while companies from all sectors except media & entertainment, and retail merchandising believed its occurrence was once per week. On the other hand, companies from all sectors except manufacturing and property & construction reported its occurrence once per day. In addition, only respondents from the retail merchandising sector believed that employees' sharing of passwords had happened several times per day in the last year. The results, therefore, suggest the high level of occurrence of employees' sharing of passwords in the retail merchandising companies that responded.

Theft of software

In contrast to other AIS security threats, the results in Table 4.69 suggest the infrequent occurrence of software theft in UK companies. The results reveal that 80.6 percent of companies claimed the non-occurrence of any software theft in the last

year, and another five companies believed that it happened once in the last year, while 6.5 percent reported its occurrence once per month. On the other hand, only two companies believed the theft of software occurred once per week, and only one company believed that it happened more than once a day.

Table 4.79 Cross-tabulation of theft of software by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	10		9		3		12		5		4		7		50
%		20		18		6		24		10		8		14	
Industry %		90.9		90		60		92.3		83.3		50		77.8	
Once a year	1		0		0		0		1		1		2		5
%		20		0		0		0		20		20		40	
Industry %		9.1		0		0		0		16.7		12.5		22.2	
Once a month	0		1		1		1		0		1		0		4
%		0		25		25		25		0		25		0	
Industry %		0		10		20		7.7		0		12.5		0	
Once a week	0		0		1		0		0		1		0		2
%		0		0		50		0		0		50		0	
Industry %		0		0		20		0		0		12.5		0	
More than once a day	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		12.5		0	
Total	11		10		5		13		6		8		9		62

In addition, the analysis by sectors (Table 4.79) reveals that some respondents from all sectors reported the non-occurrence of any software theft within their companies in the last year. The results show that 92.3 percent of respondents from property & construction agreed, followed by insurance & financial services (90.9 percent), and manufacturing (90 percent), while only half the respondents from technology & telecommunications reported the non-occurrence of software theft in the last year. In addition, respondents from all sectors except insurance & financial services, retail merchandising, and energy & utilities believed it occurred once a month, with respondents from only media & entertainment, and technology & telecommunications sectors reporting its occurrence once a week.

Interestingly, one respondent only from technology & telecommunications believed software theft occurred several times per day. This could be because, despite the significant spending on IS security, technology companies are inadequately implementing personnel-related controls (Chang and Yeh 2006), which could give employees the opportunity to steal companies' software. However, the above results suggest the low level of occurrence of software theft in UK companies that responded.

Technical software failures or errors

Technical software errors are one of the major and most serious threats to AIS security. The results in Table 4.69 show that 83.9 percent of companies reported that they suffered from technical software failures in the last year, while only 16.1 percent of companies reported their non-occurrence. The results also reveal that 40.3 percent of companies reported the occurrence of software failures once in the last year, 30.6 percent once per month, and 6.5 percent once per week. On the other hand, two companies believed that they suffered from software failures once a day in the last year, and another two companies reported their occurrence several times per day.

These results give an indication that software failures or errors are happening in most UK companies that responded, but their occurrence is infrequent, since only 10 companies reported their non-occurrence. However, two fifths of companies reported their occurrence only once in the last year.

Table 4.80 Cross-tabulation of technical software failures or errors by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	2		1		0		1		1		2		3		10
%		20		10		0		10		10		20		30	
Industry %		18.2		10		0		7.7		14.3		28.6		33.3	
Once a year	6		7		3		4		1		3		1		25
%		24		28		12		16		4		12		4	
Industry %		54.5		70		60		30.8		14.3		42.9		11.1	
Once a month	1		1		1		6		4		1		5		19
%		5.3		5.3		5.3		31.6		21.1		5.3		26.3	
Industry %		9.1		10		20		46.2		57.1		14.3		55.6	
Once a week	2		1		0		1		0		0		0		4
%		50		25		0		25		0		0		0	
Industry %		18.2		10		0		7.7		0		0		0	
Once a day	0		0		0		1		0		1		0		2
%		0		0		0		50		0		50		0	
Industry %		0		0		0		7.7		0		14.3		0	
More than once a day	0		0		1		0		1		0		0		2
%		0		0		50		0		50		0		0	
Industry %		0		0		20		0		14.3		0		0	
Total	11		10		5		13		7		7		9		62

Further analysis (Table 4.80) reveals that respondents from all sectors except media & entertainment reported the non-occurrence of any software failures in the last year. In addition, respondents from all sectors believed that their companies suffered from software failures once in the last year, given that 70 percent of respondents from manufacturing sector agreed, while only 11.1 percent from energy & utilities reported their occurrence once a year. It can also be observed from Table 4.80 that only two

companies from property & construction, and technology & telecommunications reported the occurrence of software failures once per day, and another two companies from media & entertainment, and retail merchandising sectors reported their occurrence several times a day in the last year.

The above results indicate that the majority of UK companies that responded suffered from software failures in the last year; however, the figures indicate their infrequent occurrence, since the majority of respondents claimed that they happened no more often than once per month.

Sabotage or intentional destruction of computing equipment

The results in Table 4.69 show that the intentional destruction of computing equipment remains rare in UK companies. The results reveal that 90.5 percent of respondents reported the non-occurrence of any sabotage acts within their companies in the last year, while the remaining 9.5 percent reported only infrequent occurrence of sabotage. The figures show that five respondents reported its occurrence once in the last year, while only one respondent believed that the company suffered from sabotage once per month.

The analysis by industry sector (Table 4.81) reveals that all respondents from media & entertainment, property & construction, and retail merchandising claimed that sabotage never happened within their companies in the last year, which is followed by insurance & financial services (90.9 percent), manufacturing (90 percent), energy & utilities (77.8 percent), and technology & telecommunications (75 percent).

Table 4.81 Cross-tabulation of sabotage or intentional destruction of computing equipment by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	10		9		5		13		7		6		7		57
%		17.5		15.8		8.8		22.8		12.3		10.5		12.3	
Industry %		90.9		90		100		100		100		75		77.8	
Once a year	1		1		0		0		0		1		2		5
%		20		20		0		0		0		20		40	
Industry %		9.1		10		0		0		0		12.5		22.2	
Once a month	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		12.5		0	
Total	11		10		5		13		7		8		9		63

Table 4.81 also shows that the five respondents who reported the occurrence of sabotage once in the last year are from insurance & financial services, manufacturing, technology & telecommunications, and energy & utilities sectors. On the other hand, only one respondent, who is from technology & telecommunications, believed sabotage occurred once per month. The results, therefore, indicate the rare occurrence of sabotage in media & entertainment, property & construction, and retail merchandising, and its infrequent occurrence in the other sectors that responded.

Natural disasters e.g. fire, floods, earthquakes, etc.

Despite the severe floods that hit many places in the UK last year, the results in Table 4.69 show that 69.8 percent of companies reported the non-occurrence of any natural disasters in the last year, whereas 30.2 percent of companies reported their occurrence once in the last year. These results indicate the infrequent occurrence of natural disasters that have a significant effect on the computing equipment and systems in UK companies.

Table 4.82 Cross-tabulation of natural disasters by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
None	9		7		2		10		5		6		5		44
%		20.5		15.9		4.5		22.7		11.4		13.6		11.4	
Industry %		81.8		70		40		76.9		71.4		75		55.6	
Once a year	2		3		3		3		2		2		4		19
%		10.5		15.8		15.8		15.8		10.5		10.5		21.1	
Industry %		18.2		30		60		23.1		28.6		25		44.4	
Total	11		10		5		13		7		8		9		63

Further analysis (Table 4.82) reveals that 81.8 percent of insurance & financial services companies claimed that no natural disasters had occurred in the last year, followed by property & construction (76.9 percent), technology & telecommunications (75 percent), retail merchandising (71.4 percent), manufacturing (70 percent), and energy & utilities (55.6 percent). On the other hand, only 40 percent of media & entertainment companies maintained this. The results also show that 18.2 percent of insurance & financial services companies believed that they had been affected by natural disasters in the last year, while 60 percent of respondents from media & entertainment had the same idea. The results, therefore, suggest the low level of occurrence of natural disasters in UK companies that responded.

Table 4.83 Results of Kruskal-Wallis test regarding the frequency of occurrence of each type of AIS security threats

Types of AIS security threats	Industry sectors	N	Mean Rank
Unauthorised access to data/systems by disgruntled employees	Insurance & financial services	11	32.95
	Manufacturing	10	33.80
	Media & entertainment	5	44.60
	Property & construction	13	24.50
	Retail merchandising	7	33.36
	Technology & telecommunications	8	40
	Energy & utilities	9	24.50
Chi-square value (χ^2) = 14.142, df = 6, and p-value = 0.028			
Unauthorised access to data/systems by hackers	Insurance & financial services	11	31
	Manufacturing	10	31.40
	Media & entertainment	5	34
	Property & construction	13	28
	Retail merchandising	7	32.29
	Technology & telecommunications	7	36.57
	Energy & utilities	9	31.33
Chi-square value (χ^2) = 3.852, df = 6, and p-value = 0.697			
Unintentional destruction of data by employees	Insurance & financial services	10	25.40
	Manufacturing	9	35.39
	Media & entertainment	5	36.10
	Property & construction	13	22.50
	Retail merchandising	7	38.07
	Technology & telecommunications	7	31.36
	Energy & utilities	9	33.17
Chi-square value (χ^2) = 7.040, df = 6, and p-value = 0.317			
Intentional destruction of data by employees	Insurance & financial services	11	27.73
	Manufacturing	10	28
	Media & entertainment	5	37
	Property & construction	12	25
	Retail merchandising	6	35
	Technology & telecommunications	8	37
	Energy & utilities	9	35
Chi-square value (χ^2) = 8.985, df = 6, and p-value = 0.174			
Theft of physical information e.g. printed output, computer disks, etc.	Insurance & financial services	11	31.09
	Manufacturing	10	31.20
	Media & entertainment	5	32.40
	Property & construction	12	25.50
	Retail merchandising	6	40.50
	Technology & telecommunications	7	29.57
	Energy & utilities	9	28.67
Chi-square value (χ^2) = 7.522, df = 6, and p-value = 0.275			
Introduction of computer viruses, bombs or worms to the system	Insurance & financial services	11	26.36
	Manufacturing	10	28.75
	Media & entertainment	5	39.40
	Property & construction	13	32.62
	Retail merchandising	7	36.36
	Technology & telecommunications	8	28.75
	Energy & utilities	9	37
Chi-square value (χ^2) = 4.127, df = 6, and p-value = 0.660			
Spamming attacks	Insurance & financial services	11	29.55
	Manufacturing	9	25.89
	Media & entertainment	5	39.50
	Property & construction	13	25.96
	Retail merchandising	7	25.21
	Technology & telecommunications	7	33.79
	Energy & utilities	9	42.78
Chi-square value (χ^2) = 8.476, df = 6, and p-value = 0.205			
Malware (spyware, adware) programs	Insurance & financial services	11	27.68
	Manufacturing	10	23.65
	Media & entertainment	5	37.70
	Property & construction	13	30.23
	Retail merchandising	7	32.14
	Technology & telecommunications	8	40.88
	Energy & utilities	9	37.94
Chi-square value (χ^2) = 6.514, df = 6, and p-value = 0.368			
Sharing of passwords	Insurance & financial services	9	27.28
	Manufacturing	9	27.67
	Media & entertainment	5	32.40

	Property & construction	13	20
	Retail merchandising	7	52.36
	Technology & telecommunications	7	29.29
	Energy & utilities	9	31.33
Chi-square value (χ^2) = 17.958, df = 6, and p-value = 0.006			
Theft of software	Insurance & financial services	11	28
	Manufacturing	10	28.70
	Media & entertainment	5	38.90
	Property & construction	13	27.96
	Retail merchandising	6	30.08
	Technology & telecommunications	8	41.88
	Energy & utilities	9	31.61
Chi-square value (χ^2) = 9.854, df = 6, and p-value = 0.131			
Technical software failures or errors	Insurance & financial services	11	27.91
	Manufacturing	10	26.80
	Media & entertainment	5	35.10
	Property & construction	13	37.19
	Retail merchandising	7	38.57
	Technology & telecommunications	7	26.36
	Energy & utilities	9	29.39
Chi-square value (χ^2) = 4.854, df = 6, and p-value = 0.563			
Sabotage or intentional destruction of computer equipment	Insurance & financial services	11	31.82
	Manufacturing	10	32.10
	Media & entertainment	5	29
	Property & construction	13	29
	Retail merchandising	7	29
	Technology & telecommunications	8	37.13
	Energy & utilities	9	35.89
Chi-square value (χ^2) = 6.571, df = 6, and p-value = 0.362			
Natural disasters e.g. fire, floods, earthquakes, etc.	Insurance & financial services	11	28.23
	Manufacturing	10	31.95
	Media & entertainment	5	41.40
	Property & construction	13	29.77
	Retail merchandising	7	31.50
	Technology & telecommunications	8	30.38
	Energy & utilities	9	36.50

In order to test the hypothesis and to examine whether the different types of AIS security threats and their frequency of occurrence vary among industry sectors, a Kruskal-Wallis test was conducted. The results (Table 4.83) do not indicate any statistically significant differences, at the 0.05 level, in the distribution of responses among the different industry sectors except for the unauthorised access to data or systems by disgruntled employees, and employees' sharing of passwords. The results, therefore, indicate that there are significant differences in the distribution of responses among the different industry sectors regarding these two threats, given that their p-values are 0.028 and 0.006 respectively. On the other hand, there are no significant differences in the distribution of responses among the different sectors regarding types and frequency of occurrence for the other AIS security threats, given that their p-values are greater than 0.05.

Overall, the results of this section suggest that employees are now the most common source of AIS security threats facing UK companies that responded. The common sources of security threats are now believed to come more from inside companies than

from outside, given that the majority of respondents consider authorised users or employees to be the most common source of security threats to their companies, with competitors and customers being the least common sources of threats.

The results also indicate the infrequent occurrence of some types of security threats in these companies such as the intentional destruction of data by employees, theft of physical information, theft of software, sabotage, and natural disasters. The results highlight the frequent occurrence of employees' errors that is unintentional destruction of data by employees, spamming and malware attacks, and employees' sharing of passwords. Consequently, companies must pay more attention to those threats and should implement effective controls accordingly.

4.7 AIS security controls

Having identified the most common sources and types of AIS security threats facing UK companies, the next step is to investigate the different types of AIS security controls that companies are currently using, or are planning to use in order to reduce their security threats.

According to Whitman (2003), knowing the 'enemy' that faces information security is a vital component to shaping a security defence posture. Accountants, as well as users, managers, and designers of AIS should be knowledgeable about security threats and appropriate control techniques in order to protect their own systems (Beard and Wen 2007). In addition, Chang and Yeh (2006) have argued that a lack of robust security protection raises the information security threat to companies. Consequently, companies need to understand the security requirements most relevant to their industry sector and should prepare appropriate security countermeasures to minimise threats.

In order to investigate AIS security controls, this section presents the questionnaire results on the different types of AIS security controls that UK companies in different sectors are using or are planning to use (Section 3 of the questionnaire). In addition, the questionnaire results of both Sections 2 and 3 are used to analyse the degree of correlation between different types of AIS security threats facing UK companies, and

the different types of security controls used to reduce such threats. This section also examines the effect of these controls on the reduction of companies' security threats. This section also investigates the degree of correlation between an AIS security effectiveness level (Section 1.7 of the questionnaire) and the different types of threats, and the effect of this on the reduction of these threats. Consequently, this section is concerned with testing Hypotheses 3, 4 and 5 (Section 3.2.4 in Chapter 3). These three hypotheses can be expressed as follows:

H3: There are no significant differences among UK companies in different industry sectors concerning the types of controls implemented to prevent or reduce security threats.

H4: There is no significant relationship between the different types of security controls and the reduction of AIS security threats facing UK companies.

H5: There is no significant relationship between AIS security effectiveness and the AIS security threat level in UK companies.

In order to test the first hypothesis, respondents were asked one question (Section 3 of the questionnaire). Respondents were provided with a list of AIS security controls, which were grouped under seven sub-titles, and they were asked to indicate whether their companies are currently using each of these controls, are planning to use them, or have no plans to use them.

Administrative/organisational security controls

The results in Table 4.84 show that only 38.3 percent of companies believed that they have reorganised AIS security functions and 20 percent reported that they are planning to do so. On the other hand, 41.7 percent of respondents confirmed the non-existence of reorganised AIS security functions within their companies. The results indicate that the majority of respondents are not concerned with reorganising their security functions.

Table 4.84 Organisational security controls used in UK companies

Organisational security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Reorganised AIS security functions	23	38.3	12	20	25	41.7	60
Continuous auditing techniques	33	52.4	9	14.3	21	33.3	63
Real time security awareness/incident response	24	38.7	14	22.6	24	38.7	62
Disaster recovery and business continuity plan	53	84.1	8	12.7	2	3.2	63

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

Further analysis (Table 4.85) reveals that retail merchandising appears to be the most likely sector to be concerned with this control, since two thirds of companies reported the existence of reorganised AIS security functions. On the other hand, only 10 percent of respondents from the manufacturing sector reported this. The results also show that 55.6 percent of the energy & utilities companies confirmed that they are not planning to reorganise their security functions and half the companies in each of the following sectors - insurance & financial services, manufacturing, and property & construction - held a similar view.

Table 4.85 Cross-tabulation of reorganised AIS security functions by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	4		1		3		4		4		4		3		23
%		17.4		4.3		13		17.4		17.4		17.4		13	
Industry %		40		10		50		33.3		66.7		57.1		33.3	
No, but plans to	1		4		1		2		0		3		1		12
%		8.3		33.3		8.3		16.7		0		25		8.3	
Industry %		10		40		16.7		16.7		0		42.9		11.1	
No, and no plans to	5		5		2		6		2		0		5		25
%		20		20		8		24		8		0		20	
Industry %		50		50		33.3		50		33.3		0		55.6	
Total	10		10		6		12		6		7		9		60

Table 4.84 also reveals that 52.4 percent of the companies claimed that they have continuous auditing techniques, whereas one third of companies have no plans to have them. This result is consistent with the result in Section 4.5.4 in which nearly half the companies (47.2 percent) reported that they are undertaking a security audit after suffering from a security incident. In addition, the majority of companies that responded (Section 4.5.7) claimed that they depend mainly on internal and external audits to evaluate AIS security effectiveness.

Further analysis (Table 4.86) reveals that two thirds of media & entertainment companies confirmed the existence of continuous auditing techniques, while only 40

percent of manufacturing companies confirmed their existence. Interestingly, only 45.5 percent of insurance & financial services companies reported the existence of these auditing techniques, despite being the most likely sector to be concerned with security. On the other hand, half the respondents from the manufacturing sector stated that they are not planning to undertake continuous auditing, while only one respondent from energy & utilities claimed that they were. The results, therefore, indicate that manufacturing companies need to be more concerned than they appear to be with auditing techniques.

Table 4.86 Cross-tabulation of continuous auditing techniques by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	5		4		4		7		4		4		5		33
%		15.2		12.1		12.1		21.2		12.1		12.1		15.2	
Industry %		45.5		40		66.7		53.8		57.1		57.1		55.6	
No, but plans to	2		1		1		1		0		1		3		9
%		22.2		11.1		11.1		11.1		0		11.1		33.3	
Industry %		18.2		10		16.7		7.7		0		14.3		33.3	
No, and no plans to	4		5		1		5		3		2		1		21
%		19		23.8		4.8		23.8		14.3		9.5		4.8	
Industry %		36.4		50		16.7		38.5		42.9		28.6		11.1	
Total	11		10		6		13		7		7		9		63

Table 4.87 Cross-tabulation of real time security awareness/incident response by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	6		2		3		5		3		2		3		24
%		25		8.3		12.5		20.8		12.5		8.3		12.5	
Industry %		54.5		22.2		50		38.5		42.9		28.6		33.3	
No, but plans to	2		2		2		2		2		2		2		14
%		14.3		14.3		14.3		14.3		14.3		14.3		14.3	
Industry %		18.2		22.2		33.3		15.4		28.6		28.6		22.2	
No, and no plans to	3		5		1		6		2		3		4		24
%		12.5		20.8		4.2		25		8.3		12.5		16.7	
Industry %		27.3		55.6		16.7		46.2		28.6		42.9		44.4	
Total	11		9		6		13		7		7		9		62

From Table 4.84 it can be seen that 38.7 percent of companies reported the existence of real time security awareness and incident response; 22.6 percent claimed that they are planning to do this; whereas another 38.7 percent have no plans to do so. Further analysis (Table 4.87) reveals that 55.6 percent of the manufacturing companies reported that they do not undertake real time security awareness and incident response, and they have no plans to do so, while only one respondent from media & entertainment held this opinion. The results, therefore, suggest that manufacturing

companies are less concerned about real time security awareness, which is consistent with the results presented in Section 4.5.2, in which manufacturing companies appear to devote less effort to raising security awareness compared to the other sectors.

Table 4.84 reveals that 84.1 percent of companies reported the existence of disaster recovery and business continuity plans. This result is consistent with that in Section 4.5.4. On the other hand, only 3.2 percent of companies do not have and are not planning to have disaster recovery and business continuity plans. This suggests that UK companies that responded are aware of the importance of having a current disaster recovery plan. In addition, the analysis by sectors (Table 4.88) reveals that all respondents from retail merchandising, and technology & telecommunications believed that they have a disaster recovery plan in place. On the other hand, only two companies from the insurance & financial services and manufacturing sectors reported that they have no disaster recovery plans, and they are not planning to have any.

Table 4.88 Cross-tabulation of disaster recovery and business continuity plan by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	10		6		5		10		7		7		8		53
%		18.9		11.3		9.4		18.9		13.2		13.2		15.1	
Industry %		90.9		60		83.3		76.9		100		100		88.9	
No, but plans to	0		3		1		3		0		0		1		8
%		0		37.5		12.5		37.5		0		0		12.5	
Industry %		0		30		16.7		23.1		0		0		11.1	
No, and no plans to	1		1		0		0		0		0		0		2
%		50		50		0		0		0		0		0	
Industry %		9.1		10		0		0		0		0		0	
Total	11		10		6		13		7		7		9		63

Based on the above results, it can be concluded that the manufacturing sector is the least likely to be concerned with organisational security controls and should pay more attention to this type of security control.

Personnel security controls

Since employees are a major threat to their companies' systems, respondents were asked about the existence of five personnel security controls within their companies.

Table 4.89 Personnel security controls used in UK companies

Personnel security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Background investigation/reference checks	46	75.4	4	6.6	11	18	61
Signing of confidentiality agreement by employees	53	84.1	2	3.2	8	12.7	63
Security training and awareness programs	26	41.3	16	25.4	21	33.3	63
Segregation of duties	49	77.8	4	6.3	10	15.9	63
Mandatory vacations	15	24.2	1	1.6	46	74.2	62

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

Table 4.89 shows that 75.4 percent of companies indicated that they are doing background investigations for their employees, while 24.6 percent of companies reported the non-existence of these controls. In addition, Table 4.90 reveals that all media & entertainment companies confirmed that they are undertaking background checks, followed by insurance & financial services (90.9 percent), whereas 44.4 percent of the manufacturing companies we re doing this. However, another 44.4 percent of manufacturing companies reported that they are not undertaking background checks and are not planning to do so. The results, therefore, indicate that media & entertainment is the sector most concerned with undertaking reference checks for its employees, while manufacturing is the least concerned.

Table 4.90 Cross-tabulation of background investigations/reference checks by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	10		4		5		11		3		7		6		46
%		21.7		8.7		10.9		23.9		6.5		15.2		13	
Industry %		90.9		44.4		100		84.6		50		87.5		66.7	
No, but plans to	0		1		0		0		2		0		1		4
%		0		25		0		0		50		0		25	
Industry %		0		11.1		0		0		33.3		0		11.1	
No, and no plans to	1		4		0		2		1		1		2		11
%		9.1		36.4		0		18.2		9.1		9.1		18.2	
Industry %		9.1		44.4		0		15.4		16.7		12.5		22.2	
Total	11		9		5		13		6		8		9		61

Regarding a confidentiality agreement, Table 4.89 shows that 84.1 percent of companies require their employees to sign a confidentiality agreement before joining the company, while only 15.9 percent of companies do not do so. Further analysis (Table 4.91) reveals that all media & entertainment and technology & telecommunications companies reported that employees sign a confidentiality agreement before joining, followed by insurance & financial services (90.9 percent).

Table 4.91 Cross-tabulation of signing of confidentiality agreement by employees by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	10		8		5		10		6		8		6		53
%		18.9		15.1		9.4		18.9		11.3		15.1		11.3	
Industry %		90.9		80		100		76.9		85.7		100		66.7	
No, but plans to	0		0		0		1		0		0		1		2
%		0		0		0		50		0		0		50	
Industry %		0		0		0		7.7		0		0		11.1	
No, and no plans to	1		2		0		2		1		0		2		8
%		12.5		25		0		25		12.5		0		25	
Industry %		9.1		20		0		15.4		14.3		0		22.2	
Total	11		10		5		13		7		8		9		63

On the other hand, 22.2 percent of respondents from energy & utilities claimed that employees do not sign a confidentiality agreement and their companies are not planning to oblige them to do so. These results indicate that media & entertainment and technology & telecommunications sectors are more concerned with this control than the other sectors that responded.

Table 4.89 also shows that 41.3 percent of companies reported the existence of security training and awareness programs, while 58.7 percent of companies claimed the non-existence of these programs. This result is consistent with the result in Section 4.5.2, which revealed that UK companies that responded do not pay much attention to security training and awareness programs.

Table 4.92 Cross-tabulation of security training and awareness programs by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	7		2		3		3		4		4		3		26
%		26.9		7.7		11.5		11.5		15.4		15.4		11.5	
Industry %		63.6		20		50		23.1		57.1		57.1		33.3	
No, but plans to	1		2		3		4		1		1		4		16
%		6.3		12.5		18.8		25		6.3		6.3		25	
Industry %		9.1		20		50		30.8		14.3		14.3		44.4	
No, and no plans to	3		6		0		6		2		2		2		21
%		14.3		28.6		0		28.6		9.5		9.5		9.5	
Industry %		27.3		60		0		46.2		28.6		28.6		22.2	
Total	11		10		6		13		7		7		9		63

Moreover, Table 4.92 reveals that the insurance & financial services sector is most concerned with training its employees and with raising their security awareness. The results show that 63.6 percent of companies reported the existence of security training and awareness programs, but only 20 percent of companies from the manufacturing

sector had the same opinion. On the other hand, three fifths of manufacturing companies reported that they do not have these training programs, and they are not planning to have them.

From Table 4.89, it can be seen that 77.8 percent of companies confirmed that they are segregating employees' duties, while only 22.2 percent reported the non-existence of this security control. Further analysis (Table 4.93) reveals that all respondents from retail merchandising reported the segregation of duties within their companies, followed by insurance & financial services with 90.9 percent. On the other hand, 38.5 percent of property & construction companies do not segregate employees' duties. The results, therefore, indicate that the retail merchandising sector pays more attention to the segregation of duties than other sectors.

Table 4.93 Cross-tabulation of segregation of duties by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	10		7		4		8		7		6		7		49
%		20.4		14.3		8.2		16.3		14.3		12.2		14.3	
Industry %		90.9		70		66.7		61.5		100		85.7		77.8	
No, but plans to	0		2		0		0		0		1		1		4
%		0		50		0		0		0		25		25	
Industry %		0		20		0		0		0		14.3		11.1	
No, and no plans to	1		1		2		5		0		0		1		10
%		10		10		20		50		0		0		10	
Industry %		9.1		10		33.3		38.5		0		0		11.1	
Total	11		10		6		13		7		7		9		63

It can also be seen from Table 4.89 that the majority of companies that responded are not concerned about giving their employees mandatory vacations. The results reveal that 24.2 percent of companies acknowledged the existence of mandatory vacations, whereas 75.8 percent of respondents claimed that they did not take these vacations. In addition, Table 4.94 shows that 54.5 percent of the insurance & financial services companies claimed that they are applying mandatory vacations, followed by energy & utilities (33.3 percent). On the other hand, 85.7 percent of technology & telecommunications companies reported that they do not apply these safeguards, and they are not planning to do so, followed by property & construction (84.6 percent), media & entertainment, retail merchandising (83.3 percent) and manufacturing (80 percent). It is clear that the majority of UK companies that responded do not consider mandatory vacations as an important AIS security control.

Table 4.94 Cross-tabulation of mandatory vacations by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	6		2		1		2		1		0		3		15
%		40		13.3		6.7		13.3		6.7		0		20	
Industry %		54.5		20		16.7		15.4		16.7		0		33.3	
No, but plans to	0		0		0		0		0		1		0		1
%		0		0		0		0		0		100		0	
Industry %		0		0		0		0		0		14.3		0	
No, and no plans to	5		8		5		11		5		6		6		46
%		10.9		17.4		10.9		23.9		10.9		13		13	
Industry %		45.5		80		83.3		84.6		83.3		85.7		66.7	
Total	11		10		6		13		6		7		9		62

Based on the above, it seems that the majority of UK companies that responded are more concerned with undertaking background checks for their employees, they require their employees to sign confidentiality agreement before joining, and they pay great attention to the segregation of duties. Thus, more attention should be given to security training and awareness and to the mandatory vacations.

Software security controls

The results in Table 4.95 reveal that the vast majority of companies responded (98.4 percent) test software before using it, while only one company does not do so. The results reveal that this company is from the insurance & financial services sector. This is a surprising result given the nature of financial services companies.

Table 4.95 Software security controls used in UK companies

Software security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Testing software before use	61	98.4	0	0	1	1.6	62
Off-site storage of original software	45	71.4	4	6.3	14	22.2	63
Safeguards against unauthorised access to software	62	98.4	0	0	1	1.6	63
Software audit alert tools	37	58.7	11	17.5	15	23.8	63
Virus protection software	64	100	0	0	0	0	64
Cancelling passwords for terminated employees	64	100	0	0	0	0	64
Intrusion prevention/detection software	42	65.6	15	23.4	7	10.9	64
Insurance coverage for software	26	41.9	1	1.6	35	56.5	62

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

It can also be seen from Table 4.95 that 71.4 percent of companies reported that they store their original software off-site, whereas 22.2 percent do not do so, and are not planning to do so.

Moreover, Table 4.96 shows that all respondents from media & entertainment confirmed that their companies store the original software off-site, followed by insurance & financial services with 90.9 percent. On the other hand, 46.2 percent of the property & construction companies do not do this. The results, therefore, suggest that the media & entertainment and insurance & financial services are more concerned than the other sectors about their software, and store it off-site.

Table 4.96 Cross-tabulation of off-site storage of original software by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	10		6		6		7		5		5		6		45
%		22.2		13.3		13.3		15.6		11.1		11.1		13.3	
Industry %		90.9		60		100		53.8		71.4		71.4		66.7	
No, but plans to	1		1		0		0		1		1		0		4
%		25		25		0		0		25		25		0	
Industry %		9.1		10		0		0		14.3		14.3		0	
No, and no plans to	0		3		0		6		1		1		3		14
%		0		21.4		0		42.9		7.1		7.1		21.4	
Industry %		0		30		0		46.2		14.3		14.3		33.3	
Total	11		10		6		13		7		7		9		63

The results in Table 4.95 show that the vast majority of UK companies that responded (98.4 percent) use safeguards against unauthorised access to their software, while only one company reported the non-existence of these controls. The results reveal that this company is from the property & construction sector. The results highlight the attention given by UK companies towards their software.

Table 4.97 Cross-tabulation of software audit alert tools by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	7		5		6		7		4		4		4		37
%		18.9		13.5		16.2		18.9		10.8		10.8		10.8	
Industry %		63.6		50		100		53.8		57.1		57.1		44.4	
No, but plans to	2		2		0		1		1		2		3		11
%		18.2		18.2		0		9.1		9.1		18.2		27.3	
Industry %		18.2		20		0		7.7		14.3		28.6		33.3	
No, and no plans to	2		3		0		5		2		1		2		15
%		13.3		20		0		33.3		13.3		6.7		13.3	
Industry %		18.2		30		0		38.5		28.6		14.3		22.2	
Total	11		10		6		13		7		7		9		63

It can also be seen from Table 4.95 that 58.7 percent of companies claimed that they use software audit alert tools, while 23.8 percent of companies do not use them and have no plans to do so.

Further analysis (Table 4.97) reveals that all media & entertainment companies confirmed that they use software audit alert tools, followed by insurance & financial services (63.6 percent), but only 44.4 percent of energy & utilities companies claimed to do so. On the other hand, the results show that 38.5 percent of the property & construction companies reported that they are not planning to use these alert tools, followed by manufacturing (30 percent). The results indicate that media & entertainment companies are more concerned with this security control than the other companies.

The BERR Information Security Breaches Survey (BERR 2008) indicated that "anti-virus control" is one of the areas where almost all companies, irrespective of size, sector, or location agree on the need for controls. This can be seen from Table 4.95 in which all respondents from all industry sectors reported that their companies had installed virus protection software. At the same time, the results show that all respondents from all industry sectors claimed that their companies are cancelling passwords for terminated employees, which is a very important security control to avoid unauthorised access to companies' important software.

It can also be seen from Table 4.95 that 65.5 percent of companies use intrusion prevention or detection software, while 10.9 percent of companies do not use this software, and are not planning to do so. This result is consistent with the CSI Survey (Richardson 2007) in which 69 percent of companies reported the existence of intrusion detection systems and 47 percent reported the existence of intrusion prevention systems. Furthermore, the results in Table 4.98 reveal that all respondents from media & entertainment reported that intrusion prevention or detection software is installed within their companies, followed by retail merchandising (85.7 percent), while only 37.5 percent of technology & telecommunications companies reported that they had installed intrusion prevention or detection software. However, 30 percent of manufacturing companies do not have this software, and they are not planning to install it. The results indicate that media & entertainment companies that responded are also more concerned with installing this software.

Table 4.98 Cross-tabulation of intrusion prevention/detection software by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	9		4		6		9		6		3		5		42
%		21.4		9.5		14.3		21.4		14.3		7.1		11.9	
Industry %		81.8		40		100		69.2		85.7		37.5		55.6	
No, but plans to	1		3		0		2		1		4		4		15
%		6.7		20		0		13.3		6.7		26.7		26.7	
Industry %		9.1		30		0		15.4		14.3		50		44.4	
No, and no plans to	1		3		0		2		0		1		0		7
%		14.3		42.9		0		28.6		0		14.3		0	
Industry %		9.1		30		0		15.4		0		12.5		0	
Total	11		10		6		13		7		8		9		64

Table 4.99 Cross-tabulation of insurance coverage for software by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	6		3		3		9		2		3		0		26
%		23.1		11.5		11.5		34.6		7.7		11.5		0	
Industry %		54.5		30		50		69.2		33.3		42.9		0	
No, but plans to	0		0		1		0		0		0		0		1
%		0		0		100		0		0		0		0	
Industry %		0		0		16.7		0		0		0		0	
No, and no plans to	5		7		2		4		4		4		9		35
%		14.3		20		5.7		11.4		11.4		11.4		25.7	
Industry %		45.5		70		33.3		30.8		66.7		57.1		100	
Total	11		10		6		13		6		7		9		62

Table 4.95 reveals that 41.9 percent of companies are concerned about having insurance coverage for their software, while 56.5 percent of the companies do not have software insurance coverage, and they have no plans to introduce it. This could be because the majority of UK companies that responded do not have a sufficient security budget, and therefore they cannot justify the spending on insurance coverage. It can also be seen from Table 4.99 that 69.2 percent of property & construction companies reported the existence of insurance coverage for their software, followed by insurance & financial services (54.5 percent), with only 30 percent of manufacturing companies reporting this. However, no energy & utilities companies have software insurance coverage, nor does 70 percent of the manufacturing sector.

Based on the above, it is clear that almost all UK companies that responded agree on the importance of certain controls such as virus protection software, cancellation of passwords for terminated employees, testing their software before its use, and safeguards against unauthorised access to software. On the other hand, more attention must be paid to software insurance coverage, and software audit alert tools.

Hardware/physical security controls

It is not surprising to see from Table 4.100 that all respondents from all industry sectors reported that their companies make back-ups for their hard disks, and use firewalls. This result is consistent with most previous studies. The BERR Information Security Breaches Survey (BERR 2008) indicated that almost every UK company makes back-ups, and that firewalls appear to be the basic pre-requisite for other security mechanisms. The CSI Survey (Richardson 2007) also stated that all companies reported the use of firewalls.

Table 4.100 Hardware/physical security controls used in UK companies

Hardware/physical security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Back-up for hard disks	64	100	0	0	0	0	64
Firewalls	64	100	0	0	0	0	64
Penetration testing	45	71.4	8	12.7	10	15.9	63
Restricting access to the main computing facilities	61	95.3	1	1.6	2	3.1	64
Security alarm system	59	93.7	1	1.6	3	4.8	63
Biometric techniques	9	14.5	6	9.7	47	75.8	62
Storing unused laptops in secure/locked cabinets	43	68.3	4	6.3	16	25.4	63
Placement of authorisation/database/accounting servers in secure location	59	93.7	0	0	4	6.3	63
Protecting computers from natural disasters e.g. air conditioners, etc.	59	92.2	1	1.6	4	6.3	64
Insurance coverage for hardware/computer devices	49	77.8	1	1.6	13	20.6	63

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

Table 4.101 Cross-tabulation of penetration testing by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	7		6		6		7		5		6		8		45
%		15.6		13.3		13.3		15.6		11.1		13.3		17.8	
Industry %		63.6		60		100		53.8		71.4		85.7		88.9	
No, but plans to	1		1		0		3		2		0		1		8
%		12.5		12.5		0		37.5		25		0		12.5	
Industry %		9.1		10		0		23.1		28.6		0		11.1	
No, and no plans to	3		3		0		3		0		1		0		10
%		30		30		0		30		0		10		0	
Industry %		27.3		30		0		23.1		0		14.3		0	
Total	11		10		6		13		7		7		9		63

Table 4.100 also reveals that 71.4 percent of companies undertake penetration testing, whereas 15.9 percent of companies are not planning to do so. Further analysis (Table 4.101) reveals that all media & entertainment companies claimed the usage of penetration testing, followed by energy & utilities (88.9 percent). This result is consistent with that in Section 4.5.7 in which the majority of companies from media & entertainment claimed the usage of penetration testing in evaluating AIS security

effectiveness. On the other hand, 30 percent of manufacturing companies stated that they do not undertake penetration testing and are not planning to do so.

The results in Table 4.100 show that 95.3 percent of companies restrict access to their main computing facilities, while only two companies do not, and have no plans to do so. This result is consistent with the DTI Information Security Breaches Survey (DTI 2006), in which nearly 97 percent of companies restricted access to computing facilities through locks. Interestingly, the results shows that all respondents from media & entertainment, property & construction, retail merchandising, and technology & telecommunications sectors reported that their companies restrict access to their main computing facilities. On the other hand, the two companies who claimed that they do not do so are from the insurance & financial services and manufacturing sectors.

Table 4.100 also shows that the majority of companies that responded (93.7 percent) use security alarm systems, while 6.3 percent reported the non-existence of this control. Further analysis reveals that all respondents from insurance & financial services, media & entertainment, and retail merchandising reported the existence of security alarm system within their companies; whereas only three companies from manufacturing, property & construction, and technology & telecommunications sectors claimed that they do not have and are not planning to have security alarm systems.

Regarding biometrics, Table 4.100 shows that 75.8 percent of companies have no plans to use biometric techniques, whereas only 14.5 percent of companies claimed the existence of these techniques. This result is consistent with most previous studies. Amoruso *et al.* (2005) and Chandra and Calderson (2005) argued that the use of biometric technologies in business and accounting is still in its infancy. The Global Security Survey (DTT 2006) confirmed their opinion and indicated that 11 percent of companies deployed biometrics, while 21 percent stated that they would be piloting or deploying biometric techniques over the next 18 months. In addition, the Security and Information Risk Survey (NCC 2007) stated that over 62 percent of companies have no plans at all for introducing biometrics.

Table 4.102 Cross-tabulation of biometric techniques by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	2		0		2		2		2		1		0		9
%		22.2		0		22.2		22.2		22.2		11.1		0	
Industry %		18.2		0		40		15.4		28.6		14.3		0	
No, but plans to	2		0		1		0		0		1		2		6
%		33.3		0		16.7		0		0		16.7		33.3	
Industry %		18.2		0		20		0		0		14.3		22.2	
No, and no plans to	7		10		2		11		5		5		7		47
%		14.9		21.3		4.3		23.4		10.6		10.6		14.9	
Industry %		63.6		100		40		84.6		71.4		71.4		77.8	
Total	11		10		5		13		7		7		9		62

Further analysis (Table 4.102) reveals that no manufacturing companies use biometrics, and are not planning to do so, followed by property & construction (84.6 percent), energy & utilities (77.8 percent), retail merchandising and technology & telecommunications (71.4 percent). The results, therefore, indicate that the majority of UK companies that responded do not use and are not planning to use biometric techniques.

Table 4.103 Cross-tabulation of storing unused laptops in secure/locked cabinets by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	9		6		5		9		4		6		4		43
%		20.9		14		11.6		20.9		9.3		14		9.3	
Industry %		90		60		83.3		69.2		57.1		75		44.4	
No, but plans to	0		1		0		0		1		0		2		4
%		0		25		0		0		25		0		50	
Industry %		0		10		0		0		14.3		0		22.2	
No, and no plans to	1		3		1		4		2		2		3		16
%		6.3		18.8		6.3		25		12.5		12.5		18.8	
Industry %		10		30		16.7		30.8		28.6		25		33.3	
Total	10		10		6		13		7		8		9		63

The results in Table 4.100 show that 68.3 percent of companies store unused laptops in locked cabinets, whereas 25.4 percent of companies do not, and have no plans to do so. Table 4.103 reveals that insurance & financial services companies are more concerned about their laptops, given the sensitive nature of financial data stored in them, with 90 percent of respondents reporting that unused laptops are stored in secured cabinets, followed by media & entertainment (83.3 percent), and technology & telecommunications (75 percent). On the other hand, the results show that one third of energy & utilities companies do not store unused laptops in locked cabinets, and

are not planning to do so, followed by property & construction (30.8 percent) and manufacturing (30 percent).

It can be seen from Table 4.100 that 93.7 percent of the companies place authorisation, database and accounting servers in secure locations, while only 6.3 percent of companies do not. It is encouraging to see from the results that all companies from media & entertainment, property & construction, retail merchandising and technology & telecommunications reported that they place authorisation and accounting servers in secure locations. Four respondents from the insurance & financial services, manufacturing, and energy & utilities sectors claimed not to do this.

Regarding the protection from natural disasters, Table 4.100 reveals that 92.2 percent of companies installed air conditioners, fireproofing, smoke detectors, etc. to protect their computers from natural disasters, with only 6.3 percent of companies having no plans to do so. The results reveal that all companies from the media & entertainment, technology & telecommunications and energy & utilities sectors protect their computers from natural disasters. On the other hand, only one respondent from each of the other four sectors claimed that their companies do not protect computers from natural disasters, and are not planning to install protection devices.

Table 4.104 Cross-tabulation of insurance coverage for hardware/computer devices by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	11		6		4		12		5		6		5		49
%		22.4		12.2		8.2		24.5		10.2		12.2		10.2	
Industry %		100		60		80		92.3		71.4		75		55.6	
No, but plans to	0		0		0		0		0		0		1		1
%		0		0		0		0		0		0		100	
Industry %		0		0		0		0		0		0		11.1	
No, and no plans to	0		4		1		1		2		2		3		13
%		0		30.8		7.7		7.7		15.4		15.4		23.1	
Industry %		0		40		20		7.7		28.6		25		33.3	
Total	11		10		5		13		7		8		9		63

Although 41.9 percent of companies reported that they have insurance coverage for their software, it can be seen from Table 4.100 that 77.8 percent of companies that responded reported the existence of insurance coverage for their hardware and computer devices. On the other hand, 20.6 percent are not planning to introduce this.

Further analysis (Table 4.104) reveals that all the insurance & financial services companies agreed on the existence of insurance for their hardware and computer devices, followed by property & construction (92.3 percent), and media & entertainment (80 percent). On the other hand, 40 percent of manufacturing companies had no plans to introduce such insurance coverage.

Based on the above, it can be seen that all companies that responded make back-ups for their hard disks and use firewalls. In addition, the majority of companies restrict access to main computing facilities, have security alarm systems, place their accounting servers in secure locations, and protect their computers from natural disasters. On the other hand, the majority of companies do not use and have no plans to use biometrics.

Input/data security controls

It is encouraging to see from Table 4.105 that 96.9 percent of companies are concerned about their data, and store data back-ups off-site, while only one respondent claimed that data back-ups are not stored outside company, and there are no plans to do so. The results reveal that this respondent is from the energy & utilities sector. This result suggests that UK companies that responded are more concerned with data security than their software. According to previous results, 22.2 percent of companies reported that they do not store original software off-site, and are not planning to do so.

Table 4.105 Input/data security controls used in UK companies

Input/data security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Off-site storage of data back-ups	62	96.9	1	1.6	1	1.6	64
Encryption of sensitive data	26	41.9	15	24.2	21	33.9	62
User access controls/authorisation	64	100	0	0	0	0	64

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

On the other hand, it can be seen from Table 4.105 that 41.9 percent of companies encrypt their sensitive data, while 33.9 percent of companies have no plans to do so. This result indicates that UK companies that responded do not seem much concerned about encrypting their sensitive data. This result is consistent with the CSI Survey (Richardson 2007), which indicated that only 47 percent of companies are encrypting data in storage. However, this is a surprising result, given that recent press coverage

has highlighted how confidential data can become exposed when computers and laptops are stolen (BERR 2008).

Further analysis (Table 4.106) reveals that media & entertainment companies are more concerned about encrypting their sensitive data than the other sectors. The results show that two thirds of media & entertainment companies reported the encryption of sensitive data, followed by retail merchandising (57.1 percent) and insurance & financial services (54.5 percent), while only 14.3 percent from technology & telecommunications claimed to do so. On the other hand, half the manufacturing companies do not encrypt their sensitive data, and are not planning to do so. This result is not consistent with the BERR Information Security Breaches Survey (BERR 2008), which indicated that the entertainment sectors are least likely to have taken steps to protect data held on PCs and laptops, while financial services and telecommunications had taken more steps.

Table 4.106 Cross-tabulation of the encryption of sensitive data by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	6		3		4		6		4		1		2		26
%		23.1		11.5		15.4		23.1		15.4		3.8		7.7	
Industry %		54.5		30		66.7		46.2		57.1		14.3		25	
No, but plans to	1		2		1		1		2		4		4		15
%		6.7		13.3		6.7		6.7		13.3		26.7		26.7	
Industry %		9.1		20		16.7		7.7		28.6		57.1		50	
No, and no plans to	4		5		1		6		1		2		2		21
%		19		23.8		4.8		28.6		4.8		9.5		9.5	
Industry %		36.4		50		16.7		46.2		14.3		28.6		25	
Total	11		10		6		13		7		7		8		62

Regarding user access controls and authorisations within UK companies, it is encouraging to see from Table 4.105 that all companies from all sectors that responded have user access controls. This result is consistent with the results of Whitman (2004), who indicated that access controls are the most common protection mechanisms employed, with 100 percent of respondents indicating their usage.

The above results indicate that UK companies that responded are giving a great deal of attention to access controls and to their data back-ups; however, more attention should be given to the encryption of sensitive data.

Output security controls

Table 4.107 shows that 96.9 percent of companies are restricting access to their sensitive information, while only one company claimed that it is not doing so nor planning to do so. The results show that this company is from the property & construction sector.

Table 4.107 Output security controls used in UK companies

Output security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Restricting access to sensitive information for authorised users	62	96.9	1	1.6	1	1.6	64
Storing sensitive output in secure/locked cabinets	54	84.4	2	3.1	8	12.5	64

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

The results in Table 4.107 also show that 84.4 percent of respondents believed that sensitive information is stored in secured cabinets within their companies, with 15.6 percent of companies not doing so. Further analysis reveals that all companies from the media & entertainment and energy & utilities sectors store sensitive output in secured cabinets. This result is surprising since the previous results revealed that one third of energy & utilities companies do not store unused laptops in locked cabinets.

Network security controls

In order to be more efficient, effective, and responsive, companies are increasingly using networks and computer-based IS (Dhillon and Backhouse 2000). Companies, therefore, are faced with many security threats, and must prepare for the appropriate controls for these networks.

Table 4.108 Network security controls used in UK companies

Network security controls	Yes		No, but plans to		No, and no plans to		Total
	no	%	no	%	no	%	no
Network encryption	32	50.8	11	17.5	20	31.7	63
Content and e-mail filtering software	57	90.5	2	3.2	4	6.3	63
Malware (spyware, adware) detection tools	61	95.3	1	1.6	2	3.1	64
Spam filtering software	62	96.9	1	1.6	1	1.6	64

Q 3.1 For each of the following security controls, please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it.

It can be seen from Table 4.108 that 50.8 percent of the companies have implemented network encryption, while only 31.7 percent of companies are not planning to do so. The results in Table 4.109 reveal that retail merchandising is the sector most concerned with network encryption, with 85.7 percent of companies doing so,

followed by insurance & financial services (63.6 percent) and technology & telecommunications (57.1 percent). On the other hand, half of the manufacturing companies do not encrypt their network and have no plans to do so, followed by energy & utilities (44.4 percent).

Table 4.109 Cross-tabulation of network encryption by industry sector

	Insurance & financial services		Manufacturing		Media & entertainment		Property & construction		Retail merchandising		Technology & telecommunications		Energy & utilities		Total
	no	%	no	%	no	%	no	%	no	%	no	%	no	%	no
Yes	7		5		3		5		6		4		2		32
%		21.9		15.6		9.4		15.6		18.8		12.5		6.3	
Industry %		63.6		50		50		38.5		85.7		57.1		22.2	
No, but plans to	2		0		1		3		1		1		3		11
%		18.2		0		9.1		27.3		9.1		9.1		27.3	
Industry %		18.2		0		16.7		23.1		14.3		14.3		33.3	
No, and no plans to	2		5		2		5		0		2		4		20
%		10		25		10		25		0		10		20	
Industry %		18.2		50		33.3		38.5		0		28.6		44.4	
Total	11		10		6		13		7		7		9		63

It is encouraging to see from Table 4.108 that the majority of companies that responded (90.5 percent) claimed the existence of content and e-mail filtering software, while onl y 6.3 percent of companies do not filter e-mails and are not planning to do so. This result is consistent with the BERR Information Security Breaches Survey (BERR 2008), which indicated that the number of companies filtering incoming e-mails and scanning outgoing e-mails has gone up. Further analysis reveals that all companies from the manufacturing, media & entertainment, and retail merchandising sectors are filtering their e-mail content. On the other hand, four respondents from insurance & financial services, property & construction and energy & utilities sectors claimed that their companies do not have e-mail filtering software, and are not planning to have it. The results indicate that manufacturing companies are more concerned with this security control than the other security controls.

It can also be seen from Table 4.108 that 95.3 percent of companies reported the existence of malware detection tools, while only 3.1 percent of companies are not planning to use these tools. The results reveal that all companies from insurance & financial services, media & entertainment, property & construction and retail merchandising sectors use malware detection tools. On the other hand, only two respondents, from the manufacturing and energy & utilities sectors, claimed that there

are no plans to use these tools. This result is again consistent with the BERR Information Security Breaches Survey (BERR 2008), which indicated that the majority of businesses now use anti-spyware scanning software, with the energy companies the least likely to be protected against spyware.

Regarding the existence of spam filtering software in UK companies, Table 4.108 reveals that 96.9 percent of companies claimed to use this software, while only one company reported that there are no plans to use it. This company was from property & construction sector. The result suggests that UK companies that responded pay more attention to spamming attacks, and they have prepared themselves well to reduce such attacks, since the results from Table 4.69 revealed that 62.3 percent of companies reported the occurrence of spamming attacks in the last year.

Overall, the above results indicate that the majority of UK companies that responded are now paying, relatively, more attention to software, hardware, input and output security controls than the other security controls. Consequently, these companies should devote more effort in the areas of organisational and personnel security controls, especially reorganising AIS security functions, incident response, security training and awareness, and mandatory vacations. In addition, more attention must be given to software insurance coverage, biometric techniques, data and network encryption.

Table 4.110 Results of the chi-square test for the AIS security controls used in UK companies

AIS security controls	χ^2	df	p-value
Organisational security controls			
Reorganised AIS security functions	1.897	3	0.594
Continuous auditing techniques	0.883	3	0.830
Real time security awareness/incident response	1.589	3	0.662
Disaster recovery and business continuity plan	1.865	3	0.601
Personnel security controls			
Background investigation/reference checks	10.151	3	0.017
Signing of confidentiality agreement by employees	5.013	3	0.171
Security training and awareness programs	5.147	3	0.161
Segregation of duties	2.481	3	0.479
Mandatory vacations	7.740	3	0.052
Software security controls			
Testing software before use	4.712	3	0.194
Off-site storage of original software	5.171	3	0.160
Safeguards against unauthorised access to software	1.894	3	0.595
Software audit alert tools	2.811	3	0.422
Virus protection software	-	-	-
Cancelling passwords for terminated employees	-	-	-
Intrusion prevention/detection software	1.677	3	0.642
Insurance coverage for software	1.573	3	0.665
Hardware/physical security controls			
Back-up for hard disks	-	-	-

Firewalls	-	-	-
Penetration testing	3.594	3	0.309
Restrict access to the main computing facilities	1.221	3	0.748
Security alarm system	1.070	3	0.784
Biometric techniques	1.808	3	0.613
Storing unused laptops in secure/locked cabinets	4.420	3	0.219
Placement of authorisation/database/accounting servers in secure location	2.227	3	0.527
Protecting computers from natural disasters e.g. air conditioners, etc.	3.820	3	0.282
Insurance coverage for hardware/computer devices	4.832	3	0.184
Input/data security controls			
Off-site storage of data back-ups	1.380	3	0.710
Encryption of sensitive data	0.914	3	0.822
User access controls/authorisation	-	-	-
Output security controls			
Restricting access to sensitive information for authorised users	2.440	3	0.486
Storing sensitive output in secure/locked cabinets	0.192	3	0.979
Network security controls			
Network encryption	5.260	3	0.154
Content and e-mail filtering software	3.229	3	0.358
Malware (spyware, adware) detection tools	0.785	3	0.853
Spam filtering software	1.796	3	0.616

Moreover, in order to test Hypothesis 3 and to examine whether the types of AIS security controls differ among industry sectors, a chi-square test was conducted. Despite the differences noticed from the above results, the results of the chi-square tests presented in Table 4.110 provide no evidence of any statistically significant association, at the 0.05 level, between the industry sectors and the different types of AIS security controls, except for the background investigations or reference checks, given that its p-value is 0.017 ($p < 0.05$). On the other hand, the p-values of the other AIS security controls are greater than 0.05, which indicates that there are significant association between the different industry sectors and the existence of background investigations or reference checks for their employees, which in turn indicates that some sectors that responded are concerned with these controls more than the other sectors.

Moreover, in order to test Hypotheses 4 and 5 and to examine the degree of correlation and the effect of the different types of AIS security controls and AIS security effectiveness on the reduction of the different types of security threats facing UK companies, Spearman's rank correlation and multiple regression analysis were used. Spearman's rank correlation was used to give an indication of both the direction and strength of the relationship. Then, 13 regressions were run, and the dependent variable in each regression was one type of AIS security threat, and the independent variables were the different types of security controls and security effectiveness within UK companies.

Table 4.111 The significant relationships between types of AIS security threats and types of AIS security controls using Spearman's rank correlation

	Unauthorised access to data/systems by disgruntled employees	Unauthorised access to data/systems by hackers	Intentional destruction of data by employees	Introduction of computer viruses, bombs or worms to the system	Spamming attacks	Malware (spyware, adware) programs	Sharing of passwords	Theft of software	Technical software failures	Sabotage	Natural disasters
Reorganised AIS security functions					-0.340** (0.009)	-0.375** (0.003)				-0.255* (0.050)	-0.257* (0.047)
Continuous auditing techniques					-0.312* (0.014)						
Real time security awareness/incident response				-0.307* (0.015)	-0.281* (0.030)						
Signing of confidentiality agreement by employees					-0.271* (0.033)						
Security training and awareness programs	-0.261* (0.039)		-0.299* (0.019)		-0.349** (0.006)						
Mandatory vacations					-0.270* (0.037)						
Off-site storage of original software	-0.279* (0.027)										
Software audit alert tools	-0.258* (0.041)							-0.292* (0.021)			

Intrusion prevention/detection software					-0.252* (0.048)						
Penetration testing			-0.291* (0.023)		-0.387** (0.002)	-0.386** (0.002)	-0.344** (0.008)				
Security alarm system				-0.249* (0.049)	-0.260* (0.043)						
Biometric techniques											-0.280* (0.026)
Protecting computers from natural disasters e.g. air conditioners, etc.					-0.334** (0.008)	-0.341** (0.006)					
Insurance coverage for hardware/computer devices		0.302* (0.017)						0.470** (0.000)			
Off-site storage of data back-ups									-0.278* (0.027)		
Encryption of sensitive data					-0.304* (0.018)				-0.340** (0.007)		
Malware (spyware, adware) detection tools									-0.265* (0.036)		

Table 4.111 only presents the statistically significant correlations between the different types of AIS security threats and security controls, in which correlation coefficients (r-values) appear on the first line, and the p-values appear between brackets in the next line.

In page 276, it can be seen from Table 4.111 that there are statistically significant negative correlations, at the 0.05 level, between unauthorised access to data or systems by disgruntled employees, and each of the security training and awareness programs (p-value = 0.039), off-site storage of original software (p-value = 0.027), and software audit alert tools (p-value = 0.041). However, the results reveal that the correlations are weak, given that their r-values are -0.261, -0.279, and -0.258 respectively. This result indicates that if UK companies that responded paid more attention to these security controls, they could reduce the unauthorised access to data or systems by disgruntled employees.

Table 4.111 also shows that there is a statistically significant correlation, at the 0.05 level, between the unauthorised access to data or systems by hackers and the insurance coverage for hardware and computer devices, where p-value is 0.017 ($p < 0.05$); however, a positive sign was found ($r = +0.302$), which is different from the expected sign. This result could be because hackers are now more successful at breaking into the companies' network than before; at the same time companies now have more insurance coverage for their computer devices.

The results in Table 4.111 reveal that there are statistically significant negative correlations, at the 0.05 level, between intentional destruction of data by employees and each of the security training and awareness programs (p-value = 0.019), and penetration testing (p-value = 0.023), given that their r-values are -0.299, and -0.291 respectively. Despite the observed weak correlations, these results indicate that UK companies that responded must make more effort in training their employees, and in raising their security awareness in order to reduce the above threat, since employees are considered the companies' first common source of security threats.

Table 4.111 also reveals that there are statistically significant negative correlations, at the 0.05 level, between the viruses attacks on companies' systems, and both real time

security awareness and incidence response (p-value = 0.015), and the existence of security alarm systems within companies (p-value = 0.049), given that their r-values are -0.307 and -0.249 respectively. This result indicates that if companies paid more attention to security awareness and incident response, and if they installed security alarm systems, the effect of virus attacks could be minimised.

The results in Table 4.111 reveal that there are statistically significant negative correlations, at the 0.01 level, between spamming attacks and each of the reorganised AIS security functions (p-value = 0.009; r-value = -0.340); training and awareness programs (p-value = 0.006; r-value = -0.349); penetration testing (p-value = 0.002; r-value = -0.387); and protection of computers from natural disasters (p-value = 0.008; r-value = -0.334). In addition, there are statistically significant negative correlations, at the 0.05 level, between the spamming attacks and the following security controls: continuous auditing techniques (p-value = 0.014; r-value = -0.312); real time security awareness and incident response (p-value = 0.030; r-value = -0.281); signing of confidentiality agreement by employees (p-value = 0.033; r-value = - 0.271); mandatory vacations (p-value = 0.037; r-value = -0.270); intrusion prevention or detection (p-value = 0.048; r-value = -0.252); security alarm systems (p-value = 0.043; r-value = -0.260); and encryption of sensitive data (p-value = 0.018; r-value = -0.304). Despite these weak correlations, each company should consider these security controls as a means to minimising the effect of spamming attacks facing them.

The results in Table 4.111 show that there are statistically significant negative correlations, at the 0.01 level, between malware attacks, and each of the reorganised AIS security functions (p-value = 0.003), penetration testing (p-value = 0.002), and the protection of computers from natural disasters (p-value = 0.006), given that their r-values are -0.375, -0.386, and -0.341 respectively. This result suggests that malware attacks could be minimised if UK companies that responded had reorganised functions for their AIS security, and if they paid more attention to penetration testing.

From the results in Table 4.111, it can be seen that there is a significant negative correlation, at the 0.01 level, between employees' sharing of passwords, and penetration testing undertaken by companies, given that p-value is 0.008, and the r-value is -0.344. This result is further verified in the regression analysis results.

Table 4.111 also reveals that there is a statistically significant negative correlation, at the 0.05 level, between the theft of software, and software audit alert tools, given that p-value is 0.021, and r-value is -0.292. However, there is a significant positive correlation, at the 0.01 level, between the theft of software, and the insurance coverage for hardware and computer devices, with r-value of +0.470, and p-value of 0.000 ($p < 0.001$). Although this positive sign is unexpected, this could indicate that the more the companies suffer from software theft, the more concerned they are to have insurance coverage for their computer devices.

The results also reveal the existence of significant negative correlations between technical failures or errors, and each of the off-site storage of data back-ups, and malware detection tools, at the 0.05 level, and encryption of sensitive data, at the 0.01 level, given that their p-values are 0.027, 0.036, and 0.007, and r-values are -0.278, -0.265, and -0.340 respectively. Consequently, if companies consider these controls, they could minimise the effect of any software failure.

In addition, Table 4.111 reveals that there is a significant negative correlation, at the 0.05 level, between sabotage, and the existence of organised AIS security functions within companies, given that p-value is 0.050, and r-value is -0.255. Moreover, the results reveal the existence of significant negative correlations, at the 0.05 level, between the occurrence of natural disasters and the existence of organised AIS security functions (p-value = 0.047), and the existence of biometric techniques within companies (p-value = 0.026), given that r-values are -0.257 and -0.280 respectively.

On the other hand, the results in Table 4.112 provide no evidence of any statistically significant correlations between effectiveness level of AIS security in UK companies and each type of AIS security threat. This result indicates that, irrespective of the effectiveness level of their AIS security, companies still face different types of security threats. This result is further investigated in the regression analysis.

Table 4.112 Relationships between each type of AIS security threat and the effectiveness level of AIS security management using Spearman's rank correlation

AIS security threats	Correlation coefficient	Significance level (p-value)
Unauthorised access to data/systems by disgruntled employees	0.076	0.566
Unauthorised access to data/systems by hackers	0.059	0.659
Unintentional destruction of data by employees	0.027	0.844
Intentional destruction of data by employees	-0.079	0.557
Theft of physical information e.g. printed output, computer disks, etc.	0.032	0.815
Introduction of computer viruses, bombs or worms to the system	-0.147	0.263
Spamming attacks	0.202	0.128
Malware (spyware, adware) programs	0.098	0.456
Sharing of passwords	-0.147	0.277
Theft of software	-0.030	0.821
Technical software failures or errors	0.123	0.354
Sabotage or intentional destruction of computer equipment e.g. PCs and laptops	-0.033	0.801
Natural disasters e.g. fire, floods, earthquakes, etc.	0.244	0.060

In order to examine the effect of AIS security controls and the effectiveness level on the reduction of the different types of threats facing UK companies that responded, regression analysis was employed. The results in Table 4.113 show that off-site storage of original software has a significant effect on the unauthorised access to data or systems by disgruntled employees, with adjusted R^2 of 0.074, f-value of 5.724, and p-value of 0.020 i.e. if companies store their software off-site, they can restore normal business operations if disgruntled employees access their software or cause them any harm. However, the results indicate that only 7.4 percent of the variation in the above security threat can be explained by this control. It can be concluded that although the off-site storage of original software has a statistically significant coefficient, it accounts for only a small portion of the variation in the dependent variable i.e. unauthorised access to data or system by disgruntled employees.

Table 4.113 also reveals that insurance coverage for hardware and computer devices has a significant effect on the unauthorised access to data or systems by hackers, given that adjusted $R^2 = 0.053$, f-value = 4.250, and p-value = 0.044 i.e. if companies have insurance coverage for their computer devices, they can reduce the damage caused by hackers on these devices. However, the above control can explain only 5.3 percent of the variation of the dependent variable. Therefore, the results suggest that the insurance coverage for hardware and computer devices has a small effect on minimising the unauthorised access to data or system by hackers.

Table 4.113 The results of the multiple regression analysis

Dependent variable (AIS security threats)	Independent variables	Adjusted R^2	ANOVA		Beta	t-value	Significant level
			F-value	Significance level			
Unauthorised access to data/systems by disgruntled employees	Off-site storage of original software	0.074	5.724	0.020	0.300	2.393	0.020
Unauthorised access to data/systems by hackers	Insurance coverage for hardware/computer devices	0.053	4.250	0.044	-0.263	-2.061	0.044
Unintentional destruction of data by employees	Signing of confidentiality agreement by employees	0.055	4.246	0.044	0.268	2.061	0.044
Intentional destruction of data by employees	Penetration testing	0.061	6.861	0.000	0.365	3.546	0.001
	Intrusion prevention or detection software	0.143			-0.231	-2.091	0.042
	Security training and awareness programs	0.196			0.431	3.629	0.001
	Effectiveness level of AIS Security management	0.275			-0.417	-3.607	0.001
	Disaster recovery and business continuity plan	0.326			0.254	2.341	0.023
	Storing unused laptops in secure/locked cabinets	0.364			0.208	2.053	0.046
	Continuous auditing techniques	0.413			-0.408	-3.459	0.001
	Insurance coverage for hardware/computer devices	0.447			-0.264	-2.430	0.019
	Reorganised AIS security functions	0.481			0.218	2.038	0.047
Theft of physical information e.g. printed output, computer disks, etc.	Restricting access to sensitive information for authorised users	0.137	10.638	0.000	-0.410	-3.551	0.001
	Biometric techniques	0.256			0.361	3.132	0.003
Introduction of computer viruses, bombs or worms to the system	Mandatory vacations	0.065	5.559	0.002	0.330	2.760	0.008
	Segregation of duties	0.137			-0.351	-2.877	0.006
	Biometric techniques	0.190			0.261	2.173	0.034
Spamming attacks	Reorganised AIS security functions	0.132	10.743	0.000	0.373	3.264	0.002
	Penetration testing	0.255			0.366	3.201	0.002
Malware (spyware, adware) programs	Reorganised AIS security functions	0.157	11.838	0.000	0.409	3.669	0.001
	Penetration testing	0.269			0.350	3.141	0.003
Sharing of passwords	Penetration testing	0.082	5.972	0.018	0.313	2.444	0.018
Theft of software	Insurance coverage for hardware/computer devices	0.104	6.601	0.003	-0.349	-2.904	0.005
	Biometric techniques	0.162			0.268	2.227	0.030
Technical software failures or errors	Encryption of sensitive data	0.097	5.814	0.002	0.429	3.451	0.001
	Off-site storage of data back-ups	0.148			0.288	2.429	0.018
	Background investigation or reference checks	0.199			-0.269	-2.149	0.036

Sabotage or intentional destruction of computer equipment e.g. PCs and laptops	Restricting access to sensitive information for authorised users	0.081	5.857	0.001	-0.339	-2.974	0.004
	Intrusion prevention or detection software	0.135			-0424	-3.417	0.001
	Penetration testing	0.203			0.326	2.704	0.009
	Biometric techniques	0.248			0.243	2.079	0.042
Natural disasters e.g. fire, floods, earthquakes, etc.	Biometric techniques	0.098	5.965	0.000	0.327	2.734	0.008
	Intrusion prevention or detection software	0.153			-0.347	-0.826	0.007
	Effectiveness level of AIS Security management	0.205			0.310	2.445	0.018
	Insurance coverage for software	0.252			-0.243	-2.129	0.038

It can also be seen from Table 4.113 that there is a statistically significant effect of signing confidentiality agreements before joining the company, and the unintentional destruction of data by employees, given that adjusted $R^2 = 0.055$, f-value = 4.246, and p-value = 0.044 i.e. if employees sign confidentiality agreements before joining, they could be more cautious in dealing with sensitive data. Again, even though the independent variable. AIS security control has a statistically significant coefficient, it accounts for only a small portion of the variation of the above dependent variable.

The results in Table 4.113 also show that there are statistically significant effects of nine independent variables on the intentional destruction of data by employees. These variables include penetration testing, intrusion prevention or detection software, security training and awareness programs, disaster recovery and business continuity plans, storage of sensitive output in secured cabinets, continuous auditing techniques, insurances coverage for hardware and computer devices, reorganised AIS security functions, and the security effectiveness level. For example, if employees know the companies are not checking upon them through penetration testing, intrusion prevention or detection software, or continuous auditing techniques, they can intentionally make actions that can destruct companies' sensitive data. In addition, companies can reduce the effect of destructing sensitive data by employees if they have disaster recovery and business continuity plans to contain such incidents before affecting their reputation. This result suggests that these nine variables together can explain nearly 48.1 percent of the variation of the dependent variable, given that f-value = 6.861, and p-value = 0.000 ($p < 0.001$). It can be concluded that UK

companies that responded could minimise the occurrence of the intentional destruction of data by employees if they considered the above controls together.

It can also be seen from Table 4.113 that there are statistically significant effects of restricting access to sensitive information for authorised users, and the use of biometrics on the theft of companies' physical information i.e. if companies use biometrics and restrict access to sensitive data for authorised users, they can reduce the theft of their information. The result indicates that these two controls together can explain nearly 26 percent of the variation of the above security threat, given that adjusted $R^2 = 0.256$, f-value = 10.638, and p-value = 0.000 ($p < 0.001$). This result, therefore, suggest that if companies considered these two security controls together, they could minimise the occurrence of theft of companies' physical information.

The results in Table 4.113 also show that there are statistically significant effects of mandatory vacations, segregation of duties, and the use of biometrics on the introduction of computer viruses to a system. The result reveals that these three controls together can explain nearly 19 percent of the variation of the above security threat, given that f-value = 5.559 and p-value = 0.002. Despite the small value of the adjusted R^2, still there is an effect of these security controls together on minimising virus attacks facing companies.

In addition, statistically significant effects of the existence of reorganised security functions and penetration testing on spamming attacks can be seen in Table 4.113 i.e. if companies are monitoring their networks using penetration testing, they can discover the spamming attacks quickly before causing any downtime. These two controls together can explain nearly 26 percent of the variation of the spamming attacks, given that adjusted $R^2 = 0.255$, f-value = 10.743, and p-value = 0.000 ($p < 0.001$). The results also show that there are statistically significant effects by the same two controls on malware attacks, where adjusted R^2 is 0.269 i.e. if companies are monitoring their networks using penetration testing, they can discover the malware attacks quickly before causing any harm to their systems. This result indicates that the existence of reorganised security functions, and penetration testing can explain nearly 27 percent of the variation of the malware attacks, given that f-value = 11.838, and p-value = 0.000 ($p < 0.001$). It can be concluded that companies should consider using

the above two controls together in order to minimise the spamming and malware attacks facing them.

Penetration testing also has a statistically significant effect on the sharing of passwords by companies' employees, where adjusted $R^2 = 0.082$, f-value = 5.972, and p-value = 0.018 ($p < 0.05$) i.e. if employees know that companies are monitoring networks using penetration testing, they can avoid sharing their passwords, and consequently, the security incidents related to this threat can be reduced. Despite the small value of adjusted R^2, still there is evidence from the results of the effect of penetration testing on the reduction of this threat.

Regarding the theft of software, the results show that there are statistically significant effects of each of the existence of insurance coverage for hardware and computer devices, and biometrics on reducing the occurrence of this security threat, given that adjusted $R^2 = 0.162$, f-value = 6.601, and p-value = 0.003 i.e. if companies use biometric techniques on the computer rooms, they can reduce the theft of their software. Although the results show that these two controls together can explain only 16 percent of the variation of the dependent variable i.e. theft of software, the results still provide evidence of the importance of biometrics. However, few companies have implemented them.

It can also be seen from Table 4.113 that there are statistically significant effects of sensitive data encryption, off-site storage of data back-ups, and employees' background checks on minimising the effects of technical software failures within companies, given that adjusted $R^2 = 0.199$, f-value = 5.814, and p-value = 0.002. For example, if companies encrypt their sensitive data, and if technical software failures or errors occur, and these data fall in the wrong hands, encryption can limit the damage of losing these sensitive data. The results, therefore, suggest that these three security controls together can explain nearly 20 percent of the variation of this threat.

Regarding the intentional destruction of computing equipment, it can be seen from Table 4.113 that there are statistically significant effects of restricting the access to sensitive information for authorised users, intrusion prevention or detection software, penetration testing, and biometrics on the above security threat, given that adjusted R^2

= 0.248, f-value = 5.857, and p-value = 0.001. For example, if companies use biometric techniques and restrict access to computer rooms, they can prevent intentional destruction of computing equipment. It can be concluded that these four controls together can explain nearly 25 percent of the variation of the intentional destruction of companies' computing equipment. Consequently, companies must consider using these controls together in an attempt to minimise the effect of the above security threat.

Moreover, the results show that there are statistically significant effects of the existence of biometrics, intrusion prevention or detection software, insurance coverage for software, and the effectiveness level of AIS security on minimising the effect of natural disasters within companies, given that adjusted $R^2 = 0.252$, f-value = 5.965, and p-value = 0.000 ($p < 0.001$). These results indicate that companies can reduce the effects of natural disasters if the above controls are considered together, and if the effectiveness level of security management is high.

Overall, the above results indicate the relative importance of some types of AIS security controls, compared to the others, given that these controls have a significant effect on many types of security threats. On the other hand, the regression analysis results did not reveal the effect of some security controls on any type of AIS security threat. For example, the results show that penetration testing has a significant effect on the intentional destruction of data by employees, spamming and malware attacks, sharing of passwords, and the intentional destruction of computing equipment. In addition, although only 14.5 percent of companies reported the use of biometrics (Table 4.102), the regression analysis shows that these techniques have an effect on many security threats such as theft of physical information and software, virus attacks, sabotage, and natural disasters. Consequently, companies should consider biometric techniques, and must try to gradually implement these tools.

On the other hand, the results of the regression analysis provide no evidence of any effect of some AIS security controls on any type of security threats such as software audit alert tools, back-up of hard disks, security alarm systems, users' access controls, network encryption, and spam filtering software.

From the above results, it can be concluded that some types of security controls have a significant effect on the reduction of AIS security threats facing UK companies that responded. In addition, AIS security effectiveness level impacts significantly on two types of security threats namely intentional destruction of data by employees and natural disasters. However, Spearman's test provides no evidence of any significant correlation between the effectiveness level of AIS security and the different types of security threats. These results suggest that despite the high level of security effectiveness achieved by companies, they are still faced with an increasing number of threats, and as long as there are more technological advancements, more threats will arise. Consequently, companies need to be ready to face these increasing numbers and types of security threat.

4.8 Summary of the chapter

This chapter began by presenting the sample size and response rate of the current study. It proceeded with a general discussion on the statistical methods employed to analyse data of the questionnaire and the reasons for selecting each method. The chapter then presented the main findings of the questionnaire. The profile of those who participated in the study and of their companies was discussed.

The chapter then examined the main findings regarding the elements of AIS security management framework within companies. The results indicated the existence of AIS security policy in the majority of UK companies that responded regardless of the industry sector. In addition, some sectors are taking steps to provide their employees with security training and to raise their security awareness for example the insurance & financial services, whereas other sectors such as the manufacturing sector do not pay enough attention to security training and awareness.

The results also showed that most companies do undertake a security risk assessment; however, there are no association between the different industry sectors that responded and the existence and frequency of undertaking this risk assessment.

According to the interviews' findings (Chapter 5), many companies under-reported the exact number of security incidents, and the majority of companies claimed that

they did not experience any incidents in the last year. The results also showed that there are no association between the different industry sectors that responded and the existence of security incident handling procedures, disaster recovery and business continuity plans, and the frequency of testing and reviewing these plans. The results indicated that companies have become more concerned with having formal procedures to respond quickly to the different security incidents, and having a formal up-to-date business continuity plan.

However, the results revealed that the majority of UK companies that responded do not have a separate budget for security. This could be because security is still perceived as an IT issue, and therefore, its budget is a part of the IT budget. In addition, the results indicated that software security controls was ranked first in the top three areas of spending on AIS security, followed by hardware and physical security controls, and audit activities, compliance and certification. However, the results indicated that there are no significant differences among the different sectors regarding the top areas of security spending except for hardware and physical security controls, which indicated that some sectors spend more on these controls than the others.

The results also revealed that the awareness level of the British Standard BS 7799 is high in some sectors such as the insurance & financial services, energy & utilities, and media & entertainment sectors, whereas it is weak in the technology & telecommunications sector, and very weak in the manufacturing, retail merchandising, and property & construction sectors. However, the results revealed that no statistically significant differences exist among different industry sectors concerning the awareness level of this standard among managers and employees of UK companies. Moreover, the majority of companies that responded are not certified under ISO 27001 and are not planning to be certified.

In addition, the results revealed that the most common technique used to evaluate AIS security effectiveness was the internal audit of security procedures, whereas vulnerability scanners were the least common technique used. Moreover, the results showed that the most common success indicator of security management was the successful defence against AIS security attacks, followed by information security

assurance. It is encouraging that the majority of companies that responded believed that their security management is somewhat or extremely effective.

The chapter then presented the most common sources and types of security threats facing UK companies. The results revealed that companies' employees are now the most common source of security threats, given that authorised users or employees were ranked the first common source of security threats. The results indicated the infrequent occurrence of some types of security threats such as intentional destruction of data by employees, theft of physical information and software, sabotage, and natural disasters. On the other hand, the results revealed the frequent occurrence of employees' errors i.e. unintentional destruction of data by employees, spamming and malware attacks, and sharing of passwords.

The final section of this chapter presented the results concerning the different types of AIS security controls used within UK companies. The results indicated that the majority of companies that responded are paying, relatively, more attention to software, hardware, input, output, and network security controls, than the other controls. Consequently, they must put more effort into the organisational and personnel security controls to protect their systems from different security threats.

The results of the regression analysis revealed the relative importance of some AIS security controls compared to the other controls given their significant effects on many types of threats such as penetration testing and biometrics. On the other hand, the results provided no evidence that some controls had any effect on any type of security threats such as software audit alert tools, security alarm systems, users access controls, network encryption, and spam filtering software despite their importance.

The results of this chapter raise further security issues, which were discussed in the interviews. The following chapter presents a full discussion of the results of the interviews and the methods used in data analysis.

Chapter 5
Analysis of interview results

5.1 Introduction

Chapter 4 discussed the main findings derived from the questionnaire. In order to understand and confirm the results obtained from the questionnaire analysis, to explore some issues in more depth, to enrich the quality of the information collected, and to fill in any gaps in data that might occur in the questionnaire results, some semi-structured interviews were conducted for the current study.

This chapter provides a full discussion of the interview findings. It presents the sample size, and the data analysis methods of the interviews. It also provides the opinions of the interviewees on the AIS security within their companies.

This chapter comprises 14 sections. Section 5.2 presents the sample size of the interviews. Section 5.3 explains the methods used in analysing the interviews. The interviewees' and their companies' background information are provided in Section 5.4. Sections 5.5 - 5.13 present the main findings of each of the nine interviews conducted. Each section is divided into four sub-sections. The interviewees' opinions on the management framework of AIS security within their companies are discussed in the first sub-section which addresses AIS security policy, training and awareness programs, risk assessment, incident response, disaster recovery and business continuity plans, security budget, security standards and certification, and AIS security effectiveness. The second sub-section investigates the most common sources and types of AIS security threats, and the third sub-section explores the most recent security controls employed within their companies to reduce security threats, and the security controls they are planning to use in the future. Section 5.14 concludes the chapter with a summary of the main findings of the interviews.

5.2 Selection of interviewees

As mentioned in Chapter 3 (Section 3.6.2.1), at the end of the questionnaire, the respondents were asked to provide their contact details if they were willing to

participate in a follow-up face-to-face interview to discuss some security matters in more depth.

In total, 12 managers agreed to participate and provided their contact details in the returned questionnaire. An e-mail was then sent to these managers thanking them for completing the questionnaire and for their willingness to be interviewed, and for giving their permission to be contacted again to arrange an appointment after analysing the questionnaire data. One month later, another e-mail was sent to the managers reminding them of the study and arranging an appointment for the interview. Nine managers responded and appointments were arranged to conduct the interviews. In total, nine interviews were conducted with managers of nine UK listed companies in different industry sectors. The sample size seems small, but it is not surprising that only nine respondents were willing to participate in the study. According to Kotulic and Clark (2004), security investigation research is the most intrusive type of research, and there is undoubtedly a general mistrust of any outsider attempting to gain data about the actions of the security practitioner community.

Moreover, Corbetta (2003, p.284) has argued that the qualitative interview plays a supporting role for quantitative data collection. The main empirical base is made up of the questionnaire, and the qualitative phase only serves to pave the way for the quantitative procedure, to add illustrative support to its findings, or to clarify some aspects that the quantitative data have not brought to light. In addition, since the interview was the second stage of the data collection, and its aim was to confirm the results obtained from the questionnaire, the researcher considers that the opinions provided by the nine managers are, to a great extent, sufficient to confirm the general patterns appearing in the questionnaire results. Bryman and Bell (2007) argued that interviewing managers often raises specific issues since the status and power held, particularly at a senior level, means that gaining access to this group of people and arranging a mutually convenient time to conduct an interview can be extremely difficult.

The interviews were conducted between February and April 2008. Interviews lasted between one and three hours. The date, time, location and duration of the interviews are shown in Table 5.1.

Table 5.1 The interviews dates and locations

Interview number	Interviewee code	Date	Time	Location	Duration
1	A	11/02/2008	10:00 am	Cardiff	2 hours
2	B	14/02/2008	11:00 am	London	2 hours
3	C	14/02/2008	2:30 pm	London	1.5 hours
4	D	26/02/2008	3:30 pm	London	1.5 hours
5	E	04/03/2008	2:00 pm	Huntingdon	3 hours
6	F	17/03/2008	1:30 pm	London	2 hours
7	G	19/03/2008	4:00 pm	Maidenhead	1 hour
8	H	07/04/2008	3:00 pm	Bradford	2 hours
9	I	22/04/2008	11:00 am	Reading	2 hours

All the interviews were audio-recorded after obtaining the permission of the interviewees. The audio recording was very important. It allowed the researcher to concentrate on the conversation, to maintain a more natural relationship with the interviewees, and to capture their actual quotations. The audio recording also permitted more thorough and repeated examinations of what the interviewees said (Bryman and Bell 2007; Corbetta 2003; Patton 1990). However, the audio recording did not eliminate the need for taking notes. Patton (1990) indicated that taking notes becomes a kind of non-verbal feedback to the interviewee when something is sufficiently important to be written down. On the other hand, the failure to take notes will often indicate that nothing of particular importance is being said. Consequently, the researcher took some notes in addition to audio-recording the interviews.

As mentioned in Chapter 3 (Section 3.6.2.2), the interview guide used in the interviews was based on a number of themes, including the background of interviewees and their companies, the management framework of AIS security, AIS security threats and controls. A copy of the interview guide used during the interviews is presented in Appendix 2.

5.3 Interview data analysis

After conducting and audio recording the interviews, the researcher transcribed the interviews in full. Patton (1990) argued that since the raw data of interviews are quotations, full transcriptions are the most desirable data to obtain. The researcher listened to the recorded interviews several times in order to check the accuracy of the transcriptions. However, transcribing the interviews was a very time consuming process. It took the researcher about six hours to transcribe one hour of speech.

Once the interviews had been transcribed, they were ready for analysis. However, there is no agreement in the literature as to how qualitative analysis should proceed, or what makes an acceptable analysis. Patton (1990) argued that there are no simple formulae or clear-cut rules about how to do a credible, high quality analysis. The challenge is to do one's best to make sense of a massive amount of data, in order to fairly represent and communicate what the data reveal given the purpose of the study. Punch (1998) also stated that there is no single methodological framework for qualitative data analysis. In addition, Bryman and Bell (2007) indicated that unlike a quantitative data analysis, there are few well established and widely accepted rules for the analysis of qualitative data.

On the other hand, there is an agreement in the literature that the ways in which qualitative data are analysed have to be clear to the reader of the research. Patton (1990) argued that the qualitative researcher has an obligation to be methodical in reporting sufficient details of data collection and the processes of analysis to permit others to judge the quality of the findings. In addition, Punch (1998) stated that the methods for data analysis needed to be systematic, disciplined, and be capable of being seen and described. If the method of analysis cannot be described and scrutinised, it is difficult to have confidence in the findings put forward.

As mentioned in Chapter 3 (Section 3.6.2.3), Miles and Huberman's approach to qualitative data analysis has been utilised in the current study. Miles and Huberman (1994) suggest the following main components for qualitative data analysis: data reduction, data display, and drawing and verifying conclusions.

Data reduction is the process of selecting, focusing, simplifying, abstracting, and transforming the data that appear in transcriptions (Miles and Huberman 1994). Punch (1998) indicated that data reduction occurs continually throughout the analysis. In the early stages, this happens through editing, segmenting, and summarising the data. In the middle stages, it happens through coding, and finding themes and patterns and in the last stages, through conceptualising and explaining. The objective here is to reduce the data without significant loss of information.

Data display is an organised, compressed assembly of information that permits conclusion drawing. Miles and Huberman (1994) argued that better displays are a major avenue to valid qualitative data analysis. They indicated that there are many different ways of displaying data such as matrices, graphs, charts, and networks. Sarantakos (2005) also stated that these different ways present visual information that allows the researcher to make sense of the collected information and to draw relevant conclusions.

Conclusions follow the data reduction and display. Conclusions will be in the form of propositions, and once they have been drawn, they need to be verified.

Despite the small number of interviews conducted, and the lack of broad agreement about the use of computers in qualitative data analysis, the researcher used NVivo, which is one of the best known computer-assisted qualitative data analysis software. There are many benefits to be gained from using software like NVivo. Flick (2002) indicated that qualitative data analysis software is a pragmatic tool to support qualitative research. Bazeley (2007) also stated that using a computer in analysing qualitative data simply ensures that the researcher is working more methodically, more thoroughly, and more attentively. In addition, Kelle *et al.* (1995) argued that the use of computers would make qualitative analysis more systematic and transparent, thus enhancing its trustworthiness.

The use of software like NVivo will make the process more robust, easier to control, and more enjoyable (Gibbs 2002). NVivo removes most of the clerical tasks associated with the manual coding and retrieval of data (Bryman and Bell 2007). It allows the researcher to keep interviews, codes, memos, diagrams, and audio recordings in one place, which can be a powerful support to the analysis process (Weitzman 2003). The qualitative data analysis software allows the researcher to look at data in different ways, and therefore, it increases creativity in dealing with data (Fielding and Lee 1998). In addition, one of the main advantages of the software is its data management capabilities.

Despite the above advantages, there are many concerns about using the software in qualitative data analysis. There is wide agreement in the literature that the use of

computers in analysing qualitative data can distance the researcher from the data. Gibbs (2002) argued that researchers using paper-based analysis felt they were closer to the words of their respondents than if they used computers. Fielding and Lee (1998) indicated that computer methods discourage involvement and engagement with data. However, Lewins and Silver (2007) state that software increases the access researchers have to the whole data files. They stated that whatever tools are used, "live" contact to data is always easy, increasing the researchers' closeness to data.

There is another fear that the attention attracted by the computer and software will distract the researcher from the real analytic work (Flick 2002). In addition, computers would affect creativity and reduce variety as coding and retrieval became the dominant process in working with data, which may lead to the neglect of extensive memoing, linking of ideas, holistic viewing of the text and visualising techniques. In fact, it is the opposite - using computers can improve the consistency of analysis of a block of data.

Gibbs (2002, p.65) stated, "Even with a computer program to help, there is no substitute, in the end, for close reading of and a thorough familiarity with the text". The researcher, then, began the first stage of data analysis - data reduction - by reading the interview transcripts several times attempting to find, refine, and elaborate the important concepts and themes that will help in coding the interviews. The codes developed were based mainly on the questions asked in the interviews, which were found in the interview guide, in addition to other codes that were developed after reading the transcripts. Gibbs (2002) argued that there is often much to be gained from approaching the data with an open mind, with no preconceptions about what analytic framework might be appropriate. In this case, codes were developed through the close reading of the transcripts. On the other hand, the concepts that the codes represent may come from the literature and previous studies. Gibbs (2002) indicated that most researchers move between both approaches during their analysis, and suggested that researchers do not have to become too tied to the initial codes they construct.

The researcher then imported the transcripts from Microsoft Word, after converting them to rich text format (RTF), to NVivo 2 software[3]. The researcher then entered the developed codes into NVivo, as a first step in coding the interviews' transcripts. Coding is the process of establishing a connection between a code - known in NVivo as node - and one or more passages of text. Coding brings together passages of text that are about the same issue or indicate similar ideas, concepts, actions, and descriptions (Gibbs 2002).

Once the codes were entered into NVivo, the researcher went through the interview transcripts and coded them one by one. The researcher checked the codes and the coded passages several times to ensure their accuracy, given that coding is the basis of the subsequent analysis.

Once the transcripts were coded, NVivo allowed the researcher to sort the data by grouping all data units with the same code into a single computer file. Bryman and Bell (2007) indicated that NVivo allows the researchers very rapidly to travel through all documents so that they will end up with all text that was coded at a particular code in all of their documents. NVivo helped the researcher in retrieving what all the interviewees had said about the identified concepts, themes, and events. The researcher printed these files and went through them several times. A few codes were removed since they occurred infrequently. The researcher then explored the data searching for similarities, differences, patterns and relationships between different interviews on the same concept, theme or event.

Miles and Huberman (1994, p.91) stated that the second stage of qualitative data analysis is data display. They indicated that data display is a visual format that presents information systematically, so that the researcher can draw valid conclusions. Sarantakos (2005) also stated that tables and graphs are useful tools of presentation in qualitative research, but the structure of the presentation does not seem to adhere to any strict rules, given that tables and graphs in qualitative research are always tailored to serve the needs of each particular study. Consequently, the researcher constructed a number of tables representing different codes in order to summarise the most

[3] There is a new version now of NVivo software - NVivo 8, which can import documents in both rich text format and word formats.

important text and quotations of different interviewees that would help in drawing conclusions and answering the research questions.

Given the small number of interviews conducted and the long time that would be taken for the researcher to learn the complex functions of the NVivo software, all the tables were constructed manually. Bazeley (2007, p.2) recommended that those using NVivo for a small project or for small number of interviews can work without having to learn the complex procedures.

The final stage of qualitative data analysis is the drawing and verification of conclusions. The aim of this stage is to integrate what has been done into a meaningful and coherent picture of the data. Miles and Huberman (1994) suggested some methods for drawing conclusions from interview data such as noting patterns, making contrasts, comparisons, clustering and counting. Consequently, in order to draw conclusions and to support the questionnaire results presented in the previous chapter, the researcher counted, compared, and contrasted the responses of all interviewees associated with each code. The following sections presenting the main findings of each interview based on the same sequence of the sections of the interview guide as shown in Appendix 2.

5.4 General and background information

After an introductory discussion with the interviewees, introducing the researcher, thanking the interviewees for their participation in the study, and explaining the aims and importance of the current study, Section 2 of the interview guide (Appendix 2) sought information concerning the interviewees and their companies' background.

Interviewees were asked seven questions regarding their company name, industry sector, number of employees in the company, their current position and years of experience in this position, and their professional security qualification, if applicable. The interviewees were also asked about the existence of a separate department for security within their companies, number of employees in this department, and to whom they report. These questions provided the researcher with a profile of those who participated in the study, and they were useful in the subsequent analysis of the

interview data. Table 5.2 demonstrates the general and background information of the interviewees and their companies.

Table 5.2 General and background information of the interviewees and their companies

Interviewee code	Industry sector	Number of employees	Gender	Position of interviewee	Years of experience in current position	Professional security qualification
A	Insurance & financial services	2300	Male	Information security manager	3	Yes
B	Media & entertainment	4000	Male	Technology risk manager	7	No
C	Property & construction	12000	Male	Group IT director	11	No
D	Property & construction	24	Male	Group accountant (looking after IT)	15	No
E	Energy & utilities	3500	Female	Security risk manager	6-7	Yes
F	Insurance & financial services	3000	Male	Information security manager	10	Yes
G	Media & entertainment	6500	Male	Chief technology officer	1	No
H	Energy & utilities	2200	Male	IT architecture manager	6	No
I	Technology & telecommunications	20000	Male	Information risk & security manager	5	Yes

Industry sector

Table 5.2 showed that the interviewees who participated in the study were from five industry sectors. From the table, it can be seen that one out of the nine interviewees was from the technology & telecommunications sector, whereas two interviewees from each of the insurance & financial services, media & entertainment, property & construction, and energy & utilities sectors participated in the study. It may not be surprising that no respondent from the manufacturing sector was willing to conduct a follow-up interview, given that the questionnaire findings (Chapter 4) showed that manufacturing companies do not devote much effort or resources to information security and consequently they are not concerned too much about discussing the different security aspects.

Number of employees

Table 5.2 demonstrated that six out of nine interviewees stated that their companies have more than 2000 employees, whereas two companies have more than 10000

employees. Kankanhalli *et al.* (2003) argued that larger companies spend more time and money on security than smaller companies do, and therefore, such companies have an interest in taking part in the study. On the other hand, one interviewee from the property & construction sector stated that his company has only 24 employees, however the turnover of his company is high. Interviewee D commented:

> *"There are only 24 employees working here, but our turnover is more than £300 million. We are a property company and we are dealing with high value and large buildings, so turnover is quite big".*

Position of interviewee

Interviewees were then asked about their current position in the company. Table 5.2 showed that the position of five out of nine interviewees (55.5 percent) related to the IT function in the company, their positions are technology risk manager, group IT director, chief technology officer, IT architecture manager, and group accountant looking after IT. This is consistent with the Security and Information Risk Survey (NCC 2007) which indicated that in almost two thirds of companies, the person responsible for information security is someone who sits within the IT function. It can also be seen from Table 5.2 that two interviewees are information security managers, another interviewee is a security risk manager, and the other is an information risk and security manager. Von Solms (2005) argued that the position of the information security manager has been an established position in most UK companies. The Global Security Survey (DTT 2007) also indicated that the role of the information security leader is rising through the ranks to the company's upper levels. This trend will continue in response to the changing nature of threats and growing customer and employee demands.

Years of experience in the current position

Table 5.2 revealed that the majority of employees had more than five years of experience in the current position, whereas, only two interviewees had less than five years of experience; however, they had more years of experience in the same position or in equivalent positions in other companies. All the interviewees, therefore, had sufficient experience and knowledge of all security practices within their companies, which were reflected in the quality of information provided to the researcher that helped in enriching the research.

Professional security qualification

It can be seen from Table 5.2 that four out of nine interviewees had professional security qualification. These four interviewees were from insurance & financial services, energy & utilities, and technology & telecommunications sectors. The BERR Information Security Breaches Survey (BERR 2008) stated that security qualifications are commonest in the technology sector. In addition, given that the insurance & financial services, and the energy & utilities sectors are dealing with millions of customer data, they tend to have a better understanding of security and, therefore, they employ security qualified staff. The results showed that all the interviewees who had professional security qualifications were Certified Information Systems Security Professionals (CISSP). In addition, one of the interviewees was a Certified Information Security Manager (CISM) and was studying to be a Certified Information Systems Auditor (CISA), whereas other interviewees had the Information Systems Security Professionals qualification (ISSP), and the qualification obtained from the British Computer Society (BCS).

Security department

Hitchings (1995) argued that companies with a security department take the problem of security seriously and, at the very least, can take the first step in making a company more secure. Dutta and McCrohan (2002) also indicated that if there is no structural unit that is specifically responsible for security, the implementation of security initiatives will be fragmented and may therefore be ineffective. Consequently, interviewees were asked whether they have a separate department for security within their companies, the number of employees in this department, and to whom this department reports.

The results in Table 5.3 showed that only two interviewees (G and H) believed that they had a security department, whereas four interviewees (A, E, F and I) stated that they had a small security team of three to five persons. Table 5.3 also showed that three interviewees (A, E and I) believed that the security team were included in the IT department within their companies and reported directly to the IT director, whereas interviewee F had the information security team within the group risk management department and this team reports to the head of risk management.

Table 5.3 The existence of a separate security department within the interviewees' companies

Interviewee code	Industry sector	Existence of security department	Number of employees	Reporting
A	Insurance & financial services	A security team within IT department	3	Head of IT
B	Media & entertainment	A solutions management department within IT for the technical part of security	-	-
C	Property & construction	IT team & a security risk management team	4 in each team	Chief executive
D	Property & construction	No security department or team	-	-
E	Energy & utilities	A security team within IT department	-	IT director
F	Insurance & financial services	An information security team within the group risk management department	3	Head of risk management
G	Media & entertainment	A security department, not specific for information security	30	Head of security
H	Energy & utilities	A security department	4	Operations department
I	Technology & telecommunications	An information security team within the IT department	5	CIO

One of the interviewees (D) stated that there was no security department or team within his company. However, this was not surprising given that his company had only 24 employees. The interviewee commented:

> *"We do not have a separate department for security or even an IT department, but we use an IT consultant who comes in two or three times a week or as required. One of the aspects of security is to delegate the authority to a number of people, but we cannot do that, we are very few people; we cannot break down the responsibility. This is a drawback, but we still have the controls in place".*

Table 5.3 also showed that interviewee B believed that his company did not have specific information security department, but there was a solutions management department within the IT department, particularly for the technical part of security. Another interviewee (C) stated that there were two departments in his company, one for the security of IT and for anything to do with computing i.e. technical issues, and the other was the risk management department. He also stated that this department took a much broader view of security, particularly in undertaking security risk assessment for anything that might have an impact on the company, not just the technology risks.

The above results, therefore, indicate that security is still recognised as an IT issue by the majority of companies and consequently security management is often left to the

IT department. Interviewee F provided a reason for the non-existence of a separate security department within many companies. He commented:

> *"There is no separate security department because it might cause overlap. What we do is similar to some other departments. The people in the company do many security practices as a part of their jobs e.g. fraud team, financial risk team, etc. There is too much overlap".*

However, Dodds and Hague (2004) argued that, regardless of the existence or non-existence of a separate security department, the most important issue is that each department understands their security roles and responsibilities, and perform their jobs as dictated by the policies.

The subsequent analysis of the interview findings is presented in the following sections (5.5 - 5.13) based on the same sequence of the sections and questions of the interview guide (Appendix 2).

5.5 Interview 1

5.5.1 General information

The first interview was conducted in an insurance company located in Cardiff. The company was established more than 10 years ago. The company was registered in the London Stock Exchange and there were around 2300 employees in it. The company had a small security team of three persons, which was included in the IT department and reported directly to the head of IT. On the other hand, interviewee A was an information security manager, who had three years of experience in his current position. The interviewee had two professional security qualifications - Certified Information Systems Security Professionals (CISSP), Certified Information Security Manager (CISM), and he was studying to be a Certified Information Systems Auditor (CISA).

5.5.2 The management framework of AIS security

Business environments today have become increasingly more severe, complex, and interdependent at the domestic and global level (Whitten 2008). Organisations have become more dependent upon their IS than ever before. Consequently, with this increasing usage of IS, with the amount of information stored on them, and with all the increased media attention about security related incidents and the effects that

might have (Mouratidis *et al.* 2008), it is necessary for companies to go beyond technical considerations and to adopt structured process for maintaining their AIS security. Consequently, Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding the management framework of AIS security within his company.

AIS security policy: As mentioned in Chapter 4 (Section 4.5.1), there is wide agreement in the literature that the security policy is the start of security management in a company. Eveloff (2005) argued that a security policy is at the heart of any security strategy, representing the objectives from which all security procedures are derived. Interviewee A confirmed that they had a formal security policy, which was written by the security manager in 2002, and was updated annually. According to Briney (2000), a security policy should be evaluated and updated on a regular basis to reflect changing business, regulatory, technological and personnel environments.

The policy was distributed via the company's intranet. They could not distribute hardcopies to a large number of employees. Interviewee A commented:

> *"We don't have a hardcopy to distribute among all those employees. On our intranet, we can make people aware of security. We have an electronic copy of the policy. We also have our information security team pages. On our intranet, there is all relevant information about security, not just the policy".*

He believed that it is not sufficient to write a policy, it is most important to educate people about what they should and should not do. Consequently, staff training and awareness were the most important elements of the security policy. He expressed the following opinion:

> *"Training and awareness is the most important part. With information security, it is not enough to write a policy. What we have to do is to train people. We have to let them know what is the acceptable behaviour and what is the unacceptable behaviour, only then, we can discipline people because of security responsibilities. It is a part of my responsibility as a security manager to get people and all the company security aware".*

Von Solms and Von Solms (2004) argued that there is no use in having a perfect security policy if it is not possible to monitor and enforce compliance to such policies. Interviewee A claimed that his company was checking compliance to the security

policy through the security tests undertaken by the employees every year. Moreover, he believed that the security policy is effective given that his company did not experience major security incidents in the last year, and all the people passed the test. He stated:

> *"There are many ways to see how well the policy is working. If there were a number of security incidents, this would indicate that there is a problem. We have very few minor incidents. However, it is not a matter of how big or small the incident is, it is still has to be reported, handled, managed, and communicated, and that is what we are doing. If many people fail the security test, this might indicate that either they do not listen or the training material is rubbish. However, if we get no incidents or few incidents, and all people are passing the test, there is no problem with the policy".*

Security training and awareness program: As mentioned in Chapter 4 (Section 4.5.2), employee training and awareness is the most important of all security measures (Eveloff 2005). Interviewee A stated that his company had a formal security training and awareness program. However, he believed that it is not practical to have an annual classroom training for all current employees due to time and cost constraints, and consequently, they depend on computer-based training. He expressed the following opinion:

> *"Every new employee must have a classroom security training, however, every year after that, it is not practical to have 2300 employees in a classroom. We are using the intranet. We have a Learning Management System managed by our HR department, an online course. We put together an online information security-training package for all employees, it is compulsory, and they have to do an exam every year. It is an internet-based learning system for employees".*

In addition, he highlighted the importance of the training and awareness program in the following quotation:

> *"We are planning to have a formal training and awareness program for all employees. Everyone will be given training. User awareness is very important in information security. If we cannot make people aware, then we are going to have incidents. We may have all technical controls in place, but still we have to enable people to work. No matter how many regulations we have, we still have to enable them to do their jobs perfectly. We can have regulations, but people still may do something that contravenes regulations and they are not aware. The most important is the training and awareness of employees".*

Moreover, interviewee A believed that the security awareness level in his company is very good or quite high; however, it could always be done much better. He stated:

"Security awareness level is very good, but always it should be better, since 70 percent of our problems are from people, human beings".

Risk assessment: Businesses are exposed to unlimited security risks unless they have a formal risk management framework to enable risks to be identified, evaluated, and managed (Shaw and Daniels 2002). Interviewee A believed that his company was undertaking security risk assessment for the whole company and not just for AIS security. He stated:

"We have a very well developed risk management process for the company as a whole"

Freeman (2007) argued that a regular comprehensive risk assessment should always be the guiding light for achieving organisational security goals. Interviewee A stated that his company undertakes risk assessment on a quarterly basis; however, he believed that it must be undertaken on a continuous basis and with the use of any new technology. He commented:

"Risk assessment is undertaken every 3 months, however, it is an ongoing process. I think we will have many changes in technology. So, if any new technology gets through, if there are new processes, there must be a risk assessment".

This result is not surprising, given that insurance & financial services companies are regulated by the FSA, so they have to report their security risks regularly.

Moreover, risk assessment is the responsibility of the risk management team within the company. Interviewee A commented:

"The risk management team is responsible for undertaking the risk assessment with the internal audit team. They work in the compliance department, outside the IT".

He indicated that although the risk level in his company is quite low, there is no absolute security or zero risk. He stated:

"We are quite a low risk organisation, but the security problem is relating to someone who does not follow the procedures, or we haven't checked whether they follow the procedures, then there is a potential risk. There is no absolute security. There is no zero risk".

Incident handling, disaster recovery and business continuity plan: Kieke (2006) has pointed out that the number of security breaches continues to rise. Interviewee A

believed that his company had had only two minor security incidents in the last two years, which they contained before any damage was caused. He commented:

> *"Yes, we had 2 minor security incidents. I found a couple of years ago, a USB on the back of one of our training Pcs, somebody forgot it, and they are not allowed to use USBs. I found the USB and the information on it, and I knew whose USB it was. It was an external company, who came in and tried to demonstrate the controls, but they were unable to get any information from our network. There was no damage from this incident, but it is a security incident that must be reported".*

He believed that it could be catastrophic if his company lost customer information, given that this incident could affect their reputation, customer confidence, etc. He stated:

> *"There are 2 situations which can be catastrophic; if we were to have a major data protection violation or to lose customer information. Customer information is our most sensitive asset, such as names, addresses, bank details, financial information, etc. We are a public company; it will be catastrophic if we lose customer information. It will cause reputation damage, and the share price and customer confidence will be affected. We have numerous controls in place to prevent this from happening. Another situation is of a non-compliance issue".*

Regarding the security incident handling procedures in his company, interviewee A indicated that there is an incident management team to respond to any incident. He pointed out:

> *"We have an incident management team, if there is a problem, this team would be able to respond to it. The right people can deal with any situation and they can make sure that they are doing the right things. They make different scenarios and see what will happen. These procedures are reviewed annually, at least once a year or as required. I have to verify them and get management to sign and republish them. However, they depend very much on the size and type of the problem".*

Moreover, he stated that they have different authorities and regulatory bodies to whom they could report security incidents depending on the size and nature of incidents including the FSA (Financial Services Authority) and the ICO (Information Commissioner's Office). He commented:

> *"It depends on its relevance. Internal incident like a USB incident is not a problem, but if there is an incident related to data protection, we will have to report it to the ICO. According to law, we have to report. If it is supposed to be a violation of FSA regulations, we have to report it to the FSA. If it is relevant to the payment card industry scheme, we*

have to report it to the Payment Card Industry Scheme. Part of our procedures is the communication. If we have a security breach and we did not report it to the external authorities, they can fine us, but if we speak to them straight away, they can try to work with us and help us. For example, if I am in the situation of the Nationwide Society[4] and I lose a laptop with a quarter a million of customer records, and this only got reported a month later, that is why they were fined about million of pounds. What they have to do is to demonstrate that they have encrypted their laptop. They did wrong, if they went straightaway and reported that they lost a laptop with customer information, the authorities could have helped them. It will be more damaging for companies not to report".

He also believed that after a security incident, they could improve their procedures, change their policy, if necessary, check the controls, and learn from the incident. He commented:

"As a part of the security incident handling process, we have to manage, handle, and communicate the situation. We have a reporting process. We can learn lessons from the incident. We can change our procedure and policy, if necessary. After managing an incident, we would then check our controls, maybe there is a control failure, or a human issue. But in case of an incident, we always have the opportunity to improve our procedures and to learn from that event, a continuous learning process".

Nosworthy (2000) argued that a business continuity plan involves not only the IT department, but also other areas of the business and should be incorporated into the overall business process and not just focus on IT. Interviewee A confirmed this opinion and stated:

"Yes, we have a business continuity plan, not just for the IT, but for the business as well. Each team within the company has a business continuity plan. We have a business continuity forum, we meet every 3 months to discuss different issues and to do scenario testing, but not only for IT, it is for business and IT together".

He also stated that they are constantly testing and updating their business continuity plan, particularly when any technology changes, and that the disaster recovery staff is responsible for this plan. He presented the following opinion:

"Constantly, we are testing and updating the plan. As an IT department, we do periodic tests once every quarter. We simulate a system failure, we have a disaster recovery test, and

[4] The UK regulator, the FSA, fined Nationwide £980000 for failing to manage IT security risks following the theft of a laptop from an employee in 2007. The FSA found that Nationwide did not know the laptop contained sensitive data and did not launch an investigation until three weeks after the computer was stolen (Anonymous 2008 a).

if anything happened, we learn lessons from it. Every time technology changes, there must be reviews and updates of the plan. We must continually test the plans and procedures".

Security budget: With the increase in the number of security incidents, companies are now confused about how much to spend on security and what to spend it on (Kleinfeld 2006). Interviewee A believed that there is a budget for the security team within his company; however, it is just a percentage of the IT budget. He expressed the following opinion:

"Every year in October, we start to make the budget. I look at the requirements and put the budget for the next year. Although my funding is from the IT, I have a security budget. There is a budget for the security team. The money is just for security, but within the IT budget. My budget is for information system security, for information, people, hardware, software, processes, etc. However, I don't know the percentage spent on AIS security. Security budget is a percentage of IT budget. We have an IT budget which the whole company benefits from. We don't have that granularity of controls. If the accounting department need something for security, they can ask the IT. But every year there is no separate budget for the accounting. We have a security budget for the whole organisation".

In addition, the results reveal that there is no separate budget specifically for AIS security. Interviewee A highlighted this opinion in the following quotation:

"We have a very large system which runs the whole business for us, a part of that is the accounting system. There is no separate budget for AIS security. It is just an overall information security budget. There is nothing specifically for accounting. Our accounting system, finance system, and customer database contain very sensitive information".

He believed that the decision on security spending depends on the requirements of each department, and illustrated his opinion with an example from the accounting department. He stated:

"If we have to spend money on the accounting systems, there would be a recommendation from the accounting manager. The accounting department decided what they required. We have a project team, I am part of that team, and I look for the security aspect. The accounting department make the decision, but they are supported by the IT department".

He claimed that they spend a lot of money on security testing, physical and application security controls, and on salaries of the security team. He stated:

"Physical security controls and logical security controls in order to secure our network and traffic going through our network are quite high. We spend a lot of money on testing, and

on security applications as well; physical, testing, and application security for the whole organisation. Obviously, the human part, salaries of people in the security team takes a big part of the security budget".

However, he believed that his company's security spending is not enough and the budget needs to increase.

Security standards and certification: Thorp (2004) indicated that the British Standard BS 7799 (ISO 27000) provides a good guidance and a framework for building an information security system. Interviewee A believed that although his management does not know exactly what BS 7799 is, they know everything about the policy and procedures, which are all based on it, and therefore they have very good security awareness. He commented:

"My policy and procedures are all based on BS 7799. My management does not know exactly what BS 7799 is, but they know what the policy says, what the procedures are and they still have very good security awareness. We make our reviews and audit work with different teams and departments, and we make it very relevant to each team. We make risk assessment and security awareness training; we make it relevant to each individual team as well. However, the overall security awareness package based on BS 7799 is very general. We did not train them on BS 7799. It is very much based on the documentation of procedures. We just give them what is relevant to their job, only what they need to know".

Although the literature suggests many benefits for companies from being certified under ISO 27001, interviewee A stated that his company is not certified and has no plans of certification. He believed that it is not important to be certified given that they undertake all the necessary internal and external audits, which assure them that all necessary security controls are in place. He presented his opinion in the following quotation:

"No, and we have no intention of certification. We are externally audited each year, and internally audited continually. We have quarterly BCI[5] compliance checks. It is really not important for us. We are not looking for certification right now. We know that we've got all controls in place and that is enough. The BCI says that we are secure. It needs too many processes to do; we must go through several stages. According to the industry, if more companies were certified, we can have it. We are a very complex environment with complex

[5] BCI refers to the Business Continuity Institute, which provides internationally recognised status to members, as professional membership of the BCI demonstrates the members' competence to carry out business continuity management (BCM) to a consistent high standard.

network among different and remote sites. All processes and procedures must be documented in order to be certified. I can't see any direct benefit from it".

AIS security effectiveness: No doubt, after any information security investment, companies have to assess the consequences of business returns (Huang *et al.* 2006), and to assess security effectiveness. Interviewee A confirmed the use of security awareness level among employees, feedback of security tests, and the number of security incidents to measure his company's security effectiveness. He expressed the following opinion:

"Yes according to the number of incidents. For example, if in a certain month we have four security incidents, there must be a problem. If there is no security incident, that is ok. According to the general level of security awareness among employees as well. Regarding the test, everybody has to do the course and the test or read the policy and do the test online. Everybody must do this test including management and me".

This opinion confirmed the questionnaire findings (Section 4.5.2 in Chapter 4) which indicated that insurance & financial services companies that responded devote more effort to security training and awareness, than the other sectors.

Interviewee A also believed that the number of incidents and the feedback of security tests are the company's most important success indicators of security management.

On the other hand, he claimed that people are not following the procedures and therefore they are the main obstacle of effective security within his company. He expressed the following opinion:

"People are not following the procedures. You can put computerised controls in place and they are great, computers do what you tell them to do, and systems do what the programs tell them to do. We have to test controls in place on a daily, weekly, and monthly basis. I must check whether IT department are doing their job according to procedures. Any changes in systems must be automatically reported to me, so I know what is going on. For example, I must check the antivirus in the server, whether it is working, effective, etc. The important point is that people are part of the problem. We have technical processes in place; people are responsible for these processes. People are always in a hurry; they do not want to do the right thing. The weakest link is always the people".

This opinion supported Dhillon (1999) who argued that in many security abuses technology is not causing the problems; it is the people using the technology who tend to subvert the controls in a system. In addition, according to the Security and Information Risk Survey (NCC 2007), the most prevalent risk to information security is the people involved in the development, deployment, and use of IS.

Moreover, interviewee A believed that the overall effectiveness level of AIS security management within his company is very high; however, risks are always changing. He pointed out:

> *"I think the overall security management process is very high. We have good communications, we have good policy and processes that are reviewed, and we have internal and external review processes. We spend thousands of pounds every year hiring people to break our website. We make sure the controls are working. It is not enough to have controls in place, we must constantly test them, reappraise them, review them, assess risks, etc. and we do that. We are very high security aware company, and we have all the security controls in place, but we must never stop and say we are secure. Everything is changing and risks are changing. It is an ongoing process".*

5.5.3 AIS security threats

AIS today are accessible through the internet, they become much more complex, and they are likely to have more vulnerabilities that can be exploited (Jones 2008). Consequently, security professionals need to address an ever increasing number of internal and external threats to their systems' security, while maintaining access to critical IS (Myler and Broadbent 2006). Interviewee A believed that the protection of his company's database, credit card information and identity theft are the most serious security threats facing his company. He pointed out:

> *"Every organisation has its own threats. For me, my biggest threat is the protection of my database, credit cards, not violating the Data Protection Act. The biggest threat in the financial sector is the identity theft, the computer crime right now. People are stealing using others' identity, so I will be very concerned if I see any personal information leaving my company. Identity theft is a very real risk".*

The above opinion is consistent with the Global Security Survey (DTT 2006) which indicated that identity theft is emerging as one of the crimes of the 21st century, particularly in the financial services sector. The Global Information Security Survey (Ernst & Young 2007) also stated that media news about privacy breaches, identity

theft, and loss of personal information have not only raised consumer awareness, but have motivated a sense of the leadership's personal accountability and the absolute need to give priority to privacy and data protection.

In addition, interviewee A cited, not only people inside the company, but also competitors as his company's most frequent threats. He believed that although systems are doing exactly what they should do, people are not always doing the right thing. He expressed his opinion as follows:

> *"The most frequent threat is always people, to get them to do the right thing. Systems are doing exactly what they should do. From my personal point of view, we have a website presence, 90 percent of my business comes initially from the web. We are a highly competitive industry, and people are constantly trying to steal our pricing information. It is all about competitors, they are trying to understand how our pricing policy works. They are other companies; they are trying to make their prices less to attract more customers. This is a most frequent issue, but we have controls in place to identify it".*

This opinion supported Dhillon (1999) who argued that in many security abuses, it is not technology causing problems, but the people using it who tend to subvert the controls in a system. However, in terms of competitors, the Security and Information Risk Survey (NCC 2007) indicated that competitors are one of the least of companies' worries when it comes to their security strategy.

Interviewee A also believed that the most common source of security threats is the people given that 70 percent of his company's risks are internal, whereas only 30 percent of risks are external. He stated:

> *"In the accounting area, we occasionally have instances where people are trying to hide money from their company and make illegitimate gain. In all insurance companies, people steal credit cards, and buy insurance, and we identify this. It is a common threat. Generally speaking, the most common source of security threat is the people factor, people are not following procedures. Only 30 percent of my risk is external and 70 percent of my threats are internal".*

Whitman (2004) pointed out that employees' mistakes and failures to follow policy and procedures represent a dominant threat requiring the implementation of controls to reduce the frequency and severity of such attacks. In addition, Leach (2003) argued that many companies suspect that their internal security threat, which is

predominantly the result of poor user security behaviour, is more pressing than their external threat. Schultz (2005) also indicated that people would not use controls and features that are too difficult to use. They will instead do everything they can to avoid or get around them.

Interviewee A believed that people are always the weakest link in security, and therefore they are the most likely threat his company will be concerned about over the next two years. He commented:

> *"The weakest link is always the human beings, people failing to follow procedures and practices. For example, we have a policy for use of the e-mail. E-mail is a very dangerous thing; it is the route for information to get outside my organisation. If I find someone is misusing the technology, somebody is using the e-mail inappropriately, it is violating certain policy, then I have to report that. With good controls in place, we have to keep checking, but the weakest link is always the human factor".*

This opinion is consistent with Mitnick (2003) who argued that, although companies are more security conscious than ever, some companies are still neglecting their weakest link - their employees. Furnell and Papadaki (2008, p.9) also indicated that people are often the weakest link in the security context, and therefore, even if the technical safeguards are at full strength, the actions of staff within a company could still serve to put things at risk. Moreover, in terms of the inappropriate use of e-mail, Webb (2000) stated that e-mail is probably the most widespread means of changing information; however, it is one of the most vulnerable tools. Britt (2008) also argued that, although e-mail has become the preferred communication tool in business, providing not only a medium for short correspondence but also for sending documents, invoices, etc., it has become a security threat given that sensitive information can be leaked from a company.

5.5.4 AIS security controls

There is no one security solution that is suitable for all companies (Tsohou *et al.* 2006). Security controls are increasingly complex and must be tailored to the business (Jones 2003). Interviewee A indicated that, most recently, his company reviewed the policy of using USB sticks, implemented more audit controls for call recording, detection controls, and controls for monitoring the internet activities and for checking system access. He remarked:

"The most recent security control is the review of our USB controls to make it more manageable. We have audit controls in place for call recording. Information on a telephone call is very important e.g. customer information, so we put controls in place to check who is listening to which call. We put some additional detection controls in place. We are revising our internet activity reporting tools. We are monitoring the internet activities, checking e-mails in and out, internet browsing, computer system usage, and system access. We are not checking all e-mails, we do samples. If there is a problem, we send it to managers. We must not only write the policy, but we must enforce it".

This opinion indicates that most security controls implemented within the company attempt to avoid or reduce employees' errors or their malicious activities. This is not surprising given that 70 percent of this company's risks are internal and the people or employees are its most common source of security threats. Green (2003) argued that company security starts with its own staff given that employees are the company's first line of defence. Interviewee A also stated that his company implemented additional controls for monitoring internet activities. This is consistent with the Global Security Survey (DTT 2007) in which 76 percent of financial institutions monitor employee use of the internet and IS for unauthorised or inappropriate access. Steele and Wargo (2007) also stated that a sophisticated monitoring tool could protect the company from employee error, laziness, or malicious actions. According to the BERR Information Security Breaches Survey (BERR 2008), an acceptable internet usage policy is almost a prerequisite to the implementation of other controls to prevent or detect staff misuse of the internet.

Interviewee A also reported that his company had reviewed the usage policy of USBs. Steele and Wargo (2007) argued that although employees enjoy a wealth of technology enabling remote connectivity with powerful processing and enormous storage capabilities such as laptops and USBs, this technology has increased productivity, but by extending the mobile edge of a company, new security risks arise. It is, therefore, important to determine exactly who is authorised to use these devices, what specific devices are acceptable, and how these devices are used.

In addition, he believed that there is no sizable gap between security threats and controls within his company; however, people are always looking for better systems. He expressed his opinion as follows:

"Constantly, we review security controls and vulnerabilities. There is no sizable gap, but we always want to be better. People are always thinking of better systems, so we have to look at every new system, evaluate it and, if necessary, we buy it in the following year. We have an active security department, and I think some companies do not have that sort of concern about information security. We take ours very seriously. We like to see that controls we have in place are adequate and constantly reassessed. We are constantly looking to find those gaps. In our risk assessment process, we record all risks in all areas, and report them quarterly to the risk management committee, but we should always think of better systems. New systems are coming in all the time and we are constantly appraising what is available, what is not available, and if there is any perceived benefit from it".

He believed that it is important to have a security control to protect confidentiality, integrity and availability of information altogether. He stated:

"The main aim of information security is to protect the confidentiality, integrity and availability of information. If you've got any control that cannot cover at least one of them, you are not doing the right thing. We constantly show an increase in security for those three, all of them are important together. We have some controls which cover one or two of them; we need a control to cover them all".

This opinion is consistent with Wiant (2005) who stated that UK companies regard information as the lifeblood of business and therefore they are increasingly reliant on confidentiality, availability and integrity of their data. A study undertaken by Rainer *et al.* (2007) also showed that both business management and security professionals agreed on the importance of systems that provide information confidentiality, availability and integrity.

In addition, the company is planning to implement new physical access controls on the computer room e.g. biometrics and new internet reporting system over the next year. He commented:

"New physical controls for our computer room will be used. We have already controls to prevent people from going in. No one can enter the computer room, even IT people, not all of them can enter this room, just who needs to, like the one who takes back-up tapes and puts new ones. In the past, we used ID cards. We have a new system coming in this year, which is biometric technique (fingerprint). I am investing in a new internet reporting system as well. I would like also to increase my general security to give me assurance of my people's activities. We allow our people to use the internet in work, but they cannot use commercial games, gambling sites, eBay, etc. We need to identify which sites they tried to go through and they are blocked. I can get reports on that and then give the feedback to the

management team. We want an assurance that employees are not wasting their time. There are now few sites which they can go through to. There is software to check internet activity. We've got one which is not great, so we are getting a quicker one".

The interviewee's opinion regarding biometric technique is consistent with questionnaire findings (Table 4.102 in Chapter 4) where six companies stated that they are planning to use biometrics in the next year, in which two of these companies were from the insurance & financial services sector. Biometrics is an emerging technology that has the potential to improve the effectiveness of internal controls by strengthening access control to assets and IS, improving reliability of financial data and ensuring greater compliance with regulations (Amoruso *et al.* 2005). Joyce (2008) argued that although biometrics is still not widely used, this technology is typically found in large organisations where the security need is high such as financial services, and government agencies. Moreover, their plan to invest in a new internet reporting system emphasised again that the people are their most common source of security threat. This opinion is consistent with the interviewee's opinion in which he believed that 70 percent of his company's risks are internal, and people are always the weakest link in security given that they fail to follow procedures.

Moreover, interviewee A believed that his company is a technology-laden company, and therefore it is hard to find a technology that is not used. He presented the security controls used in his company as follows:

"We probably use quite a range of different controls. We have an internet presence, so we have many controls protecting our networks. We are a very complex environment; there are many controls in place. We have encryption; we always give people access to only what they need for their job. All those controls are in place to minimise risks of losing data and getting ourselves in trouble. We have firewalls, penetration testing, etc. It is hard to find a control we don't use. This does not mean that we are not looking at what is around us. I am constantly reading information security literature to identify any new technologies and informing managers about any new control. We are a very technology-laden company. I really cannot think about any mainstream technology we are not taking advantage of. We are already employing the relevant technology for us. We have everything we need".

This opinion supported the questionnaire findings, which indicated that insurance & financial services companies that responded are more concerned about information security than the other sectors, and therefore they have all the relevant controls in

place. According to the Global Security Survey (DTT 2007), financial institutions are particularly vulnerable given the nature of information they hold. Consequently, as they race to meet customers' expectations and to survive in today's business environment, it is crucial that security controls keep pace.

Finally, interviewee A believed that the security level within his company would improve; however, there is no 'Zero Risk'. He expressed his opinion as follows:

> *"I think it will be better. New risks will emerge and new controls will come in place. Security is one of the largest areas for the IT right now. I think we will progress. I don't know what will be the main areas of spending, but I think our security will improve. There is nothing called 'Zero Risk'. We can always be exposed to more and different risks and our job is to identify and control them before they become a problem".*

To conclude, this insurance company has a structured process for maintaining their AIS security. However, there is no separate budget specifically for AIS security, management does not know exactly what the British Standard BS 7799 is, and they are not certified and have no plans of certification under ISO 27001. The protection of the company's database, credit card information and identity theft are their most serious security threats. Their most common source of security threats is the people given that 70 percent of their risks are internal, whereas only 30 percent of risks are external. Most recently, the company reviewed the policy of using USB sticks, implemented more audit controls for call recording, detection controls, and controls for monitoring the internet activities and for checking system access. In addition, they are planning to implement new physical access controls on the computer room e.g. biometrics and new internet reporting system over the next year. Interviewee A believed that his company is a technology-laden company, and therefore it is hard to find a technology that is not used.

5.6 Interview 2

5.6.1 General information

The second interview was conducted in a media company located in London. The company was established more than 20 years ago. It was registered in the London Stock Exchange and there were approximately 4000 employees working in it. Table 5.3 showed that the company did not have specific information security department,

but there was a solutions management department within the IT department, particularly for the technical part of security. On the other hand, interviewee B was a technology risk manager, who had seven years of experience in his current position. The interviewee had no professional security qualification; however, he was a member of the Institute of Risk Management[6]. Interviewee B believed that it would take him too much time to get the CISSP certification.

5.6.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding the management framework of AIS security within the company.

AIS security policy: Interviewee B confirmed that they had a formal written security policy, which was produced by the corporate risk assurance department, and was updated every two years.

Regarding the distribution of the security policy, he indicated that in their induction, new employees were given information about security, and what was necessary for their jobs. In addition, the security policy should be on the central intranet, but at the same time, the business unit managers can distribute it as required. He pointed out:

> *"The risk assurance department distribute the policy to the managing directors in each area, who push it down to the business units. The business units' managers distribute the security policy to their employees, and then go through it with them. It should be on the central intranet, but it depends on each manager to distribute it according to the needs".*

He believed that staff training and awareness are the most important elements of the security policy, as it is not sufficient to write a policy, it is most important to educate people about what they should and should not do. He also stated that as a security test takes a lot of time and money, his company checks employees' compliance with the policy through auditing. He expressed the following opinion:

> *"Employees have security training, but we will not force them to take an exam, it will cost a lot of time and money. We tailored training for employees according to their needs, and when we do the audit, we understand whether the people are enacting the policy".*

[6] The Institute of Risk Management is a risk management's leading international professional education and training body. It is a not-for profit organisation owned and governed by its members, who are all practising risk professionals.

Moreover, he believed that, from a technical point of view, the company's security policy works well; however, it is not effective from the employees' side. He presented his opinion in the following quotation:

> *"From a technical point of view, it is very effective because we introduce the technology that enables people to work; we do not introduce something so secure, they cannot work. In that way, it is very effective. However, from the employees' side, we recognised the importance of increased awareness. We need to focus on information security training and to make sure it is relevant as well".*

Security training and awareness program: Whitman (2003) argued that the implementation of a security training and awareness program is a fundamental part of a company's security function. Interviewee B stated that for the moment, there is no formal training and awareness program for all employees; however, if employees need any specific training, their managers can arrange it for them, it is provided online, and then they are scored.

On the other hand, he believed that the security awareness level in his company is very good or quite high, although his company has no formal security training and awareness program. He presented the following opinion:

> *"Security awareness level is quite high, given what is happening recently in some companies e.g. loss of customers' data, etc. People now are more aware; they know what they should do, and what they should not do. Although there is no formal training and awareness program, their awareness is quite high".*

Risk assessment: Once a company has the ability to measure its security risks, it has the power to identify and implement appropriate controls based on its real business needs (Kleinfeld 2006). Interviewee B believed that his company is undertaking security risk assessment on a monthly basis; however, this risk assessment is undertaken for the whole company and not just for AIS security. He stated:

> *"We have a risk assessment program. We ensure that any system including accounting conforms to the regulations that are appropriate for the system. There is nothing specific for accounting or AIS. Basic security can be applied to all systems".*

He believed that although the overall risk level in his company is low to medium, some risks would change with time. He commented:

"We predict some risks; we choose to live with predictable risks. The overall risk level is low to medium. It is in the low area. However, some risks will change because of the circumstances and because of our awareness. The awareness level of some areas will change with time. As a general comment: our overall risk level is very predictable".

Incident handling, disaster recovery and business continuity plan: Interviewee B claimed that his company had not experienced any incidents in the last two years. However, he believed that not working according to the PCI DSS[7] (Payment Card Industry Data Security Standard) was the worst security incident that could happen, which could have a huge impact on his company.

Williams (1995) has argued that any type or size of security breach could become disruptive and expensive, so it must make better business sense to take a preventive approach and to try to deal with such a breach as soon as possible. The sooner action is taken; the cheaper it will be for the company in the long run. Interviewee B believed that in responding to any incident, risks have to be assessed first, and then mitigated; however, there is no regulatory body to which the incident can be reported. The incidents are reported to the security technicians, who then report them to their line manager, and send a report to the CIO. Then the CIO sends a report to the managing director of the company. He commented:

"We would assess the risks of the incident. Then, we will decide on how we can mitigate the risks and take steps to mitigate it. For example, some of the employees carry personal data on their laptops, so we will give them direct training on how to protect the data and keep them secure. We assess the risks and act accordingly, but we did not have a regulatory body to report to. Even if there is a significant security incident, we are not going to report it. It is not necessary".

This opinion suggests that the company considers employee training as an important action after security incidents. This is consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that companies in the media & entertainment sector are more likely to invest in additional staff training after incidents.

[7] PSI DSS is a security standard, which applies to merchants, payment service providers, as well as banks, and requires concerned entities to implement more than 220 technical, procedural and skills transfer controls. These are grouped into 12 high-level requirements ranging from implementing security policies to providing employees with security training and collecting audit logs for specific system components (Gorge 2008).

Interviewee B also stated that his company has a formal business continuity plan, which was established by the disaster recovery committee. He pointed out:

> *"The disaster recovery committee is responsible for establishing this plan. They are constantly updating the plan to reflect new events and new changes. This committee meet once a month and are constantly aware of the system requirements, and change this plan according to these requirements. It is not something we produce and put in the cupboard".*

Moreover, he believed that his company's effectiveness in detecting and responding to security incidents is high. He commented:

> *"From insiders, we may be quite aware of every incident. We cannot go on policing the employees or bring them any harm. From the outside, we have a proxy service managed by an outside company, which constantly protects the environment from outside threats. So the company's effectiveness in detecting and responding to security threats is high".*

Security budget: Interviewee B believed that his company does not have a separate security budget; however, there is a security budget with each new system, in addition to the ongoing operational requirements for security. He expressed the following opinion:

> *"Each new system has a budget, so we have an information security budget within each new system for its security and for its compliance with the standards. We also have ongoing operational requirements for security and we have to budget it. However, we don't have a separate security budget. Any budget for handling operational requirements is to be held under the solutions management area".*

In addition, he claimed that security spending is based either on employees' requirements or on the standards or regulations, whatever is higher, and the board of directors approves it. He commented:

> *"It is approved by the board of directors. We budget the information security in two ways, based on our employees requirements and on the relevant regulations that we apply. If we have regulations or standards, and we want to meet these standards, and if they exceed the employees' requirements, the standards will be out of budget. If employees want more than standards, then we make the budget according to their requirements. So it is based on employees' requirements or the standards; whatever is the higher".*

However, he cannot predict next year's budget. He stated:

> *"We spend according to our needs. From the technical side, we do whatever we want. I cannot decide that is enough or not. We can work with a new set of requirements, and then*

in order to satisfy the requirements, we need to spend much money; we cannot dictate our usage or what should be spent. We can have a high spend one year and low spend in the next year. There is no typical spend. We have operational requirements, so we cannot know exactly how much we spend year after year. For the ongoing operational requirements it is reasonable, we do not need anymore. It satisfies all the requirements. However, the budget for the next year is unexpected".

Security standards and certification: Interviewee B believed that the overall awareness level of his company's managers and employees regarding the British Standard BS 7799 is high among IT people, whereas it is very low within the business unit. He justified this low level of awareness as follows:

"Within the IT area, the awareness level is very high, while within the business unit, it is very low. It could be because it is not promoted as a business level standard, it is promoted as an IT standard. If it is promoted as a business level standard, I think the awareness level will be greater".

He stated that it is not necessary for his company to be certified under ISO 27001; however, he emphasised the importance of being compliant with the standard. He believed that compliance could provide the company with sound information security. He stated:

"Yes absolutely, I think compliance gives us sound information security, but certification no. We comply and that should be enough".

This opinion supported Trcek (2003) who argued that many companies go only for compliance, without certification.

AIS security effectiveness: There is a strong argument that security must be tested in order to ensure that it actually works as expected (Furnell and Papadaki 2008). Interviewee B cited the use of audit in addition to the risk assessment for measuring security effectiveness. He presented his opinion as follows:

"Yes, from a technology point of view, effectiveness is measured through the risk assessment that we perform against the standards. From the users or employees point of view, the measurement is done through the audit".

He also reported employees' awareness as the most important success indicator of security management within his company. He remarked:

"The most important success indicator is the employees' awareness, not 'zero incidents', because there may be some incidents, that the employees are not aware of. There is no absolute security for any company. I am sure that people are always doing something they are not aware of".

5.6.3 AIS security threats

Interviewee B indicated that people are his company's most serious threat given that in some instances they unintentionally or intentionally bypass the system. He stated:

"People or employees are the most serious threat. Someone is doing something without thinking, someone is deliberately bypassing the system, or someone is writing down something when he should not write it down".

He also believed that the biggest and most frequent threat is the people misusing the systems. He commented:

"People are the most serious and most frequent threat facing the company's systems. I am not saying that they do it; I am saying that the biggest threat is misusing the system. It is not something external trying to get into the system. We have to be sure that we teach people how to use the system properly and I think it is the biggest threat".

Mouratidis *et al.* (2008) pointed out that the human user was the single greatest threat to the stability and security of a system. However, this threat is not always malicious. Most often, users who were uninformed of how a system operates could create negative outcomes just from a failure to adhere to policy or to follow procedures.

In addition, interviewee B stated that his company would be concerned about employees' security training and awareness in the next year given that employees' awareness could mitigate security risks. Da Veiga and Eloff (2007) indicated that since human error rather than flawed technology is the root cause of most security breaches, the solution would be to create a security aware culture.

5.6.4 AIS security controls

Interviewee B cited the vulnerability testing as the most recent security control employed in his company. Nyanchama (2005) indicated that vulnerability management is concerned with minimising risks associated with vulnerabilities. Companies without sound vulnerability management processes risk both direct and indirect losses in productivity, service outage, and reputation, among others.

Interviewee B believed that according to the risk assessment, the risk level within his company is low to medium, and they are using all security controls relevant to their businesses; consequently, there is no huge gap between security threats and controls and there is no need at the moment for new controls. However, he stated that they are planning to employ remote access controls on their network. He commented:

> *"Access to our network from outside is the most important control we are looking for. Employees have access from their homes and from remote offices that are actually on the network. This is a very important control and we are planning to employ it in the next two years, because we have companies abroad that need to have access to the system. They need to be sure that we are secure; they need to use the network securely and get into the system. So, access controls are something very important for the next two years".*

According to the BERR Information Security Breaches Survey (BERR 2008), enabling remote access opens up the core network to unauthorised users. Ewing *et al.* (2007) also argued that security is the number one reservation employers have about enabling remote access. Consequently, secure remote access has become an essential business requirement.

Finally, interviewee B believed that the security level within his company would improve given that new access controls to systems would be employed by the next year.

To conclude, this media company has a framework for managing their AIS security. However, for the moment, there is no formal training and awareness program for all employees, the company does not have a separate security budget; however, there is a security budget with each new system, in addition to the ongoing operational requirements for security. The overall awareness level of the company's managers and employees regarding the British Standard BS 7799 is high among IT people, whereas it is very low within the business unit, and it is not necessary to be certified under ISO 27001. The biggest and most frequent threat is the people misusing the systems. The company would be concerned about employees' security training and awareness in the next year given that employees' awareness could mitigate security risks. In addition, the vulnerability testing is the most recent security control employed, and they are planning to employ remote access controls on their network.

5.7 Interview 3

5.7.1 General information

The third interview was conducted in a property (real estate) company located in London. The company was established more than 20 years ago. It was registered in the London Stock Exchange and it had approximately 12000 employees worldwide. There were two departments in the company, one for the security of IT and for anything to do with computing i.e. technical issues, and the other was the risk management department. This department took a much broader view of security, particularly in undertaking security risk assessment for anything that might have an impact on the company, not just the technology risks. On the other hand, interviewee C was a group IT director, who had 11 years of experience in his current position, and he was one of the board of directors of the company.

5.7.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding the management framework of AIS security within his company.

AIS security policy: Interviewee C confirmed that they had a written security policy, which had been created nearly 10 years ago and was changing all the time or as required. In addition, he cited the user responsibility or accountability - employees and outsiders - as the most important element of their security policy.

Hinde (1998) indicated that it does not matter how brilliant a policy is, without the active commitment of employees and management it will fail. Interviewee C indicated that most of his company's applications and software could audit and check whether processes are done correctly.

However, he believed that the security policy in his company is not effective since people are always breaking the rules. He expressed the following opinion:

> *"The policy contains rules, but most of the people break the rules every day. Our policy is not effective. We make employees aware of the policy but we cannot spend a lot of time and money checking whether people comply with it".*

Security training and awareness program: Interviewee C reported the non-existence of a formal security training and awareness program within his company;

however, he believed that employees receive the relevant training for getting their work done. He also claimed that he had received security training in other companies more than 11 years ago.

Interestingly, despite the wide agreement regarding online security training and awareness, interviewee C indicated that sometimes the employees complain that there is no time even for online training, given that they have many training courses covering different security issues. He stated:

> *"With computer-based training, we can know whether people have been online, and whether they have done it. We can put a questionnaire into it, and we can put an exam at the end. But you have to understand that people will always say 'do you want me to bring some money for the company or to sit there, filling some forms, reading all this stuff'. And our answer is always 'really' to go out and earn some money for the company".*

He believed that even if companies send brochures to all employees, there is no guarantee that they read them. He commented:

> *"We can send out a very nice brochure with useful information, but we cannot guarantee people will read it. We get a small percentage who always read it, we get a small percentage who will never read it, and we get some in the middle, sometimes they read it, and sometimes they do not".*

He also believed that employees in his company did understand the need for security; however, they had acquired this awareness from their personal experience. He commented:

> *"They have a reasonable grasp, not that much from the company, but from personal experience at home from their own computers. Being hit by viruses and phishing attacks and losing much information, this makes them more aware and they became much more careful about what they are doing. They buy anti-virus software; they learn it through personal experience and apply it to work. They say: now we understand why we have to change our passwords, why we have an anti-virus system, and why we block some websites so they cannot go through. This is something that will live with them for life, but if we give them these things in training, they will forget everything about it".*

Risk assessment: Interviewee C believed that risk assessment is undertaken for the whole company and not just for AIS security. He commented:

> *"Risk assessment is not focusing on IS or AIS, but on anything that affect the company and its customers".*

He stated that a formal risk assessment is done within his company once a year; however, he believed that risk assessment is a running process undertaken throughout the year. He commented:

> *"It is formally done once a year, but there is a review process, because if we recognise a risk, we have to put actions in place to do something about it, or we have to make a judgement that says this risk is so small that we cannot do anything about it. The process is running. Once risks are listed, we must have an action plan. This is an ongoing process driven by internal team that moves on through the whole year until the whole thing is run again in the following year. Formally, it is done once a year, but actually it is ongoing".*

He also indicated that risk assessment is delivered through the risk management team within his company with the help of third parties such as external auditors, experts, and consultants. They tend to look at a scale ranging from red to green. He explained the risk assessment process as follows:

> *"Risk assessment is a part of the external audit process and is delivered through our risk management team. It looks at the risks that were recognised last year, what the action plan was to address them, what the result was after the plan, and then the whole process will be repeated. We will take this year's risks; see what we are going to do about them. Many risks tend to revolve around processes more than technology. These days we have back-ups, we put data on tapes, send it to other sites, we have disaster recovery plans, so it tends to be much more related to issues that damage the company, its brand, its reputation, leakage of information, etc. We tend to look at a certain scale ranging from red to amber to green, where red are things that are really serious, and green is ok. At the moment, all the risks of our information systems are green or amber".*

Interviewee C believed that although the risk level in his company is quite low, some risks would change with time. He pointed out:

> *"We have not had any specific security failures in the last 12 years. Of course, something can happen tomorrow. Now I am confident that the rules are appropriate. I don't think I can overdo security, unless there is enough money or if it is really worth it. However, somebody can always find a way of breaking in and doing something. For example, there is an incentive to damage a bank because there is a chance to steal a large amount of money, or to do significant damage to the reputation. But in a company like ours, if you break into our accounting systems, there are no millions there, so people do not tend to attack our company or come to us to steal money. That does not mean we should take security easy, it means we are not the highest risk type of company. Now, all risks of our IS are green or amber, so they are ok. We have to accept that somebody might break into our network, we spend a lot of money on protecting systems, but it is still possible, so it cannot be green, but*

it is not red. We do have protection here, and it is adequate, but there is no guarantee all the time that it will be green. It is an acceptable level of risk".

Incident handling, disaster recovery and business continuity plan: Interviewee C claimed that his company had not experienced any incidents in the last two years; however, he thought the loss or leakage of client data would be the worst incident that could damage his company's brand. He presented the following opinion:

"The loss or leakage of client data will be very embarrassing, the worst if it goes out to somebody that is not supposed to have it, either intentionally or by mistake. The leakage of client data is the biggest fear, not like the loss of financial information, but very specifically, the client information that we hold in trust for people, so we have to be careful. That could be the absolute worst incident that could happen to us, because it could damage our brand, then customers will not do business with us, and we will never recover".

He stated that the HR department is responsible for the security incident handling procedures within his company. He commented:

"They are part of the HR department. It is a part of the disciplinary procedures, which collect information on incidents, the behaviour of persons involved, how they comply with our general behaviour requirements of employees. It is handled by a senior manager who goes through that to decide whether we have done something inappropriate, and if necessary we bring a lawyer or the police, depending exactly on the nature of the incident".

Moreover, he believed that after a security incident, they collect data, take actions based on these data, learn from incidents, and they can change their procedures and policy to avoid the incident happening again. He stated:

"We collect data, then we take actions based on the information we collected. If information goes to the public about clients, we will have to work with them to see how we could address the situation. It will take steps to either discipline or possibly involve the police if the rules are broken intentionally. We may have to take steps to protect our image, so we tend to redevelop our procedures and change the policy if there was an error. We have to learn from it, and hopefully, we can avoid it in the future".

However, they do not have regulatory bodies or outside authorities to whom they can report security incidents. Interviewee C believed that it is more important to maintain their brand than the financial loss of any security incident, and therefore, if they are able to cover the incident internally, they do not report to the police. He expressed his opinion as follows:

"If somebody is breaking the law and gives information when he should not, you find most companies will not report it to the police because they want to protect their brand image. So, the answer is 'yes of course we would report', but in reality I doubt we actually would. If we could cover the situation, if it had not damaged a client, if we could cover the money, we could get rid of the employee and we would not take him to court. Our brand is more important than money, and more important than taking an employee to court, and the time and effort to do it is painful. We would hope we only employ honest people, but who can tell?".

He also believed that there are individual business continuity plans for each location and a national plan for the whole company and there is a specific director responsible for this plan. He stated:

"We have a specialist director responsible for business continuity, because it is not just about IT and getting the IT back. In terms of business continuity, you might lose a building, it is about what you do with staff, how you handle communications to the press, how you get in touch with relatives, etc. There is a director responsible for that, there are individual plans for each location, and there is a national plan. That is something that has become very important over the last 4 years. Many of our clients that deal with us on an ongoing basis want to see this plan before signing up to a contract. It can be because terrorist activities have been raised in people's minds, so buildings can be damaged. Now rather than just saying 'we know you are a good company', they asked 'What would happen if there are problems? How could you cope? Who would take over? Who are the other people if we lost the team?, etc.'. Our clients are much more demanding about our processes and procedures, particularly in relation to a business continuity plan".

On the other hand, he believed that, despite being adequate in detecting and responding to security incidents, there is no guarantee that nothing can happen tomorrow. He commented:

"We consider it adequate, but nobody can be 100 percent perfect. I cannot say everything is good, anything can happen tomorrow. If something happens tomorrow, we could say that it is completely inadequate. Now, I can say that everything is all right".

Security budget: Interviewee C believed that the budget within his company includes three major elements: the strategic element, maintenance, and technical enhancements. He pointed out:

"We have strategic goals for the business. We have a strategic business plan. We get some IT budget driven out of the business plan. We get budget allocation to update all our products. In security terms, if we get firewalls today, we decide that we need a new version

of it; we get some sort of maintenance. There are different elements: it is the strategic decision, maintenance, and the enhancements, which are related to specific applications or additional functions. We also need to find how the company is changing and to add to the budget. Now we have broadband everywhere, all users get access to the applications. We must have bigger network links, faster firewalls to cope with more traffic, etc. So the budget includes three major parts: strategic part, maintenance, and technical enhancements".

He stated that disaster recovery and continuity planning take a big part of the company's security budget, in addition to the anti-virus, anti-phishing, anti-spam software, and the firewalls. However, he believed that his company's overall security spending level is not enough and the budget needs to increase. Interviewee C justified the low level of security spending by the lack of understanding at the executive level. He commented:

"In truth it is less than we would like, and the problem here is the lack of understanding at the executive level, they haven't got an example of what happens if it goes wrong, if there is a major security incident. Because we have done it recently well and we haven't had a problem for years; they say: why do we need to spend all this money on new firewalls? The old ones are still working. It is difficult to convince them with a good justification".

On the other hand, he claimed that the security budget would be a bit higher next year. He believed that the budget is expected to increase by nearly 15 percent given that the company is bigger than last year.

Security standards and certification: Interviewee C believed that there is no idea at all within his company about the British Standard BS 7799. He commented:

"The business has no understanding of what is BS 7799 at all anywhere within the company. They have no understanding of it and there is no interest in it".

He also believed that there is no benefit from being certified under ISO 27001. He stated:

"Will it bring the company more money or more clients? For the moment, there is no recognised benefit to the business in being certified. It will cost time and money to do it. There is nothing driving us. We just see it as a cost, not a benefit. It is not necessary. In the commercial world, it is not about benefits, it is about balancing what is my return on investment, and the time, money and resources spent. So, what will I get back?".

He claimed that there are no benefits for his company from compliance with the standard, given that it costs too much time and effort, and the clients do not require it. He provided an example of complying with the ISO 9001, to justify his opinion:

> *"Years ago we spent a lot of money complying with the quality standard ISO 9001. We spent a lot of money getting all our departments ISO 9001 compliant, we had external auditors and evidence with huge filing systems were set up, and we got it. For a little while, there is a business benefit. At the bottom of our letterhead, we could put 'ISO Compliant', then everybody got it and it did not make any difference anymore. For the moment, clients are not asking us whether we are doing anything with the BS 7799, so there is no recognised benefit in being compliant. It will cost time and money to do it".*

AIS security effectiveness: According to Wright (2006), measuring security effectiveness eases the process of monitoring the effectiveness of a security management system, and provides tangible evidence to auditors and assurances to management that the company is in control. Interviewee C stated that his company brings specialist teams who do penetration testing and try to break in to evaluate security effectiveness. In addition, he believed that the non-occurrence of security incidents is the most important success indicator of security management within his company.

5.7.3 AIS security threats

Interviewee C cited the loss of client information as his company's most serious threat, and attributed this loss to the misbehaviour of employees. He commented:

> *"It comes back to the people, and specifically it is the loss of clients' information which leads to brand damage. With the best security systems in place, you still have got the issue that users can look at the information, can make a copy of it, can e-mail it, and can also take a screen copy, and that's what a lot of people do. They know that they can get another job, they can accept the job, and they can spend sometime copying all the stuff they want, take them home, then put in a resignation, you cannot really stop that".*

This opinion is consistent with Lin (2006) who indicated that there would always be some risk that authorised employees will misuse data they have access to in the course of their work. Gerard *et al.* (2004) also stated that a dishonest employee could steal vast amounts of a company's information and move on to a new company, before the theft is discovered. In addition, Mattsson (2007) argued that many abuses and

accidents occur because people have access to data that they do not need to see, or do need to see but should not be able to alter or delete.

Interviewee C believed that people are the most common source of security threats facing his company and that employees are his company's biggest threat over the next few years.

5.7.4 AIS security controls

Interviewee C indicated that, most recently, his company had improved the firewalls. However, he believed that his company's security controls are enough, and therefore, no gaps exist between security threats and security controls used; consequently, there is no need for new controls. On the other hand, he believed that it is better to bring new versions of all security controls implemented in his company. He commented:

> *"There is nothing I could think we are not using. Just, the qualities of the products or controls we are using are of lesser standard than the products banks and other financial institutions are putting in".*

To conclude, this property company has a framework for managing their AIS security. However, there is no formal security training and awareness program within the company, and employees receive the relevant training for getting their work done. The risk assessment is undertaken for the whole company and not just for AIS security. There is no idea at all within the company about the British Standard BS 7799, and they believed that there is no benefit from being certified under ISO 27001. The loss of client information is the company's most serious threat, and people are the most common source of threats. Most recently, the company had improved the firewalls. They believed that there is no need for new controls; however, it is better to bring new versions of all security controls implemented in the company.

5.8 Interview 4

5.8.1 General information

The fourth interview was conducted in a property (real estate) company located in London. The company was established more than 20 years ago. The company was registered in the London Stock Exchange, and there were approximately 24 employees working in it; however, the company's turnover was more than £300

million. There was no security department or team within the company, given that it had only 24 employees. On the other hand, interviewee D was a group accountant (looking after IT), who has 15 years of experience in his current position.

5.8.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding his company's management framework of AIS security.

AIS security policy: Interviewee D believed that there is no written security policy within his company. He provided a justification for the non-existence of a policy in the following quotation:

> *"We have a security policy, but it is not an official document and it is not written down. Since there is small number of persons in the company, we discuss security informally all the time. There is no need of a formal document".*

Security training and awareness program: Interviewee D indicated that his company provides training for new employees on a one-to-one basis, and then they can interact with other people in the company. He also believed that employees could get additional training if a major change to the system takes place. However, he stated that his company is not measuring or monitoring employees' security awareness.

Risk assessment: Interviewee C believed that his company is undertaking security risk assessment at least once a year with the help of third parties such as external auditors, experts, consultants, and assessors, and they are assessing their risks using a specific agenda, which he identified as follows:

> *"We have an agenda. We would have the last year assessment to see where we are in this year, where we are from the last year, what is new in this risk assessment, what are the new challenges, etc. It is a part of a wider business continuity plan".*

Incident handling, disaster recovery and business continuity plan: Interviewee D believed that his company had experienced some minor security incidents in which loss of data was one of them, and they contained them very quickly and effectively. He commented:

> *"There are no significant incidents. Obviously, they are minor ones. We had an incident where data had been lost, but we were able to recover quickly and prevent it from becoming*

a bigger incident. Obviously, we have incidents, but because they are contained quickly, they do not develop into major incidents".

He cited some serious incidents that could have a significant effect on his company including loss or corruption of data, accidental damage to IS and disgruntled employees. He stated:

"The thing that we can think of it is the disgruntled employees, or the corruption of data. We are quite a small team, and if an employee was unhappy, for any reason, we either solve the problem or force him to leave. So we could take action before the incident can cause damage, and we are proactive in this respect".

He believed that although his company has some procedures to handle any security incidents they could face, they are not formal ones. However, there is a business continuity plan within the company, which he believed is formally reviewed once a year and is informally reviewed all the time. He also emphasised the importance of this business continuity plan and presented the following opinion:

"A business continuity plan is very important to us. We need to make sure if there is an incident, we can recover and continue with our business very quickly, not only here, but in other parts of our business which may be outsourced. For example, the internet connection is outsourced, so we have to make sure that it can recover quickly if there is an incident. So we have a written business continuity plan".

Security budget: Interviewee D believed that his company does not have a separate security budget; however, it is just a percentage of the IT budget. He stated that they could not delegate security to anyone in the company; consequently, there is no specific budget for security. In addition, he claimed that security spending in his company is a need-driven not a budget-driven. If they need anything, then they can buy it regardless there is a budget for it or not. He also stated that if a small amount of money is needed, he could approve it; however, if it is large, the board of directors approves it. Moreover, he believed that physical access controls are the top areas of spending on security within his company. Consequently, he believed that the security spending level is moderate or adequate.

Security standards and certification: Interviewee D believed that there is no idea at all within his company about the British Standard BS 7799. In addition, despite believing that certification under ISO 27001 can maintain the company's public

image; he believed that the company has to spend a lot of time and money on documenting all procedures before being certified and consequently it is not necessary to be certified.

AIS security effectiveness: Interviewee D believed that they are not measuring or evaluating their AIS security effectiveness. However, he claimed that the non-occurrence of security incidents is the most important success indicator of security management. He believed that the occurrence of major or even minor incidents indicates that there is a problem in their system. He pointed out:

> *"If there are no major incidents it is good. If there are even small or minor incidents, there is a problem. If there are any incidents, I would think there is a problem in our systems and in this case we have to review these systems".*

On the other hand, he believed that the lack of support of senior management is their top obstacle of effective security. He commented:

> *"The big obstacle is that the staff want to bring in changes, but they are not able to get the board support. Without this support, they cannot implement the changes they need. Security issues are not being a top priority for the board; the board have other things to think about. They do not give sufficient time to the problems they do not understand. These problems are more technical, so they tend not to take decisions on them. I think the ignorance of the board of directors is the obstacle because there is no one pushing for change".*

This opinion is consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that in some cases, senior management might not understand the security issues their business is facing.

5.8.3 AIS security threats

Although the virus threat is no longer been identified as a key concern to the majority of companies, and the BERR Information Security Breaches Survey (BERR 2008) addressed the decline in the reported virus attacks, interviewee D cited a virus attack as his company's most serious security threat. Lin (2006) argued that it is almost impossible to protect a network completely from virus attacks. On the other hand, interviewee D cited the theft or loss of customer data as his company's most likely security threat over the next few years.

5.8.4 AIS security controls

Interviewee D indicated that, most recently, his company had employed more controls over access to the building and to some of its parts i.e. physical access controls. He believed that his company's security controls are enough; they were using all security controls relevant to their businesses and therefore, no gaps exist between security threats and security controls used. Consequently, there are no plans for any new security controls in the next year. He believed that too much security control could disrupt employees. He stated:

> *"We would not change anything substantially. We've got what we need, and I think too many controls will disrupt the work of the group, so they cannot do their work efficiently. If there are too many controls, they will be seen as 'controls just for the sake of controls'. We need the right amount of controls to do our work and to run our business efficiently".*

This opinion is consistent with Rainer *et al.* (2007) who argued that excessively rigorous security controls could reduce employee productivity and could even decrease security. In addition, Post and Kagan (2007) argued that tightening security by making systems more inaccessible could hinder employees and make them less productive. This indicates that a security level would not necessarily improve merely by using more controls. Moreover, Hunt (2006) indicated that being an effective security manager is not merely a matter of buying another layer of technology; it is a matter of seeking value in finding better ways to use what you already have.

To conclude, this property (real estate) company has no framework for managing their AIS security. Given that there were approximately 24 employees working in it, there is no written security policy, there are no formal procedures to handle security incidents they could face, they could not delegate security to anyone in the company; consequently, there is no specific budget for security. There is no idea at all within the company about the British Standard BS 7799. The virus attacks are the company's most serious security threat, and the theft or loss of customer data is the most likely security threat over the next few years. Most recently, the company had employed more controls over access to the building and to some of its parts i.e. physical access controls. However, the interviewee believed that too much security controls could disrupt employees.

5.9 Interview 5

5.9.1 General information

The fifth interview was conducted in a utilities company located in Huntingdon. The company was established more than 20 years ago. It was registered in the London Stock Exchange and there were approximately 3500 employees in it. The company had a new security team, which was included in the IT department within the company and reported directly to the IT director. On the other hand, interviewee E was a security risk manager, who had 6-7 years of experience in her current position; however, she had a total of 14 years of experience in the company. She had the Information Systems Security Professionals qualification (ISSP), and the qualification obtained from the British Computer Society (BCS).

5.9.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding the management framework of AIS security within her company.

AIS security policy: Interviewee E confirmed that they had a small written security policy, which was established and reviewed by a team within her company. This team included the finance director, IT director, risk management committee, internal auditors, and the corporate risk manager. However, the finance director had to sign this security policy. She believed that her company had not updated the security policy for nearly five years; however, they aim to update it once a year. She emphasised the importance of updating the policy annually in the following opinion:

> *"If we say we update the policy every year, it will be unfair because we didn't do it for 5 years, but our aim is to review the policy once a year and I think this will be a good discipline for us. It is better to make a simple review, just to think about what happened last year, find any difficulties, and any other improvements we could make in the policy. I think it is wise to do it once a year, even if we are not going to change it, we are confirming we have reviewed it, because it helps to think about how the risks are changing".*

She stated that in their induction, employees were given either a hardcopy of the policy or the information security booklet. On the other hand, she emphasised the importance of monitoring employees to check their compliance with the security policy. She remarked:

"We have campaigns and posters for using the e-mail and internet saying: 'Use it but not abuse it'. They can use the internet for personal reasons, but they must not abuse it. We are monitoring this. We must tell people that we are monitoring them. If people come in and want to use the system, they get it briefed in a document called '10 Steps to IT Security'. We do not want to depend heavily on saying 'If you do this, this will happen to you'. We are just trying to put a spot of light on things".

This opinion is consistent with Wood (1997) who argued that if employees know management is not going to check upon them, there would be no motivation to comply.

Security training and awareness program: Interviewee E claimed that every employee in her company - new and current - had security training. She believed that the classroom is the most effective technique for making staff aware of security issues; however, due to cost and time constraints, her company is providing employees with security awareness materials online. She also stated that although they measure and monitor staff awareness, the awareness level in her company is not high given the feedback of the security tests. She expressed the following opinion:

"Yes, we measure employees' awareness. It is a bit ad hoc. With the help of the corporate communications, we made a little test, and we sent it to our employees to complete it. However, we found that people are not aware where to look at the policy. Some of them had never read it; some of them had read it but could not remember what was in it. We learned a lot from that, it helped us to get the next poster campaign".

Risk assessment: Interviewee E confirmed that her company is undertaking security risk assessment on a continuous basis or as required. She presented her opinion as follows:

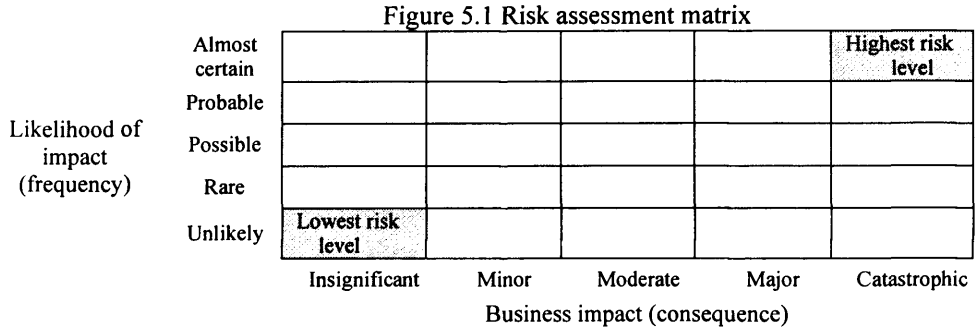
"We do series of things during the year such as penetration tests, vulnerability tests, etc. We also review projects, do business continuity exercise, taking-up tapes and try to install them. It is an as required process. It is also continuous with respect to those systems that have been established".

They use a 5*5 matrix in assessing their risks. She illustrated this matrix in Figure 5.1 and stated:

*"We have got a number of tools to help us. One of the important tools is a 5*5 matrix. There is 8 steps guide called 'Personal Guide to Managing Risks'. This guide helps people to think about impacts and probabilities. It is very generic. We use it to think about risks in terms of probability and impacts. What does that really mean to us? Does it mean potential*

loss of income or perhaps some illegal activities or perhaps we fail to comply, etc. We try to get people to think about how to manage risks and to know the processes".

Figure 5.1 Risk assessment matrix



(Source: A leaflet was given to the researcher during the interview)

Incident handling, disaster recovery and business continuity plan: Interviewee E believed that her company experienced a serious security incident in the last two years, in which they had lost a whole day's data. She considered it a serious problem, given that the company could not recover these data. This is not a surprising opinion, given that utilities companies are dealing with millions of customers; consequently, any downtime or any loss of customer data might be a disaster for such companies. In addition, she reported the occurrence of computer abuse, containing inappropriate material, which is not consistent with the BERR Information Security Breaches Survey (BERR 2008) in which the companies least affected by staff misuse are the utilities companies. She also considered the failure to recover from a disaster, given the loss of records and back-up tapes, as a worst security incident.

However, interviewee E indicated that there is a difference between dealing with an IT incident and a security incident. She stated:

"We have formal procedures. It is quite different when you have an IT incident than when you have a security incident. If you get an outage, or if people cannot work for some reason because there is an issue that will be dealt with very quickly, the help desk will respond to that very quickly. That is the service management. Security incident handling is slightly different. If you got the service down, and people cannot work, it is an incident, and if it is particularly severe, we call it 'category one', and we go down to 'category 3'. In this case, somebody must look at that incident to make sure there is no contributed effect and nothing there caused that outage to do with security. Sometimes this outage was caused by an individual pressing the button and doing wrong thing at the wrong time, which is a security incident because somebody has too much access to the system without training. The rule here is that every major incident must be investigated to make sure it is not a security-related incident, and if it is a security-related one, we must know why it happened".

On the other hand, she did not mention any authority to whom they can report security incidents; however, she indicated that it depends on the incident, whether to let the police get involved or not. She pointed out:

> *"If we identified any fraudulent activity, a decision would be made whether or not we prosecute. In the past, we had prosecuted somebody and he went to prison. If it is a low level fraud, we may not get the police involved. Getting the police involved is not automatically asked, we investigate, recommend, then we go to the HR".*

This opinion, therefore, suggests that utilities companies are not obligated to report security incidents to specific authorities despite having different authorities such as the DWI (Drinking Water Inspectorate) and the EA (Environment Agency).

Moreover, interviewee E stated that after a security incident, they could amend practices and standards, but not the policies. She remarked:

> *"It depends on the severity of the incident. If we've got a fraudulent activity, then we must document what we have got on the risk. If it is a high risk, we may choose to do or not to do anything about it. If it is a very low risk happening very often, it is not cost effective to do something about it. We could amend the practices and standards, not the policy. If we've got a certain incident, we must investigate how this happened. We have an investigation and a report of recommendations".*

She emphasised the importance of having a business continuity plan and back-ups in place. She commented:

> *"Yes we have a business continuity plan. It is easy but quite comprehensive. It is important to document what the business continuity requirements are. We need to know day by day whether there are back-ups and to make sure that everything is backed-up".*

She reported that this plan is a joint responsibility between the internal service manager within her company and an external service manager. However, although the business continuity plan is tested annually, it is not tested in full. She explained the process of testing the plan in the following quotation:

> *"We test the plan annually, but not in full. We have a comprehensive written plan. Every year around June we decide what we need to test. It is a formal testing; we take one or two back-up tapes and try to restore them, etc. Last year I asked the vulnerability testing people just to have a look at the plan and they highlighted some issues, then we update it. We find that systems change over time, hardware changes overtime, network configuration changes overtime. So a business continuity plan helps us to know what is important to do".*

According to the Canadian Institute of Chartered Accountants (CICA 2005), as data, technologies, systems, and processes evolve; a company must continually update its business continuity plan to ensure that it remains current.

Security budget: Interestingly, interviewee E, who believed her company has a separate security budget, emphasised the difficulty of asking management for this budget. She commented:

> *"We've got a security budget within the information security department. However, when you actually want to go and get the full funding, this is another hoop that you have to go through".*

This opinion supported Lindup (1996) who emphasised the great difficulty the IT professionals face in convincing management to invest in security projects.

On the other hand, she indicated that security spending decision is made within her company's five year plan, and the budget is approved by the IT director, and ultimately by the company's strategy manager. She pointed out:

> *"I draw up a 5 year plan, with every small detail around year 1 and year 2 and less around years 3, 4 and 5 because it tends to be more strategic. For this year, I have to estimate how much the security solutions products will cost. We have to do a business case for each one, and then we make a decision on what we want to spend the money on. The budget is approved by the IT director and by the company's strategy manager. The IT director has to go to the strategy manager to get his budget".*

She also indicated that outsourcing i.e. external service providers, identity management and encryption technology on laptops are the biggest part of their security budget. This reflects the reaction of some companies to encrypt their laptops after the increasing incidents of organisations losing laptops containing unencrypted sensitive information. However, she cannot predict next year's budget.

Security standards and certification: Interviewee E believed that the awareness level of the security team and of some project managers regarding the British Standard BS 7799 is high; however, there is no general awareness of the standard. In addition, they are not certified under ISO 27001; however, they are planning to be certified.

On the other hand, although she believed that there are no business benefits from this standard, she pointed out that it provides her company with an excellent reference point, and provides customers with a certain level of assurance. This opinion supported Buzzard (1999) who indicated that BS 7799 is a reference for managers and employees who are responsible for initiating, implementing, and maintaining security within their companies. Da Veiga and Eloff (2007) also argued that this standard takes the form of guidance and recommendations and is intended to serve as a single reference point for identifying the range of controls needed for most situations where IS are used.

AIS security effectiveness: Interviewee E believed that her company is undertaking internal and external security audits to evaluate security effectiveness; however, it is difficult to measure everything and it is useful to focus on small important areas to measure. She stated:

> *"At the beginning of the last year, we had PricewaterhouseCoopers to do some pre-audit work, and they were able to identify some areas for improvement. According to their recommendations, our baselines needed to improve. I personally look at how we comply, but standard is covering the best practice for everything, and we don't have the money to do all these best practices. I think it is quite useful to take one small area and to say this is really important to us, but you cannot measure everything".*

She also believed that the effectiveness level of security management within her company is moderate or reasonable.

5.9.3 AIS security threats

Interviewee E believed that contractors and inappropriate access are her company's most common sources of security threats. She commented:

> *"Contractors, actually bringing their laptops and attaching them to our networks, this is a kind of internal threat. I think the other threat is to be around inappropriate access. We can break that down into two: inappropriate access which means that managers do not understand what the employees really got access to. Inappropriate use is generally about websites, internally and externally, and we blocked now many websites having problems with gambling, dating, sports, etc. it is a security issue more than productivity".*

Frolick (2003) argued that as more companies develop websites, there is a corresponding increase in attacks to maliciously damage a company's reputation or

steal its resources. In addition, Lee *et al.* (2008) indicated that employees' internet misuse has emerged as one of the major concerns that managers deal with in today's business environment. Internet misuse has exposed companies' IS to different threats that put companies at risk (Mitchell and Jones 2002). Lee and Lee (2002) remarked that internet misuse problems tend to increase as employees become more skilled in new technologies.

Moreover, interviewee E believed that internal fraud is her company's most likely threat over the next years. Haugen and Selin (1999) stated that companies now are more susceptible to computer crime and employee fraud than ever before. As companies struggle to remain competitive in a global marketplace, systems are left open to employees' manipulation and the opportunity for significant loss is always present. Consequently, if management pays little attention to their employees, fraud will be perpetrated by those insiders in a company who have access to accounting systems. Onions (2006) also indicated that the levels of fraud in the UK are massive and the risks are not countered by sufficient controls. In addition, Clarke (2007) viewed that staff fraud is on the rise, which could hit not only the finance but also the reputation of a business.

5.9.4 AIS security controls

Interviewee E stated that, most recently, her company implemented a perimeter security system for controlling the internet and for monitoring the access. She presented the following opinion:

> *"It is a perimeter security system, looking at network security, who is trying to hack in, put it in control and monitoring the access. It is not just access, any kind of malicious and viruses as well. We must make sure that our perimeter is hard. Can you imagine if somebody can hack to our system with about 6 million customers records, bank accounts details, names, addresses, salaries, etc.?. We do not have a proper intrusion detection system. But we do monitor that through a number of ad hoc tools rather than intrusion detection or prevention systems".*

Von Solms (1998) argued that as companies link their computer networks to the internet, control over their systems and users and thus information security can be lost to a large extent. In addition, companies that manage personal information of individuals, find themselves increasingly confronted with the issue of privacy,

whether through legislation, industry self-regulation or customer expectations (DTT 2007). Consequently, hardening companies' defences from hackers and other unauthorised users should be a high priority for all businesses (Sherstobitoff and Bustamante 2007). Moreover, according to the Global Security Survey (DTT 2007), a layered approach to security, one that combines governance, strong perimeter protection, with other forms of access control, logging and monitoring and data protection techniques, is the right prescription for any company. Swartz (2007) also argued that monitoring user access to critical information and detecting unauthorised access to high risk data are critical steps all companies should take to better protect their sensitive information.

On the other hand, interviewee E believed that there is a gap between her company's security threats and controls because of the security budget. She stated:

> *"Yes, there is a gap because of the funding. Regarding the network security, in an ideal network design, we will segregate all our applications, firewalls, etc. Here, we have got a very flat structure, we have more than 150 sites, some of them could be small, and some sites run with only two or three people, so there is always a risk".*

This opinion is consistent with her previous opinion regarding the existence of security budget within the company. However, she emphasised the difficulty of asking for this security budget.

Interviewee E addressed the importance of having a risk register for her company to record risks, impacts, and the likelihood of the risk occurring. She remarked:

> *"There would be a record for recording the risks and impacts as well (risk register). We could put in place some ad hoc monitoring, something cheap and effective. Monitoring would be based on the potential impact and the likelihood of that risk occurring. For example, we should be monitoring the internal use of e-mail and internet, but we have a lack of resources, and no time to do that. We do it monthly now, we are just picking out a number of accounts and monitoring them. All the time people have to make risk decisions, because they never get all the money they want to spend on security".*

She stated before that her company is using a 5*5 matrix and eight steps guide for assessing and managing security risks and here she addressed the importance of having a risk register to record all risks, which indicate the importance given to the risk assessment within the company.

Moreover, she believed that her company is planning to use a new access control called 'provisioning control' in the next year. She presented the benefits of this new control as follows:

> *"There is a big control we are planning to put in, which is called provisioning. Without provisioning different system' administrators have to assign users to systems. We have got about 6000 systems, some of them are access databases, which means that different people have to put any new person on to these systems. Now with provisioning, if you have an HR system within the organisational structure, you can build on that. A particular job role will have access to certain systems. If the line managers bring somebody in, they could just authorise the individual's level of access without actually doing more than that. When somebody leaves, you can press a button and remove his access, or if somebody moves from one job to another job role, you can move the access. Provisioning can help in a lot of that. It can cut down the level of system administration work because it can automatically set up the accounts in systems. You just need one authorisation, which is in the HR, once you get that, you could control and manage access in that way. It defines not only what systems, but the level of access, then you can tie it into physical security controls, to manage who has access to the building, and make sure you get that up to date. So, I will propose to do it in kind of baby steps, it is going to make a big difference in the company".*

This opinion regarding the user provisioning is consistent with Aldhizer (2008) who indicated that the biggest problem with manual access management controls is keeping up with modifications to user access due to new assignments. It may take the help desk from one day to few weeks to change an existing employee's database access. However, automating new employee database access and subsequent modifications based on the individual's unique job responsibilities or roles with the company through user provisioning can substantially reduce security risks. In addition, the KPMG European Identity and Access Management Survey (KPMG 2008) emphasised the importance of the automated provisioning, or the role-based access control in regulating access to IT resources based on employee's role within a company. However, the survey revealed that many companies would not engage in the IAM (Identity Access Management) projects, including automated provisioning unless there was an external force driving them to do so.

To conclude, this utilities company has a structured process for maintaining their AIS security. However, they had not updated the security policy for nearly five years, and although they measure and monitor staff awareness, the security awareness level is

not high given the feedback of the security tests. Although the company has a separate security budget, the interviewee emphasised the difficulty of asking management for this budget. Although the awareness level of the security team and of some project managers regarding the British Standard BS 7799 is high, there is no general awareness of the standard. In addition, they are not certified under ISO 27001; however, they are planning to be certified. Contractors and inappropriate access are the company's most common sources of security threats, and internal fraud is the most likely threat over the next years. Most recently, the company implemented a perimeter security system for controlling the internet and for monitoring the access. Moreover, they are planning to use a new access control called 'provisioning control' in the next year.

5.10 Interview 6

5.10.1 General information

This interview was conducted in a financial services company located in London. The company was established more than 20 years ago. It was registered in the London Stock Exchange and there were approximately 3000 full-time employees in it. The company had a small information security team of three persons within the group risk management department and this team reports to the head of risk management (the interviewee). On the other hand, interviewee F was the head of risk management, who had 10 years of experience in his current position, and had a professional security qualification - Certified Information Systems Security Professionals (CISSP).

5.10.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding his company's management framework of AIS security.

AIS security policy: Interviewee F confirmed that they had a formal written security policy, which had been created nearly 10 years ago by the security manager, and was updated annually. He stated that the group risk committee, with a group of the board members and the chief executive were responsible for the policy. In addition, although, the ultimate responsibility was with the board, the board delegated this responsibility to the information security team.

He believed that they could not distribute hardcopies of the policy to a large number of employees; however, it was distributed via the company's intranet. He indicated that they are monitoring login incidents and security breaches and are reporting on this on a monthly basis to check compliance with the security policy. In addition, despite the high cost of security training and awareness, his company is checking awareness of policy through security tests and the achieved scores. He pointed out:

> *"We are using a number of indicators to check whether the policy is complied with. There is a training package on the intranet. At the end of this training, there is a policy awareness test. There are scores and employees can fail or pass the test, according to their awareness of the policy".*

Security training and awareness program: Interviewee F confirmed the existence of a formal security training and awareness program within his company, he stated:

> *"Yes, we have security training for managers, employees, and for contractors as well".*

He indicated that the training he received focused on system security, management, responsibilities and security policy. In addition, he believed that the classroom is the most effective technique for making staff aware of security issues; however, due to cost and time constraints, his company is providing employees with security awareness materials online. He expressed the following opinion:

> *"The classroom training is the most effective technique, it works better, but we cannot do it with all employees. Even with new employees, it is very difficult, we are quite busy and continuously there are new staff being brought in. There is very little classroom training for a few people e.g. people selling financial products, mortgages, etc. They must have formal classroom training, but we are unable to do that for all the company, it costs a lot, and it is time consuming".*

Interestingly, despite the wide agreement regarding online security training and awareness, interviewee F indicated that sometimes the employees complain that there is no time even for online training, given that they have many training courses covering different security issues.

Moreover, he confirmed that his company depends on the feedback on the security tests, which are conducted on an annual basis, in addition to monitoring the employees' performance to measure and monitor staff awareness. However, he revealed that the security awareness level in his company is not high. He stated:

"Everyone should go through training once a year. There is a quiz at the end of the training, and we can get the feedback based on that. We also monitor staff awareness, particularly through talking to their managers and looking at their performance. In my view, being a bank, it is reasonable to get staff more aware of confidentiality".

Risk assessment: Interviewee F stated that his company does not undertake a specific AIS risk assessment. However, there is a broad risk assessment program for all operational risks, which is undertaken on a quarterly basis. This result is not surprising, given that financial services companies are regulated by the FSA, so they have to report their security risks regularly.

He also stated that the operational risk team in his company is responsible for undertaking this risk assessment. He pointed out:

"Under the risk management team of the company, there are information security, operational risk, financial risk, fraud and insurance, and business compliance. The operational risk team is responsible for risk assessment, and are looking at balancing the operational risks of the company and the security risks, people risks, etc.".

Moreover, he believed that the overall security risk level within his company is medium to low.

Incident handling, disaster recovery and business continuity plan: Interestingly, interviewee F believed that the average number of security incidents experienced by his company between 2005 and 2007 was nearly 50 incidents per year. Although most of these incidents were minor ones, still there were major incidents. This result confirmed the questionnaire finding where the only respondent to state that his company had more than 15 incidents during the last year was from the insurance & financial services sector.

He indicated that they suffered from a minor phishing attack, which was discovered and dealt with very quickly. He commented:

"Two weeks ago we had a phishing incident, a minor one. Somebody had set up a website in the United States, copied our company's website, and tried to attract customers. Somebody in the United States discovered it and reported it to us. These people are trying through our website to get customer information and steal through this information; it is a financial fraud. We got this site shut down within 24 hours of it being discovered".

In addition, he believed that the loss or theft of customer information is the worst security incident that could happen, not only because of its direct cost, but also because of its reputation damage. He considered financial fraud to be a serious security incident given the high financial impact on his company. This opinion suggests that financial services companies that responded consider the loss of customer information as the worst security incident that could have a significant effect on their reputation, customer confidence and share price.

Interviewee F also believed that there are standard procedures based on the CERT (Computer Emergency Response Team) to deal with security incidents. He presented these procedures as follows:

> *"We have got standard procedures based on the CERT. There are six stages in this process: first notification (to know that an incident had happened); second analysis; third containment (managing what is going on); fourth investigation; fifth response, and six follow up (lessons learned)".*

Moreover, he stated that they have different authorities and regulatory bodies to whom they could report depending on the size and nature of incidents including the FSA (Financial Services Authority), ICO (Information Commissioner's Office), BBA (British Bankers Association), and the Payment Card Industry Scheme. He indicated that they report major incidents only to the FSA, while they can report to the BAA (British Bankers Association) in case of any kind of unexpected risks within the bank such as a loss of a database. In addition, they can report to the police if there is a crime.

He believed that his company is better prepared to recover from predicted incidents than from new ones. He presented the following opinion:

> *"Yes we can recover from the incidents that we can predict. We have insurance; we retain reserves, etc., so we are able to recover from any incident. Banks have to hold a level of capital as a reserve against any kind of losses. Our reserves have to be big enough to deal with major incidents. According to regulations, we have to be ready to respond to anything that can happen. As an information security team, we have practised many responses to incidents in many different sizes, and sorted how we can deal with them. If we cannot predict the incident, that is the issue. Until the first phishing attack happened, no one knows that it could happen. That is what the security is always worried about, because 'company cannot respond well to any new incident'. But we learnt a lot from the incident, and we*

respond very quickly to any incident we saw before. But every now and then, something new happens, and I think our response process can deal with any kind of incident".

He reported that his company improves the controls after a security incident. He presented the following example:

"After the phishing attack was discovered by an external party in the United States, we try to improve our security. We look at improving our monitoring capability to be able to detect the incident by ourselves. We can improve our controls to prevent future incidents".

He also stated that the facilities business continuity management team is responsible for establishing the plan and his security team is responsible for running it; however, the whole company has a plan, and a part of it is concerned with security incidents. He identified role of the facilities business continuity management team as follows:

"We've got a facilities business continuity management team. A major part of the role of this team is about building recovery. They make sure in case of any incident, there is another building available for work".

In addition, they do annual tests for the business continuity plan on different sizes and types of incidents. He commented:

"We do annual tests of different scenarios because we have to consider different sizes and types of security incidents and we do annual tests on different sites across the country".

Security budget: Interviewee F believed that there is no separate security budget within his company; however, IT spend nearly 5 percent of their budget on security activities and around 2 percent on information security, which ends up as nearly 7 percent of the IT budget. He pointed out:

"We do have a security budget for IT, but there is no single security budget. The two percentages we tend to be looking at are the percentage of the IT budget, and the percentage of the overall business budget. We are probably spending around 2 percent of the IT budget on information security, specifically my team's information security, and less than 1 percent of the whole group's budget. On the other side, in a very broad sense, the IT probably spend 5 percent of their budget in security activities in terms of systems, services, the whole things that go with security, so 5 percent of their budget is directly used in security matters. So, we are talking about a total of 7 percent of the IT budget".

On the other hand, he stated that security spending is a part of his company's annual business plan, which is drawn up based on their understanding of risks and on their

responsibilities. He believed that the financial director approves the security budget and he provided a justification in the following quotation:

> *"Our annual business plan has to be approved by the financial director and the board on an annual basis. The finance director approves the security budget, because ultimately, the IT report to finance. This is because the finance director is responsible for the risk department in general. The whole budget is the board's responsibility, while the finance director will decide the part of the information security".*

In addition, he stated that a big part of their security budget is spent on security testing such as penetration testing and staff, in addition to other IT services in which the IT brings in new security systems into the company.

He revealed that his company's security spending level is moderate or adequate but it is nearly the same compared to other companies in the same industry sector. He remarked:

> *"It is moderate and safe. We do comparisons with other banks and other organisations. We spend about the same proportion. It is the main question the finance director is always asking me: 'How much is everybody else spending?' when I ask him for money".*

This opinion supported Ross and Weill (2002) who pointed out that many executives look to industry benchmarks as a way of determining appropriate spending levels.

Moreover, interviewee F believed that the security budget would be a bit higher next year. He cited the current focus on confidentiality requirements as a justification for the increase in security spending. He ended the discussion of this issue with an interesting comment. He stated:

> *"Everybody is always arguing for the budget, to get more spending. But the most important thing is to spend the right amount on the right things".*

This opinion supported Tsiakis and Stephanides (2005) who pointed out that a key factor in getting value from security is to ensure that security investments protect the right things.

Security standards and certification: Interviewee F stated that although he is aware of the British Standard BS 7799, and it is used as the basis of their security processes, he did not believe that many average business people are aware of it. He commented:

> *"Yes I do, and we use BS 7799 as the basis of our processes to security. Regarding the other managers and employees, it is difficult to say because it is a very detailed standard. If you mention BS 7799 to any one of our staff, I think IT people, probably, could recognise what it is but I don't think many average business people are aware of it".*

On the other hand, he stated that his company is not certified under ISO 27001, given that certification is still not mandatory, and therefore there is no pressure on companies to be certified. He believed that the companies that already have it are those companies providing business-to-business services. He stated:

> *"We are not certified at the moment, we do not have current plans, but we keep an eye on it. It is not mandatory, and it costs money if the company is involved in certification. For those organisations that were certified, I am not sure it proves the benefits of certification. They have done it, but they did not show people their level of awareness. The organisations that already have it are those organisations that provide business-to-business services. They are the kind of customers who can ask for certification e.g. if we buy internet services from BT, we can get assurance from BT that they are certified under ISO 27001. Perhaps there is not quite a market for it now, except for business-to-business services. It costs a lot; it needs much time unless we have to do this kind of certification, if we have a banking code. But till now we don't have any pressure to do that".*

The above opinion supported Buzzard (1999) who indicated that compliance with the standard facilitates the inter-company trading by providing confidence in the security of shared information. In addition, Freeman (2007) argued that certification under ISO 27001 could make the company more appealing to potential customers; it could help assure business partners that a company is serious about security; however, certification is still optional.

On the other hand, interviewee F saw compatibility as a key benefit from complying with the standard. He pointed out:

> *"Yes, the biggest benefit is compatibility so that we can all have a common language for information security. When I talk to other banks or other organisations, we can talk in the same terms about security. It is very valuable and makes sense".*

AIS security effectiveness: Interviewee F indicated that his company measures security effectiveness through the risk assessment, in addition to the feedback of security tests, and through other key performance indicators within the company, which help them to see if controls are working.

In addition, he reported the number of incidents, the results of security tests, in addition to the vulnerability level as his company's most important success indicators of security management. He presented the following opinion:

> *"The number of incidents, test results, and what we find from vulnerabilities. If there are many minor incidents, it indicated that there is a problem. For example, if there are ten minor incidents such as internet misuse, e-mail misuse, etc., we look at them, and if there is a trend, it means that we have many people who don't know how to use the internet or e-mail appropriately. So we must train them to use the internet appropriately. If there are many minor incidents, this indicates that there is a problem with our security processes".*

On the other hand, he highlighted the lack of management support, awareness and commitment as his company's top obstacles of effective security. He stated:

> *"Quite often security takes a secondary role. Management prefer to do a lot of business, do it quickly and effectively at a low cost, and worry about security after that. It is a very common problem, because it is not the core requirements of management to do that. The top obstacle to effective security is the lack of management support, and awareness, and it is more about management commitment. They are quite happy to do things about security particularly if an incident happened, but they cannot plan security in their basic thinking, when they are doing business work".*

This opinion is consistent with Kwok and Longley (1999) who indicated that one of the problems commonly faced by security officers is the lack of full commitment from senior management. Smith and Jamieson (2006) also argued that management awareness is the top issue identified as an inhibitor to successful IS security processes. Moreover, Knapp *et al.* (2006) stated that gaining top management support is the most critical issue of an information security program.

Moreover, he believed that his bank's AIS security management is quite effective given that the security awareness level is very high. He commented:

> *"It is quite effective because we have got pretty wide security awareness in the company. Many managers know about our team. Everyone knows what is good and bad and what is*

right and wrong. We have got a good reputation; we have a lot of power in terms of our ability to stop things happening, etc.".

5.10.3 AIS security threats

Interviewee F believed that the complexity of IS and the sharing of information with an unlimited number of other companies are his company's most serious threats. He expressed his opinion as follows:

"I think it is something to do with the complexity of IS. There are many interactions between our IS and other companies' IS. There are many information flows out now, they are rapid, sometimes hidden, and sometimes difficult to monitor. I think that is a big challenge to the information security. Every day we share information with lots of different organisations for good business reasons. We need to think harder about the processes needed to control that. It is always happening. It is a day-to-day fact".

This opinion supported Barnard and Von Solms (1998) who indicated that threats are growing because of the high levels of interconnectivity both within and between organisations. Cavusoglu *et al.* (2004) also stated that the increased interconnectivity among computers enabled by the internet raised the scale and scope of information-related crimes. In addition, Schneier (2001) argued that companies now have no choice but to connect their networks to the rest of the world i.e. to link with customers, suppliers, partners, and their own employees. However, with this interconnectivity come new threats such as hackers and criminals. Moreover, Gansler and Lucyshyn (2005) pointed out that the complexity of IS is growing faster than our ability to understand their vulnerabilities and to protect them. Managers are now discovering that sharing information with other companies increases the risk that critical data will be misused (Aldhizer 2008).

On the other hand, interviewee F believed that financial fraud such as phishing and spamming attacks, and data leakage are the most frequent threats facing his company. Trites and Lavigne (2006) argued that identity theft and phishing attacks are growing threats. They also stated that many companies simply have not implemented adequate controls for e-mail messages; leaving e-mail management to the preferences of their employees, which is an inadequate approach, given the growing volume of spamming attacks. In addition, according to the Financial Crime Sector Report (FSA 2004), phishing attacks are increasing and are growing to include the smaller banks as well

as the major ones. Moreover, the Global Security Survey (DTT 2007) addressed the problem of data leakage and indicated that 14 percent of internal breaches of companies were due to theft or leakage of intellectual property. In addition, the Annual Global Security Survey (Greenemeier 2006) stated that data leakage and theft breaches are on the rise. Data is the central commodity for attackers who want to commit fraud or profit from identity theft.

Moreover, he reported that there are external and internal sources of security threats facing his company, in terms of criminals, customers, and staff. He commented:

> *"It is a combination, the source of external threat is criminals, sometimes organised, sometimes not. Sometimes customers deal with dangerous things. Sometimes it is manifested inside e.g. staff may misbehave either because they are not being careful or because they act as criminals. Staff is a part of our internal risk; sometimes they cooperate with somebody else outside the organisation to steal some money (financial fraud)".*

This opinion supported Hitchings (1995) who indicated that most computer-related fraud has been undertaken by companies' trusted employees, sometimes colluding with others. In terms of customers, Damiano (2008) argued that, despite banks' best efforts to improve security, their defences are only as strong as their customers' security habits. Unfortunately, even though customers recognise their role in keeping their sensitive information safe, they often do not take the necessary precautions.

On the other hand, he cited the theft or loss of customer data as his company's most likely security threat over the next few years. In addition, his company would be concerned with customers' awareness. He stated:

> *"I think the loss or theft of customer information, and the way by which customers themselves behave. We are increasingly worried about customers and how they are able to protect themselves from different kinds of threats. Customers are not very aware. Even those who are aware may not understand the technology very well. They can send e-mails with personal data in them, which is not protected, they do not encrypt data, and they do not know how to use technology very well. Because the internet technology is too mature, it is a big problem for us, and for all other industries as well, it is a big threat".*

Gansler and Lycyshyn (2005) indicated that the internet continues to grow rapidly and has evolved into a system of systems that is complex, lacking clear boundaries and control. Beard and Wen (2007) also argued that the use of the internet technologies

has substantially increased the vulnerability of IS. One of the fastest growing threats on the internet is the theft or leakage of sensitive financial information. Given the increasing number of incidents related to loss or theft of customer information, it is not surprising that the company will be concerned about this threat in the following years.

5.10.4 AIS security controls

Interviewee F stated that, most recently, they employed many technical controls such as client security packages, firewalls, and virus protection tools. However, he believed that given the complexity of systems, his company has a big gap in the monitoring controls. He remarked:

> *"I think the biggest gap is 'to monitor'. We do not have technology to monitor everything. We have many systems operating very fast and we have many information flows. The complexity of systems is one of our long-term big focus areas; we need to improve our abilities. We need to monitor all information flows, access to systems, external access to the internet, etc. We spend a lot of time and effort currently on intrusion detection and prevention systems".*

This opinion is consistent with a previous opinion in Section 5.10.3 in which he indicated that the complexity of IS and the sharing of information with an unlimited number of other companies are his company's most serious security threats. Steele and Wargo (2007) argued that given the technological advancements, companies must have monitoring tools to track and monitor data and insider activities. Moreover, interviewee F stated that the security level within his company would be better the following year given the nature of the banking market that is always challenging.

To conclude, this financial services company has a structured process for maintaining their AIS security. However, they do not undertake a specific AIS risk assessment; there is a broad risk assessment program for all operational risks. The average number of security incidents experienced by the company between 2005 and 2007 was nearly 50 incidents per year; however, there are standard procedures based on the CERT (Computer Emergency Response Team) to deal with these incidents. There is no separate security budget within the company, and although the interviewee is aware of the British Standard BS 7799, and it is used as the basis of their security processes, he did not believe that many average business people are aware of it. The company is not

certified under ISO 27001, given that certification is still not mandatory; however, compatibility is the key benefit from complying with the standard. The complexity of IS and the sharing of information with an unlimited number of other companies are the company's most serious threats. In addition, financial fraud such as phishing and spamming attacks, and data leakage are the most frequent threats. Most recently, they employed many technical controls such as client security packages, firewalls, and virus protection tools. However, given the complexity of systems, the company has a big gap in the monitoring controls.

5.11 Interview 7

5.11.1 General information

This interview was conducted in an entertainment company located in Maidenhead. The company was established more than 20 years ago. It was registered in the London Stock Exchange and there were approximately 6500 employees in it. The company had a security department, not specific for information security, including 30 employees and reporting to the head of security. On the other hand, interviewee G was the chief technology officer, who had one year of experience in his current position.

5.11.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding the management framework of AIS security within his company.

AIS security policy: Interviewee G confirmed that they had a formal written security policy, which had been created nearly five years ago by the IT department; however, he believed that his company had never updated this policy.

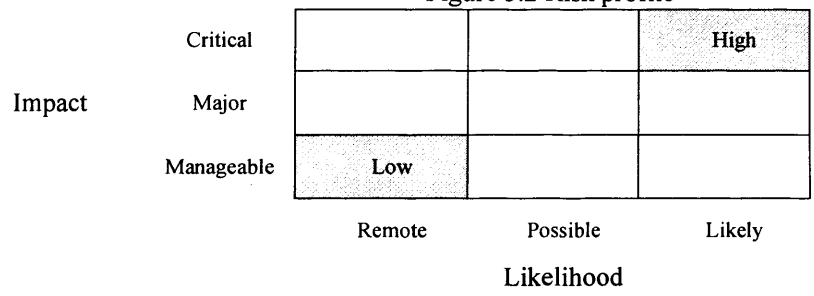
Regarding the distribution of the policy, he stated that in their induction, employees were given either a hardcopy of the policy or the information security booklet, or they had to sign some information security forms. In addition, he believed that the use of "passwords" was considered the most important element of their security policy.

Moreover, he claimed that his company checks employees' compliance with the policy, and it is a line management function. He believed that his company's security policy is effective.

Security training and awareness program: Interviewee F confirmed the non-existence of a security training and awareness program within his company. He believed that in their induction, employees had to read and sign some information security forms. In addition, despite the importance of measuring staff security awareness, they are not undertaking regular testing of security awareness within the company. Consequently, his opinions suggest that his company needs to devote more effort to training their staff and in making them security aware.

Risk assessment: Interviewee G confirmed that his company is undertaking security risk assessment once a year with the help of third parties such as external auditors, experts, and consultants e.g. Ernst & Young. He stated that, as the chief technology officer within the company, he is responsible for the risk assessment, with the help of some external consultants. He illustrated the risk assessment matrix used in assessing their risks in Figure 5.2.

Figure 5.2 Risk profile



(Source: A report was given to the researcher during the interview)

Incident handling, disaster recovery and business continuity plan: Interviewee G believed that his company had experienced some minor security incidents in the last two years. He considered hacking into their random number generators is their worst incident.

Moreover, he believed that the security department is responsible for the incident handling procedures. After a security incident, they have to arrange a proper team,

assess the impact, think about mitigations, communications, further threats, and react accordingly. He indicated that security incidents within his company are reported to the Gambling Commission.

In addition, the business continuity plan within the company is the responsibility of the head of the security department and it is updated annually.

Security budget: Interviewee G believed that his company has a separate security budget. This could be because the company has a security department including 30 employees, and consequently, there is a separate security budget for this department. He stated that, as the chief technology officer within the company, he approves the security budget. He believed that they spend the main part of their security budget on network security, intrusion detection tools, and firewalls. He believed that security spending within his company is enough and there is no need for more budget.

Security standards and certification: Interviewee G stated that although he is aware of the British Standard BS 7799, there is no general awareness of the standard among the employees and the other managers, and he could not find any benefit from complying with this standard. In addition, he believed that they are not certified under ISO 27001 and have no plans of certification.

AIS security effectiveness: Interviewee G indicated that his company is measuring AIS security effectiveness. However, he believed that the non-occurrence of security incidents is the most important success indicator of security management within his company. He claimed that employees are his company's main obstacle of effective security.

5.11.3 AIS security threats

Interviewee G addressed the problem of mobile devices such as USB sticks as his company's most serious threat. O' Hanley (2004) argued that handheld devices, which hold vital data, lack security controls and are more easily lost by their owners. In addition, removable media devices such as MP3 players, USB data sticks, and portable hard discs enable staff to extract large quantities of confidential data onto insecure and easily stolen media (BERR 2008).

He cited people as the company's most frequent and most common source of security threat. Moreover, employees are his company's biggest threat over the next few years.

5.11.4 AIS security controls

Interviewee G indicated that, most recently, his company had improved their firewalls. He believed that the company's security controls are enough, and therefore, no gaps exist between security threats and security controls used. However, he emphasised the importance of employing more security controls to protect laptops and data they contained.

To conclude, this entertainment company has no framework for managing their AIS security. The company had never updated the security policy, there is no security training and awareness program within the company, there is no general awareness of the British Standard BS 7799 among the employees and the other managers, and they could not find any benefit from complying with the standard. In addition, they are not certified under ISO 27001 and have no plans of certification. The problem of mobile devices such as USB sticks is the company's most serious threat, and employees are the biggest threat over the next few years. Most recently, the company had improved the firewalls, and the interviewee emphasised the importance of employing more security controls to protect laptops and data they contained.

5.12 Interview 8

5.12.1 General information

This interview was conducted in a utilities company located in Bradford. The company was established more than 20 years ago. It was registered in the London Stock Exchange and there were approximately 2200 employees in it. The company had a security department including four employees reporting to the operations department. On the other hand, interviewee H was the IT architecture manager, who had six years of experience in his current position in the IT department within the company.

5.12.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding his company's management framework of AIS security.

AIS security policy: Interviewee H believed there is a whole policy within his company which security is part of. This policy had been created eight years ago by the security manager and was updated every four years.

In their induction, employees were given either a hardcopy of the policy or the information security booklet, or they had to sign their contract and the security policy is part of it. However, the current employees could find the policy via the intranet or the internal website of the company.

Moreover, interviewee H cited the user responsibility or accountability - employees and outsiders - as the most important element of the security policy. He stated:

> *"The most important part of the security policy is about user responsibility - employees and outsiders. People who get access to our data must be responsible for this data and must protect it; otherwise there will be a problem".*

He believed that the audit department is running auditing activities on a yearly basis and are checking authorisations to check compliance with the policy.

Security training and awareness program: Interviewee H indicated that there is no formal security training within his company; however, it is part of the induction of new employees. In addition, every team gets together on a monthly basis and discusses different security issues. His company also depends on the intranet in providing employees with important security issues to increase their awareness.

Risk assessment: Interviewee H confirmed that his company is undertaking security risk assessment every six months with the help of third parties such as external auditors and assessors, and they use a matrix in assessing their risks. He commented:

> *"We have a matrix. ISO 27001 mandates that we have to record all our IT security risks. We record all risks and we have a matrix that illustrates the likelihood of a risk occurring, the likelihood of that causing a failure, against the impact of the failure. For every risk we get in the register, we understand those aspects, we put scores and we prioritize".*

Incident handling, disaster recovery and business continuity plan: Interviewee H believed that his company experienced two major security incidents, in which a storage network failed, which caused a major loss of service or downtime, and a lot of

minor incidents. Although the downtime remained for only one day, he believed that it was a major problem or a disaster for his company. He stated that any downtime in systems that run all company's operations is a major incident. He presented the following opinion:

> *"We had 2 incidents in which one of our storage networks failed. It is a technical downtime. We have a service manager who is responsible to bring the service back again, through back-ups, but there is no one to blame for this. We have quite good technical security. I cannot give an exact figure for the cost of these incidents, however, costs are not only financial, there are sometimes reputation costs as well".*

Moreover, he believed that embezzlement or fraud, and loss of customer data are the worst incidents that could happen in his company.

On the other hand, interviewee H stated that different departments are responsible for the security incident handling procedures, depending on the incident, such as legal department, physical security, and IT service management. After an incident, they have to arrange a team, discuss what is happening, end up with facts, and then decide what to do. This team has to meet on a regular basis to monitor the progress regarding the incident. He also believed that they are regulated by certain authorities such as the DWI (Drinking Water Inspectorate) and the EA (Environment Agency); however, they report specific incidents, not all incidents.

Interviewee H stated that there is a business continuity plan within his company, which is constantly updated by the disaster recovery staff to reflect new events and new changes.

Security budget: Interviewee H believed that they have a budget specifically for security; however, he remarked:

> *"It is part of the IT budget, but it is specifically for security. In terms of the overall company security, which is physical security and IT security, IT spend around 75 percent of the whole budget. In terms of IT budget, probably it is about 2.5 to 5 percent of IT budget spent on security".*

He stated that the security spending decision within his company is a part of the normal business planning cycle, and the approval of the budget is shared between a

number of people such as team managers, the IT architecture manager, etc. and ultimately the director signs it. He also stated that his company spends a lot of money on authorisations and on access controls and he believed that the security budget would be a bit higher next year.

Security standards and certification: Interviewee H stated that the overall awareness level of the British Standard BS 7799 is not high among managers and employees. On the other hand, his company was certified under ISO 27001, which confirmed the results shown in Table 4.53 (Chapter 4). He believed that they were only certified to prove to one of their clients that they take security seriously and that their security controls are adequate. However, he could not see more benefits from being certified. Interviewee H remarked:

> *"We do work with the Ministry of Defence, so we have to prove that our security is adequate. BS 7799 and ISO 27001 only help us doing that, they support us, this is the only reason we got it. But I can't see any more benefits. ISO 27001 is so vague and wide, you could do what you want with it. With ISO 27001, you specify the scope of measures, and you can tell them exactly which parts of your company are relevant and say 'these measures or controls are secure'. The only thing you have to do is that you prove you do it. It doesn't add anything technically to the play. But if you do all what it says: you must record all procedures and must do risk management, that is good. However, it is not mandated in the UK. I don't think it brings a great deal to the company".*

Siponen (2006) argued that the standard is more concerned with ensuring certain security activities exist in companies, and is less interested in how well they are done or how these security processes can be accomplished in practice. However, the BERR Information Security Breaches Survey (BERR 2008) pointed out that all companies that have implemented the standards have achieved benefits from doing so.

Moreover, interviewee H believed that although there is no benefit from certification it is useful to have the standard in place. Thorp (2004) argued that human beings naturally work more efficiently in a structured framework, and this can be through following a certain standard like BS 7799.

AIS security effectiveness: Interviewee H cited the number of security incidents, in addition to penetration testing as the techniques used to measure security effectiveness within his company. He commented:

"We do a couple of things. Technically, we do like penetration testing, so we get people to enter or hack our system. On a more managerial level, we review how many incidents we have".

On the other hand, he believed that employees' awareness, compliance and commitment to polices, and number of incidents are the most important success indicators of security management. He stated:

"It is probably things around compliance and audit. This is something to do with not having incidents, and awareness and commitment to policies through staff testing. If we want to test how successful we are, we could ask people, what do you know about this?, what makes you do this and do not do that?, etc.".

He also believed that the effectiveness level of security management within his company is reasonable, but it could be much better.

5.12.3 AIS security threats

Interviewee H stated that internal people extracting inappropriate data and doing wrong things are his company's biggest threat. This opinion supported Whitman and Mattord (2003) who argued that not everyone wishes deliberately to violate the security of business information. Employees may mistakenly capture data incorrectly, delete sensitive information or negligently leave information vulnerable for unauthorised users to gain access to it.

Interviewee H also believed that downtime and people getting too much access are his company's most frequently faced threats. This opinion is consistent with a previous opinion in Section 5.12.2 where he stated that his company experienced two major security incidents; namely loss of service or downtime. He believed that, although the downtime remained for only one day, it was a disaster for his company. Mattsson (2007) argued that many abuses and accidents occur because people have access to data that they do not need to see. The Global Security Survey (DTT 2005) indicated that employees in many instances have unlimited access to customer data which can increase the release of such data.

He believed that staff having more than one job role are his company's common source of security threats. Interviewee H commented:

"Staff is the threat, people having more than one job role. There is less staff, so every role is making more jobs. In terms of IT, if you ask an internet person about the constant attacks, he will be saying spam e-mails, etc. These things are going on continuously. But I cannot see them as a big threat compared to the other threats".

Davis (1997) pointed out that the lack of segregation of duties increases the potential for unauthorised changes to computer programs and data going undetected.

Moreover, interviewee H believed that mobility is his company's major threat over the next few years. He remarked:

"From an IT point of view, we have to be more protective, we have to protect equipments such as mobiles, WiFi, laptops, etc. I think mobility is the biggest threat, so that we can be losing control over data".

The KPMG Information Security Survey (KPMG 2006) indicated that the growing use of mobile devices such as mobile phones and memory sticks demands companies' attention. Companies face the challenge of achieving and maintaining an adequate level of security over these devices. Aldhizer (2008) also argued that mobile devices may not only enhance data availability, but may also increase the threat that trusted insiders could steal confidential information, customer and employee data, and financial information.

5.12.4 AIS security controls

Interviewee H stated that, most recently, his company created a DVD to raise employees' security awareness and implemented more access controls on their accounting systems as well. This is encouraging given the wide agreement in the literature regarding the importance of the human factor in security. Wood (1995) argued that no matter how sophisticated the security technology is, controls will not be sustainable unless human element has been adequately addressed. Too many people look at information security as strictly a technological problem, when in reality it is both a technological and human problem. Schneier (2001) stated that human minds are the attackers, so they need to be the defenders as well. Moreover, Beznosov and Beznosova (2007, p.421) stated, "People who think their security problem can be solved with only technology, do not understand the problem and do not understand the technology".

On the other hand, interviewee H believed that given that there is too much external access to a company's systems, they cannot have total control on this access and therefore a gap exists between their threats and controls. He commented:

> *"Yes, I think because more external people are using our system, that is more risky, so we do not have direct control over them. I think technically we are getting to the point where we know we have weaknesses that we need to address".*

Von Solms (1998) indicated that as companies link their computer networks to the internet and to their business partners' networks, control over their systems and users, and thus information security can be lost.

Interviewee H cited the importance of having single authorisation within his company in an attempt to avoid the problems of using several passwords. He commented:

> *"It will be good to get a single authorisation. I think that would help because employees cannot remember all these passwords and they have to write them down which is something wrong. If people have only one password to remember, probably they will take more care of it, so it will be more secure".*

The BERR Information Security Breaches Survey (BERR 2008) indicated that UK companies still depend on user IDs and passwords to check the identity of users attempting to access their systems. Gerard *et al.* (2004) argued that although passwords are the oldest line of defence, they still constitute the most effective method of controlling access. However, there have been too many security breaches driven by simple human error, particularly the sharing of the employees' passwords. The questionnaire findings (Table 4.78 in Chapter 4) revealed the seriousness of this threat given that 72.9 percent of companies believed that their employees are sharing passwords, which highlighted the frequent occurrence of this threat in the companies that responded.

Moreover, interviewee H believed that his company is not planning to use biometrics, given that they are difficult to control. Dimitriadis (2004) argued that designing and deploying security architectures that incorporate biometrics is not an easy task. Joyce (2008) also indicated that biometrics pose new challenges and risks. The challenges faced by companies in implementing biometrics are cost and reliability. Moreover, the storage of biometric data is a digital representation of the user's identity that can be

stolen or lost, and therefore the misuse of biometric data is a serious issue given that biometric information cannot be changed after it is created. Once a user's information falls into the wrong hands, the user could be a victim for life. In addition, the company is not planning to use patch management. Patch and vulnerability management tools can take on scanning, detecting, assessing and protecting vulnerable systems (Messmer 2008). He commented:

> *"What we don't have is the patch management. It is a typical security control, but we find it disruptive. We like to keep a very open view of all sorts of controls. There are things we do not do, but we keep watching them to see what we want to do".*

To conclude, this utilities company has a structured process for maintaining their AIS security. However, there is no formal security training within the company. The overall awareness level of the British Standard BS 7799 is not high among managers and employees. They are certified under ISO 27001 to prove to one of their clients that they take security seriously; however, they could not see more benefits from being certified. On the other hand, internal people extracting inappropriate data and doing wrong things are the company's biggest threat; downtime and people getting too much access are the most frequently faced threats, whereas, staff having more than one job role are the company's common source of security threats. Most recently, they created a DVD to raise employees' security awareness and implemented more access controls on their accounting systems as well. There is too much external access to the company's systems, they cannot have total control on this access and therefore a gap exists between their threats and controls. They emphasised the importance of having single authorisation in an attempt to avoid the problems of using several passwords.

5.13 Interview 9

5.13.1 General information

The ninth interview was conducted in a technology company located in Reading. The company was established more than 20 years ago. It was registered in the London Stock Exchange and it had approximately 20000 employees worldwide in most of Europe and India. The company had an information security team of five persons, which was included in the IT department within the company and reported directly to CIO via the interviewee. On the other hand, interviewee I was an information risk & security

manager, who had five years of experience in his current position within the company. The interviewee had a professional security qualification - Certified Information Systems Security Professionals (CISSP). In addition, he attended training sessions that were mainly focused on trends in security. He presented the important topics in the training he received as follows:

> *"My training is mostly on trends in security, how to manage things as opposed to technical security. I went to training sessions and seminars covering specific subjects, I am really looking at trends. My training is more about how people are trying to penetrate the company and steal data. Data leakage is always a big problem; the more you give people capabilities on having data on a PC".*

5.13.2 The management framework of AIS security

Section 3 of the interview guide (Appendix 2) sought the interviewee's opinions regarding his company's management framework of AIS security.

AIS security policy: Interviewee I confirmed that they had a formal written security policy, which had been created nearly 10 years ago and was updated annually. He stated that he was responsible for establishing the policy; however, the ultimate responsibility for approving and signing the policy was with the executive board.

He believed that they could not distribute hardcopies to a large number of employees. Consequently, new employees were given a CD with PDF files that they had to read and then sign if accepted. In addition, all the employees could find parts of the policy on the notice board and via the intranet.

He cited the user responsibility as the most important element of their security policy. He expressed its importance as follows:

> *"I supposed that information security is everybody's responsibility. It does not matter what job you are doing in the company. At some point, information security will be relevant to you and therefore it is everybody's responsibility".*

Hinde (1998) indicated that it does not matter how brilliant a policy is, without the active commitment of employees and management it will fail. Interviewee I had the same opinion and stated:

"Without compliance the security policy could not work. I can write a policy, but I must enforce it, otherwise it will be of little value, worthless".

He also claimed that they have a clear desk policy where they go around and monitor how people are doing in order to check people's awareness.

Moreover, he believed that the overall effectiveness of the policy is high. He indicated that they are checking people's e-mail and internet access, they are running anti-virus software, they have two audit teams checking to see if people are doing what they should not be doing, and external auditors come every six months and conduct the audit against the ISO 27001 standard. Consequently, he believed that the security policy is effective.

Security training and awareness program: Interviewee I confirmed that there is no formal security training within the company; however, it is part of the induction of new employees. In addition, every team gets together on a monthly basis and discusses different security issues. He also confirmed that the company put some articles on the intranet covering different security aspects such as phishing attacks, identity theft, and data loss to make employees security aware. He believed that the most effective technique for making staff security aware is the intranet. He stated:

"The most effective technique is via the intranet. It is the only way to get the majority of people, because people may be working from company offices, from home, from a client office, travelling around, etc. People are spread and most of them have laptops, so it is the most effective way of doing it. We can spend a lot of money, we can send out a CD to everybody, but we can get no feedback. There is no guarantee that they read it".

However, his company is not measuring or monitoring staff awareness. He expressed the difficulty of measuring staff awareness as follows:

"In the UK, it is difficult to measure staff awareness. It is not about the number of employees, it is about how spread out the employees are, and from where they are working".

He believed that the awareness level could be better if there was a sufficient budget for security. He pointed out:

"It is satisfactory, not more than that. We have a lot we want to do, but probably there is no budget. We can have wonderful systems for training and awareness, but they are expensive. If there is a legal or industry requirement, we must have this in place".

Risk assessment: Interviewee I confirmed that his company is undertaking security risk assessment every six months. However, he believed that risk assessment must be undertaken on a continuous basis. He stated:

"Risk assessment should be done every 6 months, but people should be assessing risks all the time. Because new projects come up, so people will report on their risks".

He emphasised the importance of risk assessment in the following quotation:

"We have a risk assessment program driven from the top. The executive board is doing the risk assessment, and each department should have its risk assessment processes. They should demonstrate that they are assessing risks. The board is doing high level risk assessment. They are doing a sort of Turnbull Report[8]. After Enron, the company has to report the business risks they have, so that shareholders can be aware, so that there will be no hidden risks. The board gathers all major risks of the departments and makes a Turnbull Report".

In addition, he stated that risk assessment is the responsibility of every team or department in the company. He commented:

"Every team in the company should have their own risk databases and should demonstrate that they are assessing the risks. I have a responsibility within the IT department, and look after IT risk database. We also do some risk assessment training so that people can understand why we do it, how we do it, etc.".

Incident handling, disaster recovery and business continuity plan: The results showed that the company had had only two minor security incidents in the last two years, which they contained before any damage was caused. Interviewee I stated:

"There are 2 incidents, one is the theft or loss of personal laptops, and the other is a virus attack, but on individuals' laptops. We know that we have people who occasionally bring their laptops in, connect them when they should not do that. However, they contained the incidents, they do not affect anybody else, and so they were minor ones".

[8] The Turnbull Report refers to the Internal Control: Guidance for Directors on the Combined Code. It was published by the Institute of Chartered Accountants in England and Wales in September 1999 to provide guidance to assist listed companies to implement the requirements in the Code of the Committee on Corporate Governance relating to internal control.

He believed that the loss of sensitive client data and a complete virus or malware attack that shuts down the system would be the worst incidents. He pointed out:

> *"The worst security incident would be either a virus or malware that shuts down absolutely everything, from the IT point of view, or the loss of client data. If we would be responsible for losing sensitive client data that probably would be the worst incident".*

He indicated that, as the security risk manager, he is responsible for security incident handling procedures within his company, which come through the help desk and are found on the intranet as well. He also stated that after a security incident, the incident has to be reported, then information about it has to be collected and recorded, and lessons have to be learned. He remarked:

> *"It needs to be reported. We need to find out why it happened and whether it has affected us and the clients, or the clients. We need to understand which data and systems have been affected, whether people are at risk, etc. We need to record the information about each incident, so that we can have history to look back on. We need to see the trends, which is very important and to learn from the incident as well".*

On the other hand, he confirmed the questionnaire finding and emphasised the importance of raising employees' security awareness after any security incident. He expressed the following opinion:

> *"One of the things we do is to review the risks linked to the incident. It is also necessary to advise our staff. If many laptops had been stolen, we will need to communicate that to the clients, users and employees to raise their awareness. In my opinion, if an incident happened, we can address the incident, look to why the incident occurs, and address the issues that lead to it, but I don't think this requires reviewing the policy".*

Moreover, interviewee I believed that although his company is reasonably prepared to recover from a serious incident, given that they have back-ups, disaster recovery sites, etc., there is no guarantee that everything will be absolutely recovered.

Security budget: Interviewee I believed that they have a budget for security; however, this budget is about 5 percent of the IT budget. He pointed out that security spending includes ongoing elements such as anti-virus software, e-mail security and other new elements developed by the information and security manager and his team, and is ultimately approved by the CIO and the CFO within the company.

Furthermore, he cited e-mail and internet security controls, and firewalls as their top areas of spending. This is consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that preventing outages is most important in technology companies given that they depend heavily on system availability.

He also believed that the overall security spending level within his company is not enough and the budget needs to increase. However, he cannot predict next year's budget.

Security standards and certification: Interviewee I stated that the overall awareness level of his company's managers and employees regarding the British Standard BS 7799 is high. This could be because his company has 27001 certification (Table 4.53 in Chapter 4). He believed that compliance with the standard provides a framework or guidance to the company to ensure that it is looking seriously for all areas of security, and it gives security assurance to clients. He remarked:

> *"It provides a framework to guide us to ensure that we are looking and thinking of all security areas. It is also good to demonstrate to our clients that we take information security seriously. It costs money to get and keep it going. We use it, we feel we are aware, we use it in the same way we used ISO 9001[9]. The clients need to be happy that we demonstrate that we actually focus on security".*

This opinion supported Thorp (2004) who argued that this standard provides a good guidance and a framework within which to build an information security system. Myler and Broadbent (2006) also pointed out that the standard provides a framework to establish risk assessment methods, polices, controls, and countermeasures.

AIS security effectiveness: Interviewee I confirmed the use of internal and external audits to evaluate security effectiveness within the company. He commented:

> *"We audit, and we are audited by our external auditors and by our clients' auditors as well. Some of our clients have a risk and compliance manager and their responsibility is to produce reports for the clients".*

[9] ISO 9001 (2000) is the Quality Management Systems – Requirements. This standard specifies the requirements for a quality management system (ISO 2000).

He also emphasised people awareness and number of security incidents such as virus and spam, as his company's success indicators of security management. He commented:

> *"The most important one is 'the people know about information security management'; to know we have got a security team, where to go to report incidents, etc. Also the indicators include the low level of virus problems, low level of spam, low level of security incidents".*

On the other hand, he believed that the lack of support, awareness and commitment of senior management is the top obstacle of effective security within the company.

5.13.3 AIS security threats

Interviewee I believed that the loss of clients' data is the most serious security threat facing the company given that it could damage its integrity. He also believed that loss of data, particularly data on portable laptops and memory sticks, is his company's most frequent threat. Lin (2006) argued that besides being expensive, laptops often contain corporate data, access codes to company networks and sensitive information. Zambroski (2006) also stated that laptops could be lost or sold with financial and personal data remaining on the hard drive. In addition, O'Hanley (2004) indicated that handheld devices still lack adequate security controls and are more easily lost by their owners. Moreover, Scott (2008) argued that with all the worry about phishers and thieves, the biggest problem in keeping data safe is still laptops left in cars and other locations by employees. The biggest issue now for government agencies and private companies is how to maintain the security of their laptops. For example, Skipton Financial Services (SFS) has breached the Data Protection Act after an unencrypted laptop containing 14000 customer records was stolen from one of its contractors. The Information Commissioner's Office (ICO) believed the company should have had encryption in place to limit the damage (Anonymous 2008 c). Consequently, the UK government has banned laptops leaving government buildings unless their contents are encrypted (Golden 2008).

In addition, interviewee I cited employees as the most common security threat within his company, and the theft or loss of customer data as the company's most likely security threat over the next few years.

5.13.4 AIS security controls

Interviewee I stated that recently his company reviewed the remote access controls in place. He commented:

> *"We did a thorough review of remote access that has taken place in the company i.e. everybody who connects in from outside the company, working from home, from other offices, etc.".*

This opinion supported Healey (2008) who stated that remote employees are their companies' biggest threat, among all users. In addition, this opinion is consistent with the BERR Information Security Breaches Survey (BERR 2008) which indicated that UK companies open their systems to access from outside their physical network boundaries, which opens up their core networks to unauthorised outsiders. The survey also indicated that technology companies are most likely to have additional security over their remote access.

Furthermore, interviewee I identified data encryption as the gap between his company's security threats and controls. He stated:

> *"Yes, encryption of data is a gap. I don't think we protect our data enough. We need to protect the data, so that if a laptop is lost, the data in it are useless to anybody".*

Golden (2008) pointed out that the use of laptops, often by mobile workers has generated many of the companies' most serious security threats. Laptops have always been easy to steal and easy to lose. Today, however, the implications are much greater because they generally store much more data than before. Consequently, the volume of potential information loss has significantly increased. Moreover, given the endless incidents of the loss of laptops containing sensitive data, the UK government has banned laptops leaving government buildings unless the contents are encrypted. Moulds (2008) indicated that encryption is a mechanism to add a tighter layer of access control. By encrypting sensitive data within an application or storage environment, a user wishing to read information not only has to have rights to access the data but must also have the ability to decrypt that data.

Moreover, interviewee I cited data encryption, protection of sensitive databases, and restricting users' access to data and systems as the most important security controls. He stated:

> *"Encryption of data and better security on sensitive database. Sometimes people have too much access to these data, as a part of their job, they need it, but we must not allow too much access, we allow them only what they require for getting their work done. Someone will need to take a copy of the whole database, he may need it, but I need to know about it, and I have to query him and ask why he took a copy of it".*

This opinion supported Swartz (2007) who argued that many companies give employees too much access. However, it is better to give insiders as much access as they need to do their jobs, but no more. Consequently, monitoring user access to critical information and detecting any unauthorised access are critical steps all companies should take to protect their information adequately. This opinion also supported the 'need to know principle' mentioned by Ward and Smith (2002) who suggested the necessity to provide access to systems and information based on employees' defined role within the company.

On the other hand, interviewee I believed that the security level within his company would be the same next year given that his company was not planning to put any new controls in place.

To conclude, this technology company has a framework for managing their AIS security. However, there is no formal security training within the company, and they are not measuring or monitoring staff awareness. The interviewee believed that the awareness level could be better if there was a sufficient budget for security. The overall awareness level of the managers and employees regarding the British Standard BS 7799 is high. This could be because the company has 27001 certification. The loss of clients' data, particularly data on portable laptops and memory sticks, is the most serious security threat and the most frequent threat facing the company given that it could damage its integrity. On the other hand, most recently the company reviewed the remote access controls in place; however, data encryption was identified as the gap between the company's security threats and controls.

5.14 Summary of the chapter

This chapter began by presenting the selection of interviewees, how they were contacted, and the date, time and duration of each interview. It proceeded with discussing the approach used in analysing interview data, and how the qualitative data analysis software (NVivo) was used to support Miles and Huberman's approach in the current study. The profile of the interviewees and the main characteristics of their companies were then discussed.

The chapter then presented the main findings of each of the nine interviews, together with the interviewees' opinions concerning the elements of their companies' AIS security management framework, the most common sources, types, and most frequent security threats facing their companies, and the different types of security controls implemented in their companies to reduce security threats.

A security policy is a wide ranging document for managing the business as a whole, managing it securely and protecting its information (Woodward 2000). Interviewees' opinions confirmed the questionnaire findings regarding the existence and frequency of updating their security policy. The results showed that a security policy now exists in the majority of the companies responded regardless of the industry sector, and the majority are updating it every year. The results also showed that the ultimate responsibility of the policy is now with the management or board of directors, who delegate some responsibilities to other departments such as security department, risk assurance department, and IT department. In addition, companies' intranet is now the most common cost effective means of distributing their security policy among employees.

Whitman (2003) indicated that the awareness programs seek to keep security on the minds of employees as they deal with vital information on a daily basis. Interviewees' opinions confirmed the questionnaire findings regarding security training and awareness programs. The results indicated that although some sectors are taking steps to provide their employees with security training and to raise their security awareness for instance the insurance & financial services sector, there is still much to be done in the companies in this respect. The results also suggest that despite the non-existence of a formal security training program in the majority of companies, there is wide

agreement of the importance of security training for new employees, which is a part of their induction program. Moreover, the companies responded find it more practical and cost-effective to do security training and awareness online, via the intranet or through publishing some articles covering different security issues on their web page. The results are consistent with the study undertaken by the European Network and Information Security Agency (Enisa 2007) in which companies believed that the benefits of the computer-based training and awareness include cost effectiveness, consistency of delivery, and the ability to measure the results.

Regarding risk assessment, the results are encouraging given that all interviewees believed that their companies are undertaking a security risk assessment, not only for their IS or AIS, but for the company as a whole. In addition, the majority of companies responded now have a certain manager or team, specifically, for undertaking risk assessment tasks and in some instances, they seek the support of external consultants to ensure compliance with regulations. Tchankova (2002) stated that risk management is a continuous process that depends directly on the change of a company's internal and external environment. Since the nature and degree of threats to companies vary, the risk levels are not static, and the technological vulnerabilities are uncovered over time. The risk assessment is undertaken in two ways, either formally on a regular basis, at least once a year, or informally on an ongoing basis or when required, and the majority of companies use a well-developed risk assessment process, regardless of the industry sector. Moreover, the results suggest that although almost all companies responded believed that the security risk level is moderate or low, and it is predictable, risks can change and consequently they are not confident of the future.

As predicted, interviewees' opinions regarding security incidents that occurred within their companies in the last two years were not consistent with the questionnaire findings in which only 17.2 percent of companies stated that they had experienced security incidents in the last year, whereas 82.8 percent claimed that they had not experienced any security incidents in the last year. The majority of interviewees stated that their companies had suffered from some security incidents in the last year. However, the majority of companies reacted, and contained the incidents very quickly, which prevented them from becoming major incidents. This result may be either because the security level had improved in the last year compared to two years

ago, so the number of companies suffering from security incidents had decreased, or because many companies were reluctant to report their security incidents in a questionnaire to a stranger.

The results suggest that although interviewees reported different serious security incidents that could happen in their companies e.g. financial fraud, the failure to recover from a disaster, accidental damage to IS, virus or malware attacks that shut down the whole system, hackers, and disgruntled employees, the loss of customer information remains the biggest fear for the majority of companies.

On the other hand, the results confirmed the questionnaire findings regarding the existence of security incident handling procedures, and the existence and frequency of testing and updating the business continuity plan, which emphasised the importance of these procedures and plans in the face of any security incident.

Ryan and Ryan (2006) argued that making decisions concerning investments in security requires a calculation of the net benefits expected from the investment. However, because security is at its best when nothing happens, it is difficult to measure or quantify. Interviewees' opinions confirmed the questionnaire findings that the majority of companies responded do not have a separate security budget, but they have the security budget within their IT budget, and this represents nearly 5 percent or less of the IT budget. The results also suggest that there is no separate budget specifically for AIS security. Interviewees' opinions also confirmed the questionnaire findings regarding the companies' top areas of spending on security. The results indicate that the majority of companies responded spend the biggest part of their security budget on software security controls, physical security controls and on security testing.

Moreover, interviewees' opinions highlighted the fact that the overall awareness level of the two parts of the British Standard BS 7799 is still low among managers and employees in UK companies, except for those managers who have a professional security qualification. Interviewees' opinions also indicated that the majority of companies responded are not certified under ISO 27001, and are not planning to be certified, and even those who are certified cannot see much benefit from this

certification. The majority believe that it requires much time, effort and money, it is not mandated by any regulatory body or authority, and consequently it is not necessary to be certified. However, the majority emphasised the usefulness of complying with the standard.

Interviewees' opinions also confirmed the questionnaire findings regarding techniques used to measure security effectiveness; however, they were not consistent with the findings concerning the most important success indicators of their companies' security management. The results suggest that the majority of companies responded depend on the internal and external audits to evaluate their security effectiveness, followed by penetration testing, risk assessment, number of security incidents, and the security awareness level among employees. In addition, the results emphasised the number of security incidents and employees' awareness as the most important success indicators of security management cited by the majority of companies. The results also revealed that the majority of companies in different sectors, except for the insurance & financial services sector, were not sufficiently confident about the effectiveness level of their security management, which was consistent with the questionnaire findings.

The results confirmed the questionnaire findings concerning the most common sources, types, and most frequent security threats facing the companies. The results revealed that employees are the most common security threat in terms of failing to follow procedures, having too much access to systems and information, misusing the internet, or intentionally undertaking malicious activities. Moreover, people were cited as the most frequent security threat facing the majority of companies through their unintentional errors or mistakes, data leakage, financial fraud in terms of phishing and spamming attacks, and downtime. In addition, the results suggest that employees and loss of customer information are likely to be the main concerns of the majority of companies responded over the next few years, while some companies are concerned about customers, mobile devices such as mobile phones, laptops, memory sticks, and the internal fraud as well.

Although the majority of companies have begun to recognise the human factor in all aspects of information security, interviewees' opinions showed that they are still

focusing on the solid security technologies alone to counter their security threats e.g. employees, and they underestimate the importance of security standards and their commitment to raising employees' awareness. Dutta and McCrohan (2002) argued that if the gap between expectations and reality is large, and if the companies have not exercised due diligence in protecting their systems and information, they will encounter significant corporate, and possibly personal liability. The majority of companies were confident that they had enough security controls in place, believing there was no need for more controls, and therefore, no gap existed between their security threats and the controls implemented. On the other hand, a few companies believed that a gap existed between threats and controls, mainly due to funding reasons. Finally, the results showed that the majority of companies responded were confident that the security level would improve in the next year, which indicates that these companies are taking security seriously and are spending more time and effort in improving their security level.

The following chapter concludes the research, summarises its main findings and presents some recommendations drawn from these findings. The limitations of the study are also highlighted along with the future research possibilities.

Chapter 6

Summary and conclusion

6.1 Introduction

Chapter 5 was concerned with discussing the main findings derived from the semi-structured interviews. It presented the selection of interviewees, and the data analysis methods of the interviews. It also provided the opinions of the interviewees on AIS security within their companies.

This chapter concludes the research, summarises its main findings and presents some recommendations drawn from these findings. This chapter comprises seven sections. Section 6.2 reviews the research aims and objectives. The data collection methods used in the current research are presented in Section 6.3. Section 6.4 provides a summary of the main findings of the research. Section 6.5 indicates the limitations of the research, while Section 6.6 presents the recommendations drawn from the research findings. Section 6.7 suggests some areas for future research, and finally Section 6.8 concludes the research.

6.2 Aims of the research

The security issue has received considerable attention from both academics and professionals. IS security has become a part of core business processes in companies of all sizes and types, and it has become more vital than ever that companies need to have an organised, efficient, and proactive security approach to their IS (Booker 2006). In the UK, the priority given to security remains high across all companies. According to the BERR Information Security Breaches Survey (BERR 2008), four fifths of companies believe that information security is a high or very high priority to their senior management. In addition, the American Institute of Certified Public Accountants' 19th Annual Top Technology Initiatives Survey (AICPA 2008) indicated that information security management is a key factor in doing business. For six consecutive years, the survey identified information security as the country's number one technology concern.

However, while the importance of AIS security is being increasingly recognised, a number of significant gaps exist, particularly in the academic literature. For example, security research is fragmented and no comprehensive framework exists. In addition, while a number of surveys have been conducted to investigate different security issues, they have been commercially oriented surveys and not formal academic studies. Moreover, the literature review reveals that there are different dimensions for security - technical and non-technical - that have to work together to create a secure environment. However, much research on AIS security has been focused on the technical aspects with limited consideration of the non-technical such as security policy, training and awareness, and consequently, lacks an overall view of the AIS security issue. Wood (1995) argued that, no matter how sophisticated the information security technology is, controls will not be sustainable unless the human factor has been adequately addressed. Chang and Yeh (2006) also indicated that effective information security should address both IT and non-IT related issues instead of simply considering IT aspects of the AIS. More recently, Kritzinger and Smith (2008) stated that technical and non-technical security issues should be balanced to ensure that the technical issues do not overshadow the non-technical issues so that the human side of information security is adequately addressed when developing a common body of knowledge for security suited to industry. Moreover, each of the previous studies addresses only one security dimension.

The current study is therefore an attempt to fill these gaps and to present an integrated view of the AIS security in UK companies by addressing both the technical and non-technical aspects of security. More specifically, the current study intends to achieve the following objectives:

1. To examine the existence of an adequate management framework of AIS security within UK companies in different industry sectors.
2. To investigate the different types of AIS security threats facing UK companies in different industry sectors.
3. To investigate the security controls implemented by UK companies to prevent or reduce security threats.
4. To investigate the effect of the security controls implemented on the reduction of AIS security threats facing UK companies.

5. To investigate the relationship between AIS security effectiveness of UK companies and their AIS security threats level.
6. To examine the security perception among different industry sectors in the UK.

In order to achieve these objectives, five hypotheses were developed (Section 3.2.4 in Chapter 3). These hypotheses addressed the different types of threats facing UK companies in different industry sectors, different types of controls implemented to prevent or reduce these threats, and the existence of AIS security management framework within companies in different industry sectors.

6.3 Data collection methods of the current research

In order to test the research hypotheses, the current study employed quantitative and qualitative approaches using a postal questionnaire and semi-structured interviews. The first stage involved a postal questionnaire. This method was chosen because of its specific relevance to the nature of this study as well as the advantages it poses compared to other research methods (Section 3.6.1). Moreover, it is the most popular method used in previous research into IS security such as Abu-Musa (2004a and b), Chang and Ho (2006), Henry (1997), Hitchings (1995), Hong *et al.* (2006), Huang *et al.* (2006), Kankanhalli *et al.* (2003), Kotulic and Clark (2004), Loch *et al.* (1992), Ryan and Bordoloi (1997), Whitman (2004), and Yeh and Chang (2007).

The final version of the questionnaire was sent by post to the IT managers of 800 UK listed companies in several industry sectors. A total of 104 responses were received. However, 65 questionnaires were usable for statistical analysis, resulting in a usable response rate of 8.1 percent (Table 4.1 in Chapter 4). As was mentioned in Chapter 3 (Section 3.6.1), the first and most important problem of using a postal questionnaire is the poor response rate as identified and experienced by many IS security researchers (Table 3.3 in Chapter 3) particularly when dealing with very sensitive and intrusive security issues.

The frequency distribution tables and the cross-tabulations were used in the current study as the first step in data analysis. As the analysis progressed beyond the descriptive stage, the researcher applied the non-parametric tests for many reasons.

First, the sample size in the current study is small. Second, the data collected are nominal and ordinal. Third, non-parametric techniques require no assumptions about the shapes of the sampled populations. Fourth, the sample in the current study was made up of observations from seven industry sectors. Consequently, Kruskal-Wallis One-Way Analysis of Variance, Chi-Square Test of Independence, and Spearman's Rank Correlation were used to analyse the data of the questionnaire. Then, a series of stepwise regressions were run in an attempt to identify the significant effect of the different types of security controls implemented in UK companies and the security effectiveness level on the reduction of the companies' AIS security threats (Section 4.3 in Chapter 4).

The second stage involved semi-structured interviews. Interviews have become increasingly recommended and utilised in IS research in general and AIS security in particular such as Keller *et al.* (2005), Mitchell *et al.* (1999), Straub and Welke (1998), and Tryfonas *et al.* (2001). In the current study, the main empirical base is made up of the questionnaire, and the qualitative phase - interviews - serves to add illustrative support to the questionnaire findings and to clarify some aspects that the quantitative data have not brought to light. As mentioned in Chapter 3 (Section 3.6.2.1), at the end of the questionnaire, the respondents were asked to provide their contact details if they were willing to participate in a follow-up face-to-face interview to discuss some security matters in more depth. In total, nine interviews were conducted with managers of nine UK listed companies in different industry sectors. It seems that the sample size is small, but it is not surprising that only nine respondents were willing to participate in the study. According to Kotulic and Clark (2004), the security investigation research is the most intrusive type of research, and there is undoubtedly a general mistrust of any outsider attempting to gain data about the actions of the security practitioner community. The researcher believes that the opinions provided by the nine managers are, to a great extent, enough to confirm the general patterns appeared in the questionnaire results. The interviews lasted between one and three hours (Table 5.1 in Chapter 5). The researcher took some notes in addition to audio recording all the interviews. The researcher transcribed the interviews in full and used the qualitative data analysis software (NVivo) to support Miles and Huberman's approach in analysing the interview data (Section 5.3 in Chapter 5).

6.4 Main findings of the research

The findings of the current research are presented in three main sections. First, the management framework of AIS security within UK companies; second, AIS security threats facing UK companies in different industry sectors; and finally, AIS security controls implemented by UK companies to prevent or reduce security threats.

6.4.1 The management framework of AIS security

A review of the literature revealed that companies and their AIS are subject to increasing numbers and types of security threats. Consequently, the importance of an AIS security management framework has become evident, and companies now strive to establish effective security management practices. AIS security management is a stream of management activities that aim to protect the AIS and create a framework within which AIS operates as expected by the company (Eloff and Von Solms 2000). The security management framework in the current study includes the security policy, security training and awareness, risk assessment, incident handling, disaster recovery and business continuity plans, security budget, security standards and certification, and AIS security effectiveness.

Table 6.1 Results of the existence of a management framework for AIS security

Hypotheses	Questionnaire results	Interview results	Remarks
H1.1: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security policy and the frequency of updating this policy.	*H1.1* cannot be rejected.	The interviews confirmed these findings.	Some sectors such as the energy & utilities and media & entertainment do not devote enough efforts to updating their security policy.
H1.2: There are no significant differences among UK companies in different industry sectors concerning the existence of an AIS security training and awareness program and the security awareness level.	*H1.2* cannot be rejected regarding the existence of an AIS security training program. However, the results showed that there are significant differences among UK companies in different industry sectors regarding the communication of security awareness issues in response to specific incidents.	The interviews confirmed these findings.	The results suggest that although some sectors are taking steps to provide their employees with security training and to raise their awareness, security training is still the most neglected security practice in the majority of companies compared to other security practices.
H1.3: There are no significant differences among UK companies	The results provide strong support for *H1.3*.	The interviews confirmed these findings.	The majority of companies are undertaking a broad

in different industry sectors concerning the existence of an AIS risk assessment program and the frequency of undertaking this program.			risk assessment for the whole company and not just for AIS security in particular.
H1.4: There are no significant differences among UK companies in different industry sectors concerning the existence of security incident handling procedures, disaster recovery and business continuity plans and the frequency of testing and updating these plans.	*H1.4* cannot be rejected.	The results are not consistent with the questionnaire findings, given that the interviews revealed that the majority of companies that responded had experienced security incidents in the last two years.	The results showed that the only companies who stated that they had more than 15 security incidents in the last year were from the insurance & financial services sector, while the other sectors had from one to five security incidents.
H1.5: There are no significant differences among UK companies in different industry sectors concerning the existence of a security budget and areas of spending on AIS security.	*H1.5* cannot be rejected regarding the existence of a security budget. However, the results showed that there are significant differences in the distribution of responses among industry sectors regarding the hardware and physical security controls.	The interviews confirmed these findings.	The majority of companies that responded do not have a separate security budget. In addition, there is no separate budget specifically for AIS security.
H1.6: There are no significant differences among UK companies in different industry sectors concerning the awareness level of the British Standard for Information Security Management BS 7799 and the certification under ISO 27001.	The results provide strong support for *H1.6*.	The interviews confirmed these findings.	The overall awareness of the British Standard BS 7799 in UK companies that responded is low, whereas the awareness level is somewhat higher among those managers who have a professional security qualification, and among some IT staff.
H1.7: There are no significant differences among UK companies in different industry sectors concerning the techniques used to evaluate AIS security effectiveness, the success indicators of AIS security management, and the effectiveness level of AIS security management.	The results provide a strong support to *H1.7*.	The interviews confirmed these findings.	

6.4.1.1 AIS security policy

In line with the results of previous studies (BERR 2008; Fulford and Doherty 2003), the questionnaire findings (Table 4.10 in Chapter 4) revealed that the majority of UK companies that responded have a written security policy, and 58.7 percent of companies updated their security policy every year (Table 4.11). The interviews confirmed these findings; however, they revealed that some companies still do not have a security policy, but they have a whole policy of which security is a part. On the other hand, despite the importance of updating and reviewing the security policy, interviewee E from the utilities sector stated that the security policy had not been updated for nearly five years, and another interviewee (G) from an entertainment company believed that his company had never updated the security policy.

The results of the interviews also indicated that companies shared two common means for distributing the security policy, either in a hard copy in the induction of new employees or via the intranet or the companies' internal website, which is considered the most cost-effective way of distributing the policy on current employees. However, the scope of security policy varies according to the objectives and requirements of the different companies that responded.

Von Solms and Von Solms (2004) argued that it is no use having a perfect security policy if it is not possible to monitor and enforce compliance to such a policy. The results showed that the companies use different techniques to check employee compliance with the policy; however, the most common techniques used are auditing and employee monitoring. Interestingly, the majority of interviewees believed that their companies' security policy was effective, whereas one interviewee (C) from the property sector claimed that the policy was not effective given that people were always breaking the rules to get their work done.

Overall, the results (Table 6.1) indicate that AIS security policy is now available in the majority of UK companies that responded regardless of the industry sector. However, some sectors such as the energy & utilities and media & entertainment do not devote enough efforts to updating their security policy. Tracy (2007) argued that, it is not enough to establish a security policy. The rapid increase in new threats, frequent and extensive changes to IT environments and new requirements for

regulatory compliance mean that companies need to be proactive and to perpetually update and enforce their policies.

6.4.1.2 Security training and awareness program

There is wide agreement in the literature regarding the important role of the security training and awareness programs in companies, given that employees are often the weakest link in security and the cause of many security threats (Chen *et al.* 2008; Goucher 2008; IFAC 1998; Vroom and Von Solms 2004). Peltier (2005) argued that an effective security program cannot be implemented without implementing an employee awareness and training program to address policy, procedures and tools. In addition, awareness of the risks and available controls is the first line of defence for IS security (OECD 2002).

Despite this importance, the questionnaire findings (Chapter 4) suggested that UK companies that responded still do not make enough effort to train their employees and raise their security awareness. The results (Section 4.5.2) revealed that 29 percent of companies provide security training for their managers (Table 4.14), 25.8 percent provide training for their employees (Table 4.15), whereas only 17.2 percent provide training for the other users such as third parties and contractors (Table 4.16). The results also revealed that some sectors are taking more steps to provide their managers and employees with security training and to raise their awareness (e.g. the insurance & financial services) than other sectors (e.g. the property & construction and manufacturing). In fact, there is a wide agreement that financial services companies are more concerned with security than the other companies. Goodhue and Straub (1991) stated that financial services companies are more likely than other companies to rely extensively on AIS for their operations. Consequently, they tend to have a greater concern for AIS security due to large potential losses that may occur from AIS security abuses. In addition, Holmes (2006) argued that the financial services sector must adhere to the most stringent information security laws, and therefore it leads other sectors in following proven, strategic security practices.

The interviews confirmed the questionnaire findings. Interviewee C stated:

"I worked in banks before. In banks, they are much more aggressive about testing that people are aware and understand the rules, since they are regulated by the FSA (Financial Services Authority)".

However, the results indicated that despite the non-existence of a formal security training program in the majority of companies for current employees, there is wide agreement of the importance of security training for new employees, which is a part of their induction program. In addition, it is not practical to have annual classroom training for current employees due to the time and cost constraints, and consequently, companies depend on computer-based training via the intranet or through publishing some articles covering different security issues on the companies' web pages. However, some companies combine this computer-based training with other media such as classroom, one-to-one basis, and regular meetings.

Despite the importance of measuring staff security awareness, the questionnaire findings (Table 4.21) revealed that only 28.6 percent of companies agreed or strongly agreed that they conduct regular testing of security awareness. The interviews confirmed these findings and suggested that the majority of companies are not making enough effort to test their employees' security awareness or to measure the effect of the training program on the company. This might be due to the limited time and resources devoted to security training and awareness, and the difficulty companies found in measuring their employees' security awareness level. Given that security awareness is about people's behaviours and these are always hard to measure, it is a challenging area for most companies (Enisa 2007). Consequently, it is not surprising that the majority of interviewees believed that the overall security awareness level within their companies is medium or just satisfactory.

Overall, the results (Table 6.1) suggest that although some sectors are taking steps to provide their employees with security training and to raise their awareness such as insurance & financial services, security training is still the most neglected security practice in the majority of companies compared to other security practices. Consequently, there is much to be done in UK companies that responded, particularly with the increasing number of security incidents in the press everyday.

6.4.1.3 Risk assessment

Given that companies are exposed to unlimited security risks, there is wide agreement regarding the important role of risk assessment to enable risks to be identified, evaluated, and managed. Once a company has the ability to measure its security risks, it has the power to identify and implement appropriate controls based on its real business needs (Kleinfeld 2006). The questionnaire findings (Table 4.23 in Chapter 4) revealed that 64.4 percent of companies that responded have an AIS risk assessment program, and all interviewees believed that their companies are undertaking security risk assessment. This may be because the majority of companies are undertaking a broad risk assessment for the whole company and not just for AIS security in particular. Moreover, the majority of interviewees believed that the different security practices could be applied to all systems within companies and not specifically for AIS. The results (Table 6.1) also showed that the media & entertainment sector has become more concerned with security and is taking more steps to assess security risks, given that all respondents from this sector have a risk assessment program.

Moreover, there is broad agreement, not only in the literature, but also in practice regarding the importance of continuous security risk assessment in companies. The questionnaire findings (Table 4.24) revealed that 86.1 percent of companies are undertaking risk assessment every year or more frequently and all interviewees confirmed this finding and stated that risk assessment is undertaken formally at least once a year and informally on a continuous basis. For example, interviewees from the insurance & financial services sector believed that their companies undertake risk assessment on a quarterly basis. This is not surprising, given that insurance & financial services companies are regulated by the Financial Services Authority, and they have to undertake and report their risks regularly.

Given that threats vary over time, companies are more concerned with reassessing their security risks, and with reconsidering the effectiveness of their security controls. The results revealed that the majority of UK companies that responded have a certain manager or team, specifically for undertaking risk assessment tasks, such as a risk management team or an operational risk team and in some instances, they seek the support of external consultants.

Lichtenstein (1996) argued that since each company possesses its own characteristics, an ideal risk assessment that would suit all companies does not exist. The results also showed that the majority of companies have a well developed risk management process. Some companies use a matrix or certain scale to assess their security risks, whereas other companies assess their risks against standards and baselines such as ISO 27001. Moreover, almost all companies that responded believed that they rarely have high risks. They are confident that their risk level is medium to low and is predictable. However, since risks are changeable, they are not confident of the future.

Overall, the results suggested that these companies are devoting much time and effort to undertaking security risk assessment compared to other security practices. This could be because risk assessment and reporting have become obligatory for most UK listed companies.

6.4.1.4 Incident response, disaster recovery and business continuity plan

It is hard to ignore the stream of security incidents covering the daily news. For example, in November 2007, a UK government department, HM Revenue & Customs, lost two discs containing 25 million records - the whole child benefit database (Anonymous 2008 a), a laptop containing unencrypted information on about 600000 potential recruits was stolen from a Royal Navy officer's car on January 2008, and the bank details of about 3500 people were included on the laptop. Moreover, Marks & Spencer has been ordered to ensure all company hard drives are encrypted by April 2008. The enforcement from the ICO (Information Commissioner Office) came after the theft of an unencrypted laptop containing the personal information of 26000 employees (Anonymous 2008 b). It is, therefore, vital for all types of companies to have security incident handling procedures to deal with these incidents and to react quickly to any disruption in normal business operations.

Interestingly, the results of the interviews revealed that the majority of companies that responded had experienced security incidents in the last two years; however, they believed that they were able to react and contain the incidents very quickly. This result is not consistent with the questionnaire findings (Table 4.31 in Chapter 4) in which only 17.2 percent of companies stated that they had experienced security incidents in the last year, whereas 82.8 percent claimed that they did not have any

incidents in the last year. This result may be either because the security level had improved in the last year compared to two years before, or most probably because many companies were reluctant to report their security incidents in a questionnaire to a stranger to maintain their reputation. This opinion supports the results of previous studies such as BERR Information Security Breaches Survey (BERR 2008), Fenrich (2008), Whitman (2004), etc.

The results interestingly revealed that the only companies who stated that they had more than 15 security incidents in the last year were from the insurance & financial services sector, while the other sectors had from one to five security incidents (Table 4.32). The results of the interviews are consistent with the questionnaire findings, given that interviewee F from the financial services sector believed that the average number of security incidents experienced by his company between 2005 and 2007 was nearly 50 incidents per year. This result could be because insurance & financial services companies devote more time and effort to training their staff and raising their awareness. Consequently, employees are more aware of the security incidents they are suffering from. Interviewee A from the insurance sector stated:

> *"There is a complex relationship between security awareness and the number of incidents. Once people become aware of security, the number of incidents recognised increases, because if people have no security awareness, they are not aware that they are making mistakes. There is a relationship between security awareness and incident level. According to the classic model, security awareness will rise, and the number of incidents also rises".*

Moreover, the results showed that UK companies that responded suffered from different types of security incidents in the last year such as financial fraud, unauthorised access to data or system by current or former employees, virus attacks, data loss and internet misuse (Table 4.33). The interviews confirmed the questionnaire findings and cited other types of incidents as well for example the inappropriate use of mobile devices such as USB sticks, phishing attacks, abuse of computers, theft of laptops and the loss of service or downtime. Further analysis revealed that the majority of the industry sectors suffered from financial fraud and loss of data or laptops. This result is consistent with previous surveys (BERR 2008) which indicated that over half of large UK companies had a staff computer fraud in the last year. In addition, the CSI Survey (Richardson 2007) stated that financial fraud together with data loss account for nearly half the overall reported losses.

Given the stream of incidents of data leakage and theft, and the loss of laptops containing financial and sensitive information, it is not surprising that the majority of interviewees considered data loss as the worst security incident that could happen to their companies. Consequently, UK companies that responded are beginning to address this problem and to implement appropriate security controls to prevent data from falling into the wrong hands.

The questionnaire findings revealed that the majority of companies have formal security incident handling procedures in place, except for the manufacturing companies in which only one third have formal procedures (Table 4.34). Interviewees confirmed these findings, and almost all interviewees believed that there are formal procedures within their companies to handle any security incident. These results are consistent with the results in Sections 4.5.1 and 4.5.2 (Chapter 4) in which nearly half of the manufacturing companies have a security policy and 80 percent do nothing to train their managers and employees on their security responsibilities. These results indicate that manufacturing is the sector least concerned with AIS security.

The results also indicated that the majority of UK companies that responded took just one day to restore normal operations after a serious security incident (Table 4.35). However, the only companies that spent between a week and a month to restore their operations after a serious incident are from the insurance & financial services and energy & utilities sectors. This could be because these two sectors deal with thousands of customer data, and therefore, if any security incident arises, it takes them weeks to restore normal operations. Moreover, after a security incident, the majority of companies improve their disaster recovery and business continuity plan, update their security policy, or undertake a security audit (Table 4.36). However, Table 4.37 revealed that all the technology & telecommunications companies improve security awareness and training after a security incident, in contrast to the manufacturing companies that do not make any effort to improve security awareness. This result confirmed a previous result (Section 4.5.2 in Chapter 4) in which the manufacturing sector is the least likely to provide staff with the relevant security training. Interviewees confirmed these findings and reported other actions as well such as investigating the incident, reviewing risks, checking existing controls, improving

procedures, amending practices and standards, reviewing the policy, communicating the incident to employees, and learning from incidents.

There is wide agreement in the literature that many security incidents go unreported because of the fear of negative publicity (Allen 2006; Olnes 1994; Richardson 2007; Willison and Backhouse 2006). The results indicated that the majority of companies that responded prefer to maintain their brand and to deal with security incidents internally even if these incidents cost them time and money, except the insurance & financial services companies which are obligated to report their security incidents to the relevant authorities such as FSA, ICO, BBA, otherwise they will be fined.

On the other hand, the questionnaire findings (Table 4.38) and the interviews showed that the business continuity plan is now a common document within almost all companies. This could be because the severe floods that took place in July 2007 highlighted the business continuity threats that companies could face, or companies have the desire to be certified under the new British Standard BS 25999 that covers business continuity. In addition, Table 4.39 revealed that the majority of companies test and review their business continuity plan every year or more frequently. Interviewees confirmed these findings and indicated that all companies, regardless of the industry sector, are formally testing their business continuity plan at least once a year, in addition to informal tests throughout the year, which highlights the importance of this plan for all types of companies in today's business environment.

It is encouraging also that the majority of interviewees believed that their companies were effective in detecting and responding to security incidents. However, a few companies admitted they were less confident as there is no guarantee that something unexpected will not happen tomorrow.

6.4.1.5 Security budget

There is wide agreement that spending the right amount on information security continues to challenge UK businesses (DTI 2006), since over-expenditure reduces profitability, while under-investment can leave the business exposed. In addition, security is still perceived to be an IT issue; therefore, most companies do not have a security budget separate from their IT budget. The questionnaire findings (Table 4.41

in Chapter 4) and the interviews indicated that the majority of UK companies that responded do not have a separate security budget; however, they have the security budget within their IT budget, and this represents nearly 5 percent or less of the IT budget. The results also revealed that there is no separate budget specifically for AIS security (Table 6.1).

In addition, the results revealed that the security spending decision is based either on the requirements of each company or is a part of the company's annual business plan. Moreover, the approval of the security budget is undertaken by different directors such as IT director, financial director, CIO; and the ultimate responsibility of approving and signing the budget is for the board of directors.

Furthermore, interviewees' opinions regarding the top areas of spending on security confirmed the questionnaire findings (Table 4.46) which revealed that software security controls were considered the first area of spending, followed by hardware and physical security controls, audit activities, incident response and business continuity. However, the results of the Kruskal-Wallis test (Table 4.47) did not indicate any statistically significant differences in the distribution of responses among sectors except for hardware and physical security controls, which indicates that some sectors such as insurance & financial services are depending on these controls and are spending on them more than the other sectors. In addition, some companies believe their security spending level is not enough and they need a higher security budget, while others believe that it is adequate according to the industry benchmarks. On the other hand, other companies believe that security spending is enough and there is no need for more spending. However, the results showed that senior management who often lacks security awareness always takes decisions concerning the appropriate level of security spending.

6.4.1.6 Security standards and certification

Many authors such as Brenner (2007), Dodds and Hague (2004), Karabacak and Sogukpinar (2006), and Kouns (2007) claimed the importance of the British Standard BS 7799 (now ISO 27000) and its two parts ISO 27002 (part 1: Code of Practice) and ISO 27001 (part 2: Certification). It gained recognition as an essential standard for information security.

Despite the benefits highlighted in the literature, the results (Tables 4.48 and 4.49 in Chapter 4) illustrated that the respondents are not sufficiently aware of the two parts of the standard. One third of respondents stated that their awareness level of part 1 is high, whereas only 23.8 percent had the same opinion regarding part 2. The interviewees confirmed these findings given that the majority believed that their awareness level is low. This is a surprising result given that the respondents are IT managers and the people responsible for all security aspects in their companies. Moreover, further analysis suggested that the awareness level is somewhat high in the insurance & financial services, and energy & utilities, whereas it is weak in technology & telecommunications and very weak in the manufacturing, retail merchandising, and property & construction sectors.

The overall awareness level of the other managers and employees is low as well. Unfortunately, the questionnaire findings revealed that 73 percent of companies indicated that their managers' awareness level of the standard is low, and 93.7 percent had the same opinion regarding the employees (Tables 4.50 and 4.51). The interviewees confirmed these findings, which suggested that the overall awareness of the British Standard BS 7799 in UK companies that responded is low, whereas the awareness level is somewhat higher among those managers who have a professional security qualification, and among some IT staff (Table 6.1).

Moreover, although the literature suggests many benefits for companies of being certified under ISO 27001 (Section 3.2.1.3 in Chapter 3); the questionnaire findings (Table 4.53) and the interviews revealed that only two companies are certified. This is not surprising given that more than three quarters of respondents stated that their awareness level of part 2 of the standard, against which companies seek certification, is moderate or low (Table 4.49). In the interviews, many reasons were given for not being certified. Some interviewees could not see any benefit in being certified, others believed that it needed much time and cost to become certified, whereas other interviewees believed that not being mandatory, it was not necessary to become certified. They believed that companies who are certified are those companies providing business-to-business services, in order to prove to their clients that they take security seriously and that their controls are adequate. These results, therefore, indicated that, in practice, many UK companies that responded believe that preparing

for this certification is a comprehensive and time-consuming effort, and even some of the companies, which are already certified under ISO 27001, could not see enough benefit from being certified.

On the other hand, although the majority of interviewees could not see benefits from being certified under ISO 27001, they saw many benefits of complying with the standard for example compliance could provide sound information security, assurance for customers, an excellent reference point, a framework and could facilitate compatibility. However, some companies in different sectors still cannot see any benefit from compliance. In their opinion, it takes up too much time, effort and money, and is still optional and not required by clients. This opinion in not consistent with the BERR Information Security Breaches Survey (BERR 2008) which pointed out that all companies that have implemented the standard have achieved benefits from doing so.

6.4.1.7 AIS security effectiveness

Measuring IS effectiveness has been an important research issue in previous studies such as DeLone and McLean (1992), Huang *et al.* (2006), Kankanhalli *et al.* (2003), and Wright (2006). There is a strong argument that measuring security effectiveness ensures that security actually works as expected, eases the process of monitoring the effectiveness of security management, reduces the number of security incidents, and provides evidence to auditors and assurance to senior management that a company is in control (Furnell and Papadaki 2008; Wright 2006).

The results (Table 4.54 in Chapter 4) indicated that the majority of UK companies that responded depend on an external and internal security audit and on penetration testing to evaluate AIS security effectiveness whereas the least common technique used is "vulnerability scanners". The interviewees confirmed these findings and stated other techniques as well such as risk assessment, number of security incidents, and security awareness level among employees. The results revealed again that the insurance & financial services companies put more effort into training their staff and raising their security awareness than the other sectors, given that they were the only companies who emphasised the use of employees' security awareness as a major technique in evaluating security effectiveness.

Moreover, the results (Table 4.60) revealed that the companies' most common success indicators of AIS security management are the successful defences against security attacks, information security assurance, and the increased ability to recover from disasters, whereas an increased AIS security budget is the least common success indicator. These results could be because most UK companies that responded (Table 4.41) do not have a separate security budget, and those who have, do not allocate a specific amount of this budget for AIS security. However, interviews did not confirm the above results. The majority believed that the non-occurrence of security incidents is their companies' most important success indicator of security management, in addition to employees' security awareness, commitment to policies, vulnerability level and compliance.

In addition, the majority of interviewees mentioned two main obstacles to effective security, namely, people using systems and lack of management support, awareness and commitment. These results supported previous studies such as Chen *et al.* (2008), Fenrich (2008), Gansler and Lucyshyn (2005), and Hagen *et al.* (2008), which indicated that people are the weakest link in security, and lack of management awareness and support is a major concern for companies attempting to defend their IS (Briney 2001; Kwok and Longley 1999).

Regarding the effectiveness level of AIS security management, the questionnaire findings (Table 4.62) revealed that 60 percent of companies believed that their AIS security management was somewhat effective, whereas 23.3 percent believed that it was extremely effective. Interviewees' opinions confirmed these findings, and only one third of interviewees believed that their security effectiveness level was very high, whereas the other interviewees from different sectors believed that the effectiveness level of security management was moderate or reasonable. Further analysis showed that some companies from all sectors except the technology & telecommunications believed that their AIS security management was extremely effective. However, in the interviews, the two interviewees from the insurance & financial services sector believed that their security management was very effective. This could be because insurance & financial services companies are more concerned with security than other sectors and therefore they have all the relevant controls in place, which give them more confidence. In addition, given that all the technology & telecommunications

companies believed that they improved security training and awareness after security incidents (Table 4.37), these companies could be more aware of the different types of threats facing their systems, and therefore they are not fully confident that they have an extremely effective security management.

6.4.2 AIS security threats

The review of the literature revealed that companies and their AIS are subject to increasing numbers and types of security threats. However, due to resource constraints, companies cannot implement unlimited controls to protect their systems. Instead, they should first understand the major threats, and then implement effective controls accordingly (Lin 2006). However, despite the progress made by companies in protecting their systems and information stored in them from outside threats, many studies such as Magklaras *et al.* (2006), Mouratidis *et al.* (2008), Olnes (1994), Swartz (2007), and Wood and Banks (1993) showed that security threats are mainly from staff within companies rather than from outsiders.

The questionnaire findings supported the previous studies and revealed that employees are now the most common source of AIS security threats facing UK companies that responded. The results (Table 4.67 in Chapter 4) showed that authorised employees are the companies' first common source of threats, followed by former employees (second source), and computer hackers (third source). Interviewees confirmed these findings (Table 6.2) and they believed that people or employees are their companies' most common source of threats in terms of not following procedures and polices, having too much access to systems and information, misusing the internet, misbehaving either unintentionally or through ignorance or acting as criminals and having more than one job role. However, the results of the Kruskal-Wallis test (Table 4.68) implied that there are significant differences in the distribution of responses among the different sectors regarding the authorised users or employees, whereas there are no significant differences among the different sectors regarding the other sources of security threats. These results suggest that users or employees have different effects on different sectors, given that only one third of respondents from the energy & utilities sector considered employees their first common source of threats.

Table 6.2 Results of the sources and types of AIS security threats

Hypotheses	Questionnaire results	Interview results	Remarks
H2: There are no significant differences among UK companies in different industry sectors concerning the sources and types of AIS security threats.	The results showed that there are significant differences in the distribution of responses among the different sectors regarding the authorised users or employees as a source of security threats, and the unauthorised access to data or systems by disgruntled employees, and employees' sharing of passwords as types of security threats.	The interviews confirmed these findings.	The results revealed that employees are now the most common source of AIS security threats facing UK companies that responded. The results indicated the frequent occurrence of employees' errors (unintentional destruction of data by employees), spamming and malware attacks, and employees' sharing of passwords.

Moreover, the questionnaire findings (Table 4.69) indicated the infrequent occurrence of some types of security threats such as intentional destruction of data by employees, theft of physical information, theft of software, sabotage, and natural disasters. However, the results indicate the frequent occurrence of employees' errors i.e. unintentional destruction of data by employees, spamming and malware attacks, and employees' sharing of passwords.

Table 4.70 revealed that the unauthorised access to data or systems by disgruntled employees rarely occurred in the property & construction, and energy & utilities sectors, but could happen in the other sectors. The property & construction companies that responded are also rarely faced with unauthorised access to data or systems by hackers, whereas the most likely sector to suffer from this threat is the manufacturing sector (Table 4.71).

It is not surprising that the unintentional destruction of data by employees occurred in 63.3 percent of companies that responded (Table 4.72), given that employees' accidental actions were recognised in many previous studies such as Davis (1997), Loch *et al.* (1992), and Steele and Wargo (2007). However, the results indicated the infrequent occurrence of the intentional destruction of data by employees (Table 4.73). These results supported Im and Baskerville (2005) who argued that the major source of unmanaged risks to IS continues to be accidental in nature.

The results (Table 4.75) also suggested that viruses are no longer a big issue for UK companies. This could be because the media attention given to viruses has increased the awareness level of this threat or because anti-virus defences have significantly improved. However, the results (Table 4.76) indicated the frequent occurrence per day of spamming or e-mail attacks.

The results also suggested the frequent occurrence of malware attacks in UK companies that responded, despite the increasing use of malware detection tools. Moreover, further analysis (Table 4.77) indicated that manufacturing companies are the least affected by malware attacks, while energy & utilities and technology & telecommunications are the most affected companies. This could be because manufacturing companies have a lower level of computerisation compared to other sectors, and therefore they are the least affected companies by malware attacks (Yeh and Chang 2007), whereas energy companies are least likely to be protected against spyware (BERR 2008).

On the other hand, 72.9 percent of companies that responded reported that employees shared their passwords in the last year, which indicates its frequent occurrence, particularly in the retail merchandising companies, where they believed that it happens several times per day (Table 4.78).

Interestingly, one respondent only, from technology & telecommunications believed software theft occurred several times per day (Table 4.79), which indicated the low level of occurrence of software theft in UK companies that responded. On the other hand, the results gave an indication that software failures are happening in most companies, since few companies claimed their non-occurrence (Table 4.80).

The results also indicated the rare occurrence of sabotage in media & entertainment, property & construction and retail merchandising, its infrequent occurrence in the other sectors (Table 4.81), and the low level of occurrence of natural disasters in UK companies that responded (Table 4.82).

The results of the Kruskal-Wallis test (Table 4.83) revealed that there are statistically significant differences in the distribution of responses among the different industry

sectors regarding the unauthorised access to data or systems by disgruntled employees, and employees' sharing of passwords, which suggested their high level of occurrence in some sectors compared to the other sectors. On the other hand, there are no significant differences in the distribution of responses among the different industry sectors regarding types and frequency of occurrence for the other AIS security threats.

The interviewees' opinions confirmed the questionnaire findings. Interestingly, people or employees were cited by interviewees from all industry sectors that responded as one of their companies' most serious and frequent security threats or as their only serious threat, in terms of misusing the systems, getting too much access, and their unintentional errors and mistakes. Interviewees cited other security threats as well such as loss or leakage of data, identity theft and financial fraud in terms of phishing and spamming attacks, complexity of IS, sharing of information, poor configuration, mobile devices such as USB memory sticks, and downtime. In addition, the majority of interviewees believed that their companies will be more concerned about employees and loss or theft of confidential data over the next two years. This is not surprising given that these threats were emphasised in many previous studies such as Beard and Wen (2007), Furnell and Papadaki (2008), and Mitnick (2003). Consequently, UK companies should consider employee security training and awareness seriously, given that employees are their weakest link and their first line of defence as well. In addition, interviewees cited other concerns such as customers, mobile devices (mobile phones, laptops, USB memory sticks), and financial fraud, which must be considered by companies as well.

6.4.3 AIS security controls

Having identified the most common sources and types of AIS security threats facing UK companies that responded, the next step was to investigate the different types of AIS security controls that these companies are currently using, or are planning to use to reduce their threats. These security controls were grouped under seven sub-titles.

Regarding organisational security controls, the results (Table 4.85 in Chapter 4) indicated that the majority of UK companies that responded are not concerned with reorganising their security functions, except for retail merchandising given that two thirds of companies reported the existence of reorganised AIS security functions. On

the other hand, the majority of companies undertake continuous auditing, except for the manufacturing companies that need to be more concerned with these auditing techniques (Table 4.86). The results (Table 4.87) also indicated that manufacturing companies are less concerned about real time security awareness, which is consistent with the results in Section 6.4.1.2 where these companies appeared to devote less effort to raising security awareness compared to other sectors. Moreover, the majority of companies are aware of the importance of having a current disaster recovery and business continuity plan (Table 4.88). Overall, it can be concluded that manufacturing companies are the least likely to be concerned with organisational security controls compared to the other companies and consequently, they should pay more attention to this type of control.

Regarding personnel security controls, the results (Table 4.89) revealed that the majority of UK companies undertake background checks for their employees; they pay great attention to segregation of duties, and their employees sign a confidentiality agreement before joining. On the other hand, more attention must be given to security training and awareness, and to mandatory vacations. Table 4.90 indicated that media & entertainment is the sector most concerned with undertaking reference checks for employees, while manufacturing is the sector least concerned. The media & entertainment and technology & telecommunications sectors are more concerned with the employees' confidentiality agreement than other sectors (Table 4.91). Moreover, the insurance & financial services sector is most concerned with training and awareness programs (Table 4.92) as shown in Section 6.4.1.2. On the other hand, the retail merchandising sector is paying a great deal of attention to the segregation of duties (Table 4.93), while the majority of companies do not consider a mandatory vacation as an important control (Table 4.94).

With respect to software security controls, the results (Table 4.95) revealed that almost all companies emphasised the importance of certain controls such as anti-virus software, cancellation of passwords for terminated employees, testing software before use, and safeguards against unauthorised access to software. On the other hand, more attention should be paid to the insurance coverage for software, and software audit alert tools. This could be because the majority of companies did not have a sufficient security budget, and therefore they could not justify the spending on insurance

coverage. However, Table 4.96 suggested that media & entertainment and insurance & financial services companies were more concerned about their software, and were storing it off-site. Media & entertainment companies were more concerned about software audit alert tools and the intrusion prevention or detection software as well (Tables 4.97 and 4.98).

Regarding hardware and physical security controls, the results (Table 4.100) indicated that all companies made back-ups for their hard disks and used firewalls. The majority restricted access to main computing facilities, had security alarm systems, placed their accounting servers in secure locations, and protected their computers from natural disasters as well. On the other hand, the majority did not use biometrics and were not planning at all to use it. Table 4.101 revealed that all media & entertainment companies claimed the use of penetration testing. Moreover, Table 4.103 indicated that insurance & financial services companies were more concerned about their laptops, given the sensitive nature of financial data stored in them, and 90 percent of companies stored unused laptops in secured cabinets. Although nearly two fifths of companies had insurance coverage for their software, Table 4.104 showed that 77.8 percent reported the existence of insurance coverage for hardware and computer devices, with all insurance & financial services companies reporting its existence.

With respect to the input or data security controls, the results (Table 4.105) suggested that UK companies that responded gave much attention to access controls and to data back-ups. However, more attention must be given to data encryption, except for the media & entertainment companies, which are more concerned about encrypting their data than other sectors (Table 4.106). This is a surprising result, given that recent security incidents have highlighted how confidential data can become exposed when laptops and other mobile devices are stolen or lost.

Moreover, the results (Table 4.107) revealed that UK companies that responded pay much attention to output security controls, given that the majority restrict access to their sensitive information, and store it in secured cabinets.

Given the increasing use of the internet and email in all companies' operations, it is not surprising to find them more concerned about the network security controls than

ever before. The results revealed that the majority of companies have content and e-mail filtering software, malware (spyware and adware) detection tools, and spam filtering software, while half the companies have implemented network encryption. Table 4.109 indicated that retail merchandising was the sector most concerned with network encryption, whereas manufacturing companies were more concerned with the content and e-mail filtering software than the other controls.

Overall, the results (Table 6.3) indicate that the majority of companies that responded are paying more attention to software and hardware security controls, and input and output controls; however, more effort should be devoted to the organisational and personnel controls, namely, reorganised AIS security functions, incident response, training and awareness, and mandatory vacations. Regarding the other categories of controls, more attention must be given to the insurance coverage for software, biometrics, data and network encryption as well. Interviewees confirmed these findings and reported the existence of most of these controls, in addition to other recently employed controls relevant to their companies. Moreover, the results suggested that the majority of companies are now addressing the human factor in security, through additional controls over internet activities, access to systems and information, the use of mobile devices such as USBs, and the creation of DVDs to raise security awareness. This is not surprising, given that people are seen as the companies' most common source of threat. Consequently, companies' security should start with their own staff given that employees are their first line of defence (Green 2003).

Interestingly, the majority of interviewees are confident that they have enough security controls in place, and there is no need for more controls. However, some companies believed that a gap exists between their threats and controls in terms of a limited security budget and consequently a low level of monitoring controls over systems and internet usage, and a low level of data protection controls. This is not surprising, given that, the majority of companies do not have a separate security budget and the budget is just a part of their IT budget. Moreover, although the majority of companies believed that there were no gaps between their threats and controls, they reported some important security controls; namely, controls for protecting confidentiality, integrity and availability of information, monitoring

controls, single authorisation, risk registers, access controls, and data encryption. The results suggested that companies keep a watch on the emerging security controls around them and select the most relevant ones. In addition, interviewees cited some new security controls their companies were planning to use, namely, biometrics, intrusion detection and prevention systems, access controls on systems and networks, internet reporting system, and provisioning tools.

The majority of interviewees were confident that the security level within their companies would be better in the next year; however, they believed that there is nothing called 'absolute security' or 'Zero Risk'.

Table 6.3 Results of the types of AIS security controls

Hypotheses	Questionnaire results	Interview results	Remarks
H3: There are no significant differences among UK companies in different industry sectors concerning the types of controls implemented to prevent or reduce security threats.	The results provide no evidence of any statistically significant association between the industry sectors and the different types of AIS security controls except for the background investigations or reference checks.	The interviews confirmed these findings.	The majority of companies that responded are paying more attention to software and hardware security controls, and input and output controls; however, more effort should be devoted to the organisational and personnel controls.

Despite the differences noticed among industry sectors, the results of the chi-square test (Table 4.110) provided no evidence of any statistically significant association between the industry sectors and the different types of AIS security controls, except for the background investigations (Hypothesis 3 in Section 3.2.4). This result indicated that some sectors are concerned about these checks more than the others.

Overall, the results suggested that although the majority of companies that responded had begun to address the human factor in security and to realise that people are their most common source of security threat, they still counter this threat using technology alone. However, it can be recognised from the literature that the key to successful security depends more on policies and procedures that companies put in place and on their commitment to raising employees' awareness levels than on implementing technology for its own sake (Golden 2008).

Table 6.4 Results of the Spearman's rank correlation and the regression analysis

Hypotheses	Questionnaire results	Interview results	Remarks
H4: There is no significant relationship between the different types of security controls and the reduction of AIS security threats facing UK companies.	The results showed the relative importance of some types of controls such as penetration testing, and biometrics, compared to other controls, given that these controls have a significant effect on many types of threats.	The interviews confirmed these findings	The results provided no evidence of any effect of some controls on any type of security threats such as software audit alert tools, back-up for hard disks, security alarm systems, users access controls, network encryption, spam filtering software, etc.
H5: There are no significant relationship between AIS security effectiveness and the AIS security threat level in UK companies.	The results provide a strong support to *H5*.	The interviews confirmed these findings	The results suggested that irrespective of their security effectiveness level, companies still face new types of security threats.

On the other hand, the results of the Spearman's rank correlation (Table 4.111) and the regression analysis (Table 4.113) showed the relative importance of some types of controls such as penetration testing, and biometrics, compared to other controls, given that these controls have a significant effect on many types of threats. However, the results provided no evidence of any effect of some controls on any type of security threats such as software audit alert tools, back-up for hard disks, security alarm systems, users access controls, network encryption, spam filtering software, etc. Despite these results, every company should select the relevant mix of controls according to its requirements, given that no single control can protect AIS from all possible threats.

On the other hand, the results (Table 4.112) provided no evidence of any statistically significant correlations between the effectiveness level of AIS security in UK companies that responded and each type of threats. This result suggested that irrespective of their security effectiveness level, companies still face new types of security threats.

6.5 Limitations of the research

As with all previous studies, the current study has its limitations. The first and most obvious is the low response rate. As mentioned in Section 3.6.1 (Chapter 3), the most serious problem with the postal questionnaire was the poor response rate particularly

when dealing with very sensitive and intrusive security issues. Although, the response rate is comparable with many previous security studies (Table 3.3), it demands caution in the interpretation of the results and may hinder the generalisability of findings on all large UK listed companies. Moreover, the questionnaire was directed to the IT managers of UK listed companies. It can be assumed that the internal auditors and finance directors within the same companies might have different opinions regarding different security practices. In addition to these limitations, the postal questionnaire has other drawbacks as mentioned before in Section 3.6.1.

Another limitation relates to the small number of interviews conducted. Although all the managers who were willing and able to participate further in the study were interviewed and they provided rich and detailed answers, the interview findings may not be generalisable to the population of IT managers in UK listed companies, given that the number of interviews conducted was only nine interviews. In addition, it can be assumed that those who were willing to be interviewed had more interest in security. Other managers could have different attitudes to security practices within their companies. There is also a possibility of the interviewer's personal influence and bias directing the discussion towards confirming or finding justifications for the questionnaire results. Other limitations of the interviews were mentioned in Section 3.6.2.

A further limitation is that the results may not be generalisable beyond UK listed companies, given that only listed companies were investigated due to time and cost constraints. There is, therefore, a possibility that managers of unlisted companies could have different opinions and could have provided a clearer picture regarding AIS security level within UK companies.

Moreover, although the questionnaire was directed to IT managers in many industry sectors in the UK, the managers who responded were from a limited number of sectors, which hindered the researcher from investigating security practices in the other industry sectors not participating in the study. On the other hand, the current study did not focus on certain industry sectors. Ma *et al.* (2008) argued that studies that focused on a specific industry sector would be able to identify specific objectives and practices that are more relevant to that specific sector.

Although the current study attempted to provide an overall and comprehensive view of the AIS security issue, it did not cover all the important issues in this field such as the nature and type of AIS used, and the outsourcing of AIS security services within companies, due to some considerations regarding the length of the questionnaire.

Despite the above limitations, the consistency between the majority of the questionnaire and interview results provides an assurance of the validity of the research findings. In addition, the results may provide a useful guide to show common AIS security trends within different industry sectors in the UK.

6.6 Recommendations

Based on the research findings, the researcher recommends the following:

1. The study showed that security is still recognised as an IT issue, and therefore, security management is often left to the IT department, not to the accounting or finance department. Dutta and McCrohan (2002) argued that if there is no structural unit that is specifically responsible for security, the implementation of security initiatives will be fragmented and may therefore be ineffective. Consequently, it is important for UK companies to have a separate security department and security personnel who receive special training and are able to spend all their time on improving security, instead of having security as an additional task. In addition, if there is a separate security budget for this department, it becomes easier to justify the extra security spending to the board of directors.

2. Although security policy now exists in the majority of UK companies regardless of the industry sector, some companies do not devote much time or effort to updating their security policy and checking employees' compliance with the policy. Consequently, companies should make much more effort in reviewing their security policy on a regular basis to keep pace with any changes in business, regulatory, technological and personnel environments. In addition, more effort is needed in monitoring and enforcing the compliance to such policies, given that there is no motivation to comply, if management is not checking upon employees.

3. Although employees are often the weakest link in security and the cause of many security threats, the study reported that UK companies still do not expend enough

energy in training their employees and raising their security awareness, particularly property & construction and manufacturing companies. In addition, companies are not making enough effort to test their employees' awareness or to measure the effect of a training and awareness program on the company. It is important, therefore, for all companies and particularly for property & construction and manufacturing companies to provide their employees with sufficient security training and to raise their awareness level, given that employees are the first line of defence in security.

4. Although the majority of UK companies have formal security incident handling procedures in place, manufacturing companies need to be more concerned with security and to have formal procedures to deal with any security incident.

5. In line with previous studies, many security incidents go unreported since the majority of companies prefer to maintain their brand and to deal with security incidents internally except for the insurance & financial services companies, which are obligated by law to report their security incidents to the relevant authorities. Consequently, it is important to have a specific authority for every industry sector to assist companies if they need help and to deal with security incidents with full confidentiality in order to encourage them to report all their incidents.

6. The study reported that the overall awareness of the British Standard BS 7799 (now ISO 27000) in UK companies is low, except among those managers who have a professional security qualification. Given the importance of complying with this standard, companies must devote more time and effort to increase their staff awareness of it through different means such as arranging seminars, publishing relevant sections of it on companies' intranet, e-mail messages, security awareness newsletters, and periodic briefings.

7. The study has shown that people or employees are the most serious and frequent security threat facing UK companies and they will be their main security concern over the coming years as well. Companies, therefore, face a human threat. Consequently, they must put more effort into non-technical solutions for example security policy, training and awareness, and risk assessment instead of focusing only on technical solutions.

8. The study reported the frequent occurrence of employees' errors i.e. unintentional destruction of data by employees, phishing, spamming and malware attacks, sharing of passwords, data loss or leakage, identity theft, and inappropriate use of mobile devices such as USB memory sticks. Consequently, UK companies must address these threats and must implement the appropriate security controls in an attempt to reduce their occurrence.

9. The study reported that the majority of UK companies are now paying, relatively, more attention to software and hardware security controls, and input and output controls than the organisational and personnel security controls, despite their importance. It is important, therefore, to devote more effort to some controls, namely, security training and awareness, mandatory vacations, insurance coverage for software, biometrics, and encryption of sensitive data and network.

6.7 Suggestions for future research

Based on the limitations of the current study, the following suggestions may provide opportunities for future research:

1. The questionnaire was directed to the IT managers of UK listed companies. It is important to broaden the research and to investigate unlisted companies as well. In addition, a comparative study could be carried out to investigate the differences between UK listed and unlisted companies regarding their security threats, security controls, and their AIS security management framework.

2. The questionnaire could be directed to other managers e.g. internal auditors, and finance directors within the same companies and to the external auditors as well, in order to investigate the differences in their opinions regarding security practices.

3. It may be possible to also investigate the security threats, security controls, and AIS security management framework within small companies in the UK.

4. Although this study aimed to investigate the security level in UK companies, it could also be possible to use the same questionnaire to investigate the AIS security level in other countries.

5. Although the study aimed to investigate the differences among UK companies in different industry sectors, future studies are needed to focus on one sector such as the financial services sector given that studies that focused on a specific industry sector would be able to identify specific practices more relevant to that sector.

6. Although the questionnaire was directed to IT managers in many industry sectors, the respondents came from a limited number of sectors. Future studies therefore are needed to investigate the security practices in the other sectors that did not participate in this study such as education, health care and government.

7. Given the low response rate to the questionnaire and the small number of interviews conducted, a large scale study could be undertaken to investigate the possibility of generalising the findings of the current research on large UK listed companies.

8. Given the low response rate to the questionnaire and the small number of interviews conducted, a future study could be undertaken using the case study method for data collection in order to investigate the security practices of one or more companies in more depth.

9. Although the study is an attempt to present an integrated view of the AIS security in UK companies, future studies are needed to investigate certain security issues in more depth, namely, security training and awareness, and the British Standard BS 7799, given that they are the most neglected areas compared to the other security issues.

10. Due to some considerations related to the questionnaire length, certain important security topics are not covered such as the nature and type of AIS used, and outsourcing of AIS security services within companies. Future studies, therefore, will be necessary to investigate these topics.

11. It would be useful to compare the results of the current study with those obtained from similar future studies in order to investigate the new threats facing UK

companies, and the more advanced security controls implemented to reduce these threats.

6.8 Conclusion of research

Overall, this study has attempted to fill the gaps in the literature on AIS security. First, most of the previous studies have dealt with IS security or information security in general without particular attention to AIS security. Second, security research is fragmented and most of the previous studies lack an overall view of the AIS security issue. Third, much research on IS security has been focused on the technical aspects with limited consideration given to non-technical issues. Fourth, much security research focused on one of the activities forming the management framework for the AIS security rather than the full range of activities underpinning this framework.

In an attempt to extend this area of research, the current study presented an integrated view of the AIS security in UK companies by addressing both the technical and non-technical aspects of security, and by investigating the different sources and types of AIS security threat, the types of AIS security controls, and the existence of a management framework for AIS security within UK companies in the different industry sectors.

The current study achieved its objectives (Section 6.2) using a postal questionnaire and semi-structured interviews. The study reported the existence of a management framework of AIS security within UK companies in different industry sectors (Objective 1). However, some practices forming the framework are well known and undertaken by the majority of UK companies such as an AIS security policy, risk assessment, incident handling procedures and business continuity plans, while other practices are neglected such as security training and awareness programs, a security budget, and the British Standard BS 7799. It is therefore important to draw the managers' attention to the importance of these neglected practices in forming an adequate management framework of AIS security.

In addition, the current study showed that employees are now the most common source of AIS security threat facing UK companies in terms of not following procedures and policies, having too much access to systems and information,

misusing the internet, misbehaving either unintentionally or through ignorance or acting as criminals and having more than one task. Moreover, the study highlighted the infrequent occurrence of some types of security threats such as intentional destruction of data by employees, theft of physical information, theft of software, sabotage, and natural disasters. However, UK companies faced the frequent occurrence of employees' errors (unintentional destruction of data), spamming and malware attacks, and employees' sharing of passwords. UK companies are also concerned about loss or leakage of customer data, identity theft, and financial fraud, complexity of IS, sharing of information, mobile devices, and downtime (Objective 2). The results of the current study should increase managers' awareness in the different industry sectors of the common sources and types of security threat facing their systems so that they can take the appropriate precautions.

The current study also showed that the majority of companies are paying more attention to the software, hardware, input, and output security controls compared to the organisational and personnel controls such as incident response, security training and awareness, and mandatory vacations (Objective 3). The study suggested that more attention should be given to other security controls such as the insurance coverage for software, biometrics, and data and network encryption. Additionally, it appeared that the majority of UK companies are now addressing the human factor in security through additional controls over internet activities, access to systems and information, and the use of mobile devices. However, they still counter their most common source of security threats (people) using technology alone. The current study therefore provides the managers of UK companies with the different types of security controls implemented in the different industry sectors to help them select the most appropriate controls according to their companies' needs.

Moreover, the current study reported the relative importance of some types of controls such as penetration testing and biometrics compared to other controls given their significant effect on many types of threats. However, the results provided no evidence of any effect of some controls such as audit alert tools, back up of hard disks, alarm systems, network encryption, and spam filtering software (Objective 4).

Regarding the security perception among different industry sectors, the current study reported that some sectors such as the insurance & financial services are more concerned about security than other sectors such as manufacturing (Objective 6). It is important therefore to draw their attention to the importance of security in order to be able to take all security aspects seriously and to spend more time and effort in improving their security level.

In fact, although the study aimed to investigate the security of AIS in UK companies, the results showed that the different security practices could be applied to all systems within companies and not specifically for AIS. In addition, the study showed that security is still perceived to be an IT issue, and therefore, security management is often left to the IT department, not to the accounting or finance department.

To conclude, the current study has successfully filled some of the major gaps in the literature on IS security since it specially focused on AIS security. This study could be an important source of information to the accountants and IT managers in UK companies since it has addressed the different aspects of the AIS security. Moreover, this study should help managers to identify security weaknesses in their companies' AIS and to take the appropriate precautions according to their industry sectors in order to reduce the security threats facing their companies.

References

Abu-Musa, AA (2002a) "Computer Crimes: How Can You Protect Your Computerised Accounting Information Systems?", *Journal of American Academy of Business*, 2:1, 91-101.

Abu-Musa, AA (2002b) "Security of Computerised Accounting Information Systems: A Theoretical Framework", *Journal of American Academy of Business*, 2:1, 150-155.

Abu-Musa, AA (2002c) "Security of Computerised Accounting Information: An Integrated Evaluation Approach", *Journal of American Academy of Business*, 2:1, 141-149.

Abu-Musa, AA (2003) "The Perceived Threats to the Security of Computerised Accounting Information Systems", *Journal of American Academy of Business*, 3:1/2, 1-12.

Abu-Musa, AA (2004a) "Exploring the Perceived Threats of Computerised Accounting Information Systems in Emerging Countries: An Empirical Study of Saudi Organisations", *Paper Presented at the Seventh European Conference on Accounting Information Systems* (ECAIS), 30-31 March, Prague, Czech Republic.

Abu-Musa, AA (2004b) "Investigating the Security Controls of CAIS in an Emerging Economy: An Empirical Study on the Egyptian Banking Industry", *Managerial Auditing Journal*, 19:2, 272-302.

Abu-Musa, AA (2006a) "Exploring Perceived Threats of CAIS in Developing Countries: the Case of Saudi Arabia", *Managerial Auditing Journal*, 21:4, 387-407.

Abu-Musa, AA (2006b) "Perceived Security Threats of Computerised Accounting Information Systems in the Egyptian Banking Industry", *Journal of Information Systems*, 20:1, 187-203.

Abu-Musa, AA (2007a) "Evaluating the Security Controls of CAIS in Developing Countries: An Examination of Current Research", *Information Management & Computer Security*, 15:1, 46-63.

Abu-Musa, AA (2007b) "Evaluating the Security Controls of CAIS in Developing Countries: An Empirical Investigation", *Information Management & Computer Security*, 15:2, 128-148.

AICPA/CICA (2001) *SysTrust Principles and Criteria for Systems Reliability*, American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants.

AICPA (2002) *Trust Services Principles & Criteria: Incorporating SysTrust & WebTrust*, Exposure Draft, American Institute of Certified Public Accountants, New York.

AICPA (2008) *The 19th Annual Top Technology Initiatives Survey*, The American Institute of Certified Public Accountants, New York.

Aldhizer, GR (2008) "The Insider Threat", *The Internal Auditor*, 65:2, p.71.

Allen, M (2006) "Coping With a Major Security Breach?", *Management Services*, 50:2, 22-23.

Allison, PD (1999) *Multiple Regression: A Primer,* Pine Forge Press, Thousand Oaks, California.

Amoruso, AJ, Brooks, RC and Riley Jr, RA (2005) "Biometrics and Internal Control: An Emerging Opportunity", *The Journal of Government Financial Management*, 54:2, 40-44.

Anderson, DR, Sweeney, DJ, Williams, TA, Freeman, J and Shoesmith, E (2007) *Statistics for Business and Economics*, Thomson Learning, Bedford Row, London.

Anderson, JM (2003) "Why We Need a New Definition of Information Security", *Computers & Security*, 22:4, 308-313.

Anonymous (2008a) "2007 Sees Profile of IT Security Soar for Wrong Reasons", *Computer Fraud & Security*, 2008:1, 5-6.

Anonymous (2008b) "UK Ministry of Defence Cracks Down on IT Security after Laptop Theft", *Computer Fraud & Security*, 2008:3, 2-3.

Anonymous (2008c) "Finance Advisory Firm Breaches Data Protection Act", *Computer Fraud & Security,* 2008:4, p.4.

Austin, RD and Darby, CAR (2003) "The Myth of Secure Computing", *Harvard Business Review*, June, 120-126.

Babbie, E (1998) *The Practice of Social Research*, 8th ed, Wadsworth Publishing, London.

Bagranoff, NA, Simkin, MG and Norman, CS (2005) *Core Concepts of Accounting Information Systems*, 9th ed, John Wiley & Sons, USA.

Bailey, KD (1994) *Methods of Social Research*, 4th ed, The Free Press, New York.

Barnard, L and Von Solms, R (1998) "The Evaluation and Certification of Information Security Against BS 7799", *Information Management & Computer Security*, 6:2, p.72.

Bazeley, P (2007) *Qualitative Data Analysis With NVivo*, Sage Publications, London.

Beard, D and Wen, HJ (2007) "Reducing the Threat Levels for Accounting Information Systems", *The CPA Journal*, 77:5, 34-42.

Beer, S (1981) *Brain of the Firm*, 2nd ed, John Wiley & Sons, Chichester.

Berinato, S (2007) *The 5th Global State of Information Security Survey*, CIO and PricewaterhouseCoopers, CIO Magazine.

BERR (2008) *Information Security Breaches Survey (ISBS)*, Department for Business Enterprise & Regulatory Reform, London, UK.

Beznosov, K and Beznosova, O (2007) "On the Imbalance of the Security Problem Space and its Expected Consequences", *Information Management & Computer Security*, 15:5, 420-431.

Bhaskar, R (2005) "A Proposed Integrated Framework for Coordinating Computer Security Incident Response Team", *Journal of Information Privacy & Security*, 1:3, 3-17.

Black, K (1994) *Business Statistics: Contemporary Decision Making*, West Publishing Company, Minneapolis, Saint Paul.

Blaxter, L, Hughes, C and Tight, M (2001) *How to Research*, 2nd ed, Open University Press, Buckingham.

Booker, R (2006) "Re-Engineering Enterprise Security", *Computers & Security*, 25:1, 13-17.

Boritz, E, Mackler, E and McPhie, D (1999) "Reporting on Systems Reliability", *Journal of Accountancy*, 188:5, 75-87.

Bowen, P, Chew, E and Hash, J (2007) *Information Guide for Government Executives*, National Institute of Standards and Technology, US Department of Commerce, USA.

Bowerman, BL and O'Connell, RT (2007) *Business Statistics in Practice*, 4th ed, McGraw-Hill, New York.

Brenner, J (2007) "ISO 27001: Risk Management and Compliance", *Risk Management Magazine*, 54:1, 24-29.

Briney, A (2000) "The 2000 Information Security Industry Survey", *Information Security Magazine*, September, 40-68.

Briney, A (2001) "The 2001 Information Security Industry Survey", *Information Security Magazine*, October, 34-47.

Britt, P (2008) "You've Got Mail and Security Breaches", *Information Today*, 25:7, p.1.

Bryman, A (1988) *Quantity and Quality in Social Research*, Contemporary Social Research: 18, Unwin Hyman, London.

Bryman, A (1989) *Research Methods and Organization Studies*, Contemporary Social Research: 20, Unwin Hyman, London.

Bryman, A (2001) *Social Research Methods*, Oxford University Press, New York.

Bryman, A and Bell, E (2003) *Business Research Methods*, Oxford University Press, New York.

Bryman, A and Bell, E (2007) *Business Research Methods*, 2nd ed, Oxford University Press, New York.

Bryman, A and Cramer, D (2001) *Quantitative Data Analysis With SPSS Release 10 for Windows: A Guide for Social Scientists*, Routledge, Hove, East Sussex.

BS 7799-1 (1999) *Information Security Management - Part 1: Code of Practice for Information Security Management*, British Standards Institute, London.

BS 7799-2 (1999) *Information Security Management - Part 2: Specification for Information Security Management*, British Standards Institute, London.

BS 25999 (2008) *Business Continuity Management*, British Standards Institute, London.

BSI (2000) *IT Baseline Protection Manual*, German Federal Information Security Agency, Germany.

Burns, RB (2000) *Introduction to Research Methods*, 4th ed, Sage Publications, London.

Buzzard, K (1999) "Computer Security - What Should You Spend Your Money on?", *Computers & Security*, 18:4, 322-334.

Cannoy, S, Palvia, PC and Schilhavy, R (2006) "A Research Framework for Information Systems Security", *Journal of Information Privacy & Security*, 2:2, 3-29.

Cavusoglu, H, Cavusoglu, H, and Raghunathan, S (2004) "Economics of IT Security Management: Four Important Improvements to Current Security Practices", *Communications of the Association for Information Systems*, vol.14, 65-75.

Cerullo, MJ and Cerullo, V (2005) "Threat Assessment and Security Measures: Justification for Advanced IT Networks", *Information Systems Control Journal*, vol.1, 35-44.

Chandra, A and Calderson, TG (2003) "Toward a Biometric Security Layer in Accounting Systems", *Journal of Information Systems*, 17:2, 51-70.

Chang, AJ and Yeh, Q (2006) "On Security Preparations Against Possible IS Threats Across Industries", *Information Management & Computer Security*, 14:4, 343-360.

Chang, SE and Ho, CB (2006) "Organizational Factors to the Effectiveness of Implementing Security Management", *Industrial Management & Data Systems*, 106:3, 345-361.

Chen, CC, Medlin, BD and Shaw, RS (2008) "A Cross-Cultural Investigation of Situational Information Security Awareness Programs", *Information Management & Computer Security*, 16:4, 360-376.

Chiasson, MW and Davidson, E (2005) "Taking Industry Seriously in Information Systems Research", *MIS Quarterly*, 29:4, 591-605.

Chou, DC, Yen, DC, Lin, B and Chen, PH-L (1999) "Cyberspace Security Management", *Industrial Management & Data Systems*, 99:8, 353-361.

CICA (1998) *Information Technology Control Guidelines*, Canadian Institute of Chartered Accountants, Toronto.

CICA (2005) *20 Questions Directors Should Ask About the Information Technology Aspects of Business Continuity Planning*, The Information Technology Advisory Committee, Canadian Institute of Chartered Accountants, Toronto.

Clarke, E (2007) "Stop Thief", *People Management Magazine*, February, 34-36.

COBIT (2000) *Control Objectives for Information and Related Technologies*, 3rd ed, IT Governance Institute, Information Systems Audit and Control Foundation, USA.

Collette, R and Gentile, M (2006) "The Security Architect: Bridging the Gap Between Business, Technology and Security", *The ISSA Journal*, April, 42-44.

Collis, J and Hussey, R (2003) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, 2nd ed, Palgrave Macmillan, New York.

Conrath, DW and Sharma, RS (1993) "Evaluation Measures for Computer-Based Information Systems", *Computers in Industry*, 21:3, 267-271.

Cooper, DR and Schindler, PS (2006) *Business Research Methods*, 9th ed, McGraw-Hill, Inwin, Boston.

Corbetta, P (2003) *Social Research: Theory, Methods and Techniques*, Sage Publications, London.

Creswell, JW (1998) *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*, Sage Publications, London.

Creswell, JW (2003) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 2nd ed, Sage Publications, London.

Creswell, JW, Clark, VLP, Gutmann, ML and Hanson, WE (2003) Advanced Mixed Research Designs, in Tashakkori, A and Teddlie, C (eds), *Handbook of Mixed Methods in Social & Behavioural Research*, Sage Publications, Thousand Oaks, California.

Daft, R, Sormunen, J and Parks, D (1988) "Chief Executive Scanning, Environmental Characteristics, and Company Performance: An Empirical Study", *Strategic Management Journal*, 9:2, 123-139.

Damiano, P (2008) "Great Expectations: Banks are Challenged to Meet Consumers' Expectations for Online Security", *Bank Systems & Technology*, 45:6, p.14.

Dancey, CP and Reidy, J (2004) *Statistics Without Maths for Psychology: Using SPSS for Windows*, 3rd ed, Pearson, Prentice Hall, England.

D'Arcy, J and Hovav, A (2007) "Deterring Internal Information Systems Misuse", *Communications of the ACM*, 50:10, 113-117.

Da Veiga, A and Eloff, JHP (2007) "An Information Security Governance Framework", *Information Systems Management*, 24:4, 361-372.

David, J (2002) "Policy Enforcement in the Workplace", *Computers & Security*, 21:6, 506-513.

Davis, CE (1997) "An Assessment of Accounting Information Security", *The CPA Journal*, 67:3, 28-34.

DeLone, WH and McLean, ER (1992) "Information Systems Success: The Quest for the Dependent Variable", *Information Systems Research*, 3:1, 60-95.

Denzin, NK (1970) *The Research Act: A Theoretical Introduction to Sociological Methods,* Aldine, Chicago.

De Vaus, D (1996) *Surveys in Social Research*, 4th ed, UCL Press, London.

De Vaus, D (2002) *Surveys in Social Research*, 5th ed, Routledge, London.

Dhillon, G (1999) "Managing and Controlling Computer Misuse", *Information Management & Computer Security*, 7:4, p.171.

Dhillon, G and Backhouse, J (2000) "Information System Security Management in the New Millennium", *Communications of the ACM*, 43:7, 128-131.

Dhillon, G and Moores, S (2001) "Computer Crimes: Theorizing About the Enemy Within", *Computers & Security*, 20:8, 715-723.

Diamantopoulos, A and Schlegelmilch, BB (1997) *Taking the Fear Out of Data Analysis*, Dryden Press, London.

Dill, WR (1958) "Environment as an Influence on Managerial Autonomy", *Administrative Science Quarterly*, 2:4, 409-443.

Dillman, DA (2000) *Mail and Internet Surveys: The Tailored Design Method*, 2nd ed, Wiley, New York.

Dimitriadis, C (2004) "Biometrics: Risks and Controls", *Information Systems Control Journal*, vol.4. Available at: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=21329&TEMPLATE=/ContentManagement/ContentDisplay.cfm

Dodds, R and Hague, I (2004) "Information Security - More Than an IT Issue?", *Chartered Accountants Journal*, 83:11, 56-57.

Doherty, NF and Fulford, H (2005) "Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis", *Information Resources Management Journal*, 18:4, 21-39.

Doherty, NF and Fulford, H (2006) "Aligning the Information Security Policy With the Strategic Information Systems Plan", *Computers & Security*, 25:1, 55-63.

Donaldson, L (2001) *The Contingency Theory of Organisations*, Sage Publications, Thousand Oaks, California.

Down, MP and Sands, RJ (2004) "Biometrics: An Overview of the Technology, Challenges and Control Considerations", *Information Systems Control Journal*, vol.4, 53-56.

Drazin, R and Van de Ven, AH (1985) "Alternative Forms of Fit in Contingency Theory", *Administrative Science Quarterly*, 30:4, 514-539.

DTI (2004a) *Information Security: Protecting Your Business Assets*, The Information Security Policy Team, Department of Trade and Industry, London.

DTI (2004b) *Information Security: A Business Manager's Guide*, The Information Security Policy Team, Department of Trade and Industry, London.

DTI (2004c) *Information Security Breaches Survey (ISBS)*, Department of Trade and Industry, London.

DTI (2006) *Information Security Breaches Survey (ISBS)*, Department of Trade and Industry, London.

DTT (2005) *Global Security Survey*, Global Financial Services Industry Group, Deloitte Touche Tohmatsu, London.

DTT (2006a) *Global Security Survey*, Global Financial Services Industry Group, Deloitte Touche Tohmatsu, London.

DTT (2006b) *Protecting the Digital Assets: The 2006 Technology, Media & Telecommunications Security Survey*, DTT Technology, Media, Telecommunications Industry Group, Deloitte Touche Tohmatsu, London.

DTT (2007) *Global Security Survey, the Shifting Security Paradigm*, Global Financial Services Industry Group, Deloitte Touche Tohmatsu, London.

Ducan, R (1972) "Characteristics of Organisational Environments and Perceived Environmental Uncertainties", *Administrative Science Quarterly*, 17:3, 313-327.

Dutta, A and McCrohan, K (2002) "Management's Role in Information Security in a Cyber Economy", *California Management Review*, 45:1, 67-88.

Easterby-Smith, M, Thorpe, R and Lowe, A (1991) *Management Research: An Introduction*, Sage Publications, London.

Ekenberg, L, Oberoi, Sand Orci, I (1995) "A Cost Model for Managing Information Security Hazards", *Computers & Security*, 14:8, 707-717.

Eloff, MM and Von Solms, SH (2000) "Information Security Management: A Hierarchical Framework for Various Approaches", *Computers & Security*, 19:3, 243-256.

Enisa (2007) *Information Security Awareness Initiatives: Current Practice and the Measurement of Success*, European Network and Information Security Agency, Greece.

Ernst & Young (2005) *Global Information Security Survey 2005: Report on the Widening Gap*, London.

Ernst & Young (2006) *Global Information Security Survey 2006, Achieving Success in a Globalized World: Is Your Way Secure?*, London.

Ernst & Young (2007) *Global Information Security Survey: Achieving a Balance of Risk and Performance*, London.

Eveloff, SH (2005) "Technology", *Pennsylvania CPA Journal*, 76:1, 14-15.

Ewing, J, Falcon, J and McGrane, K (2007) "IT Security: Preventing the March of Madness", *Business Communications Review*, 37:3, 50-53.

Fenrich, K (2008) "Securing Your Control System", *Power Engineering*, 12:2, p.44.

Fielding, J and Gilbert, N (2000) *Understanding Social Statistics*, Sage Publications, London.

Fielding, NG and Lee, RM (1998) *Computer Analysis and Qualitative Research*, Sage Publications, London.

Finne, T (1996) "The Information Security Chain in a Company", *Computers & Security*, 15:4, 297-316.

Finne, T (1998) "A Conceptual Framework for Information Security Management", *Computers & Security*, 17:4, 303-307.

Flick, U (2002) *An Introduction to Qualitative Research*, 2nd ed, Sage Publications, London.

Flowerday, S and Von Solms, R (2005) "Real-Time Information Integrity = System Integrity + Data Integrity + Continuous Assurances", *Computers & Security*, 24:8, 604-613.

Fonseca, F (2007) "Maslow's Pyramid Applied to Continuity Planning", *The ISSA Journal*, May, p.35.

Fontana, A and Frey, JH (2000) The Interview from Structured Questions to Negotiated Text, in Denzin, NK and Lincoln, YS (eds), *Handbook of Qualitative Research*, 2nd ed, Sage Publications, London.

Frankfort-Nachmias, C and Nachmias, D (1992) *Research Methods in the Social Sciences*, 4th ed, Edward Arnold, London.

Freeman, EH (2007) "Holistic Information Security: ISO 27001 and Due Care", *Information Systems Security*, 16:5, 291-294.

Fried, L (1994) "Information Security and New Technology: Potential Threats and Solutions", *Information Systems Management*, 11:3, 57-63.

Frolick, M (2003) "A New Webmaster's Guide to Firewalls and Security", *Information Systems Management*, Winter, 29-34.

Frosdick, S (1997) "The Techniques of Risk Analysis are Insufficient in Themselves", *Disaster Prevention and Management*, 6:3, 165-177.

FSA (2004) *Countering Financial Crime Risks in Information Security: Financial Crime Sector Report,* FSA Risk Review Department, Financial Services Authority, London.

Fulford, H and Doherty, NF (2003) "The Application of Information Security Policies in Large UK Based Organisations: An Exploratory Investigation", *Information Management & Computer Security*, 11:2/3, 106-114.

Furnell, S and Papadaki, M (2008) "Testing our Defences or Defending our Tests: The Obstacles to Performing Security Assessment References", *Computer Fraud & Security,* 2008:5, 8-12.

Gansler, JS and Lucyshyn, W (2005), "Improving the Security of Financial Management Systems: What are We to Do?", *Journal of Accounting and Public Policy*, 24:1, 1-9.

GAO (1998) *Executive Guide - Information Security Management: Learning From Leading Organisations*, Accounting and Information Management Division, General Accounting Office, USA.

GAO (1999) *Information Security Risk Assessment: Practices of Leading Organisations - A Supplement of GAO's May 1998 Executive Guide on Information Security Management*, Accounting and Information Management Division, General Accounting Office, USA.

GAO (2004) *Information Security: Information System Controls at the Federal Deposit Insurance Corporation*, Report to the Board of Directors, Federal Deposit Insurance Corporation, General Accounting Office, USA.

Garcia, A (2006) "Information Security Governance: Setting the Tone at the Top", *The ISSA Journal*, July, p.19.

Garg, A, Curtis, J and Halper, H (2003) "Quantifying the Financial Impact of IT Security Breaches", *Information Management & Computer Security*, 13:2/3, 74-83.

Gaston, SJ (1996) *Information Security: Strategies for Successful Management*, The Canadian Institute of Chartered Accountants, Toronto.

Gerard, G, Hillison, W, and Pacini, C (2004), "What Your Firm Should Know about Identity Theft", *The Journal of Corporate Accounting & Finance*, 15:4, 3-11.

Gerber, JA and Feldman, ER (2002) "Is Your Business Prepared for the Worst?", *Journal of Accountancy*, 193:4, 61-64.

Gerber, M and Von Solms, R (2001) "From Risk Analysis to Security Requirements", *Computers & Security*, 20:7, 577-584.

Gerber, M and Von Solms, R (2005) "Management of Risk in the Information Age", *Computers & Security*, 24:1, 16-30.

Gercek, G and Saleem, N (2005) "Securing Small Business Computer Networks: An Examination of Primary Security Threats and Their Solutions", *Information Systems Security*, 14:3, 18-28.

Ghauri, P and Gronhaug, K (2002) *Research Methods in Business Studies: A Practical Guide*, 2nd ed, Prentice Hall, England.

Gibbs, GR (2002) *Qualitative Data Analysis: Explorations With NVivo*, Open University Press, Buckingham.

Golden, C (2008) "Coming to Terms With End Point Security", *Computer Fraud & Security*, 2008:4, 16-17.

Gomez, JM and Paxmann, S (2006) "Online Security Solutions in the Financial Industry Based on a Commercial Risk Assessment Matrix", *Journal of Information Privacy & Security*, 2:3, 21-41.

Goodhue, DL and Straub, DW (1991) "Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security", *Information & Management*, 20:1, 13-27.

Gordan, ME (2005) *Adopting 7799: Practical, Achievable Security*, White Paper, CyberTrust. Available at: http://www.infosec.co.uk/ExhibitorLibrary/168/Adopting_7799.pdf

Gordon, LA and Loeb, MP (2006) "Budgeting Process for Information Security Expenditures", *Communications of the ACM*, 49:1, 121-125.

Gordon, LA, Loeb, MP, Lucyshyn, W and Richardson, R (2005) *The Tenth Annual CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, San Francisco.

Gordon, LA, Loeb, MP, Lucyshyn, W and Richardson, R (2006) *The Eleventh Annual CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, San Francisco.

Gorge, M (2008) "Data Protection: Why are Organisations Still Missing the Point?", *Computer Fraud & Security*, 2008:6, 5-8.

Goucher, W (2008) "Enabling Secure Behaviour", *Computer Fraud & Security*, 2008:2, 12-14.

Granat, B (1998) "Up in Smoke Security and Information Management Source", *Inform*, 12:1, p.34.

Grance, T, Hash, J, Stevens, M, O'Neal, K and Bartol, N (2003) *Guide to Information Technology Security Services: Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology (NIST), Department of Commerce, USA.

Grant, RM (1998) *Contemporary Strategy Analysis: Concepts, Techniques, Applications*, 3rd ed, Blackwell, Boston.

Green, M (2003) "Securing the System", *Best's Review*, 103:10, p.80.

Greene, JC and Caracelli, VJ (1997) Defining and Describing the Paradigm Issue in Mixed-Method Evaluation, in Greene, JC and Caracelli, VJ (eds), *Advances in Mixed-Method Evaluation: The Challenges and Benefits of Integrating Diverse Paradigms*, Jossey-Bass, San Francisco.

Greenemeier, L (2006), *Ninth Annual Global Security Survey*, InformationWeek, USA.

Guba, EG and Lincoln, YS (1994) Competing Paradigms in Qualitative Research, in Denzin, NK and Lincoln, YS (eds), *Handbook of Qualitative Research*, Sage Publications, London.

Gupta, A and Hammond, R (2005) "Information Systems Security Issues and Decisions for Small Business: An Empirical Examination", *Information Management & Computer Security*, 13:4, 297-310.

Hagen, JM, Albrechtsen, E and Hovden, J (2008) "Implementation and Effectiveness of Organisational Information Security Measures", *Information Management & Computer Security*, 16:4, 377-397.

Hancock, B (2002) "Security Crisis Management - The Basics", *Computers & Security*, 21:5, 397-401.

Hanushek, EA and Jackson, JE (1977) *Statistical Methods for Social Scientists*, Academic Press, New York.

Haugen, S and Selin, JR (1999) "Identifying and Controlling Computer Crime and Employee Fraud", *Industrial Management Data Systems*, 99:8, p.340.

Healey, M (2008) "Top 6 Technologies", *InformationWeek*, 1194, p.39.

Healy, M and Perry, C (2000) "Comprehensive Criteria to Judge Validity and Reliability of Qualitative Research Within the Realism Paradigm", *Qualitative Market Research: An International Journal*, 3:3, 118-126.

Healy, M and Rawlinson, M (1994) Interviewing Techniques in Business and Management Research, in Wass, VJ and Wells, PE (eds), *Principles and Practice in Business and Management Research*, Dartmouth, England.

Henry, L (1997) "A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia", *The Mid-Atlantic Journal of Business*, 33:3, 171-189.

Hicks, M (2004) "Spam Costs, Volumes Soar Despite New Laws", *eWeek*, June. Available at: http://www.accessmylibrary.com/coms2/summary_0286-21590266_ITM

Higgins, HN (1999) "Corporate System security: Towards an Integrated Management Approach", *Information Management & Computer Security*, 7:5, p.217.

Hinde, S (1998) "Recent Security Surveys", *Computers & Security*, 17:3, 207-210.

Hitchings, J (1995) "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology", *Computers & Security*, 14:5, 377-383.

Holland, J and Campbell, J (2005) Context and Challenges for Combining Methods in Development Research, in Holland, J and Campbell, J, (eds), *Methods in Development Research: Combining Qualitative and Quantitative Approaches*, ITDG Publishing, Rugby.

Hollander, M and Wolfe, DA (1999) *Nonparametric Statistical Methods*, 2nd ed, Wiley, New York.

Holmes, A (2006) "The Global State of Information Security 2006; Some Things are Getting Better, Slowly, but Security Practices are Still Immature and, in Some Cases, Regressing", *CIO*, 19:23, p.1.

Hone, K and Eloff, JHP (2002) "Information Security Policy: What Do International Information Security Standards Say?", *Computers & Security*, 21:5, 402-409.

Hong, KS, Chi, YP, Chao, LR and Tang, JH (2003) "An Integrated System Theory of Information Security Management", *Information Management & Computer Security*, 11:5, 243-248.

Hong, KS, Chi, YP, Chao, LR and Tang, JH (2006) "An Empirical Study of Information Security Policy on Information Security Elevation in Taiwan", *Information Management & Computer Security*, 14:2, 104-115.

Huang, SM, Lee, CL and Kao, AC (2006) "Balancing Performance Measures for Information Security Management: A Balanced Scorecard Framework", *Industrial Management & Data Systems*, 106:2, 242-255.

Hunt, S (2006) "Imagine - More Security Value, Less Money", *Security*, 43:7, p.14.

Hunter, A and Brewer, J (2003) Multimethod Research in Sociology, in Tashakkori, A and Teddlie, C (eds), *Handbook of Mixed Methods in Social & Behavioural Research*, Sage Publications, Thousand Oaks, California.

Hunton, JE (2002) "Back Up Your Data to Survive a Disaster", *Journal of Accountancy*, 193:4, 65-69.

Hussey, J and Hussey, R (1997) *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, Palgrave, New York.

Icove, D, Seger, K and Vonstorch, W (1999) *Computer Crime - A Crimefighter's Handbook,* O'Reilly & Associates, Sebastopol.

IFAC (1998) *Managing Security of Information*, Information Technology Committee, International Federation of Accountants, New York.

IFAC (2002) *E-Business and the Accountant*, Information Technology Committee, International Federation of Accountants, New York.

Im, GP and Baskerville, RL (2005) "A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error", *Database for Advances in Information Systems*, 36:4, 68-79.

ISACA (2005) *Critical Elements of Information Security Program Success*, Information Systems Audit and Control Association.

ISACF (2001) *Information Security Governance: Guidance for Boards of Directors and Executive Management,* IT Governance Institute, Information Systems Audit and Control Foundation.

ISF (2005) *The Standard of Good Practice for Information Security*, Information Security Forum, London.

ISF (2007) *The Standard of Good Practice for Information Security*, Information Security Forum, London.

ISO/IEC TR 13335-1 (1996) *Information Technology: Guidelines for the Management of IT Security - Part 1: Concepts and Models for IT Security*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC TR 13335-2 (1997) *Information Technology: Guidelines for the Management of IT Security - Part 2: Managing and Planning IT Security*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC TR 13335-3 (1998) *Information Technology: Guidelines for the Management of IT Security - Part 3: Techniques for the Management of IT Security*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC TR 13335-4 (2000) *Information Technology: Guidelines for the Management of IT Security - Part 4: Selection of Safeguards*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC TR 13335-5 (2003) *Information Technology: Guidelines for the Management of IT Security - Part 5: Safeguards for External Connections*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC 15408-1 (1999) *Information Technology: Security Techniques, Evaluation Criteria for IT Security - Part 1: Introduction and General Model*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC 17799 (2005a) *Information Technology - Security Techniques - Code of Practice for Information Security Management*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ISO/IEC 27001 (2005b) *Information Technology - Security Techniques - Information Security Management Systems - Requirements*, International Organisation of Standardisation, ISO/IEC, Switzerland.

ITSEC (1990) *Information Technology Security Evaluation Criteria*: Harmonised Criteria of France, Germany, Netherlands and the UK, Department of Trade and Industry, London.

Jarvenpaa, SL and Ives, B (1990) "Information Technology and Corporate Strategy: A View from the Top", *Information Systems Research*, 1:4, 351-375.

Jenkins, B and Pinkney, A (1978) *An Audit Approach to Computers: a New Practice Manual*, Institute of Chartered Accountants in England and Wales, London.

Johnson, B and Turner, LA (2003) Data Collection Strategies in Mixed Methods Research, in Tashakkori, A and Teddlie, C (eds), *Handbook of Mixed Methods in Social & Behavioural Research*, Sage Publications, Thousand Oaks, California.

Jones, A (2008) "The Changing Nature of Malicious Attacks", *Computer Fraud & Security*, 2008:6, 15-17.

Jones, DA (2003) *"Does Do-It-Yourself Security Always Make Sense?"*, Information Risk Management Team, KPMG, London.

Joyce, M (2008) "The Challenges and Future of Biometric-Based Security Systems", *Internal Auditing*, 23:2, p.14.

Jung, B, Han, I and Lee, S (2001) "Security Threats to Internet: A Korean Multi-Industry Investigation", *Information & Management*, 38:8, 487-498.

Kabay, ME (1996) *The NCSA Guide to Enterprise Security*, McGraw-Hill, New York.

Kadam, AW (2007) "Information Security Policy Development and Implementation", *Information Systems Security*, 16:5, 246-256.

Kankanhalli, A, Teo, HH, Tan, BCY and Wei, KK (2003) "An Integrative Study of Information Systems Security Effectiveness", *International Journal of Information Management*, 23:2, 139-154.

Karabacak, B and Sogukpinar, I (2006) "A Quantitative Method for ISO 17799 Gap Analysis", *Computers & Security*, 25:6, 413-419.

Karyda, M, Kiountouzis, E and Kokolakis, S (2005) "Information Systems Security Policies: A Contextual Perspective", *Computers & Security*, 24:3, 246-260.

Katz, D (2000) "Elements of Comprehensive Security Solution", *Health Management Technology*, 21:6, 12-16.

Kelle, U, Prein, G and Bird, K (1995) *Computer-Aided Qualitative Data Analysis: Theory, Methods and Practice*, Sage Publications, London.

Keller, S, Powell, A, Horstmann, B, Predmore, C and Crawford, M (2005) "Information Security Threats and Practices in Small Business", *Information Systems Management*, 22:2, 7-19.

Kieke, R (2006) "Survey Shows High Number of Organisations Suffered Security Breach in Past Year", *Journal of Health Care Compliance*, 8:5, p.49.

King, WR (1994) "Organisational Characteristics and Information Systems Planning: An Empirical Study", *Information Systems Research*, 5:2, 75-109.

Kleinfeld, A (2006) "Measuring Security", *EDPACS*, 34:4, 10-16.

Knapp, K, Marshall, T, Rainer, K, and Morrow, D (2006) "The Top Security Issues Facing Organisations: What Can Government Do to Help?", *Information Systems Security*, 15:4, 51-58.

Kotulic, AG and Clark, JG (2004) "Why There Aren't More Information Security Research Studies", *Information & Management*, 41:5, 597-607.

Kouns, B (2007) "The Real Power of ISO 27001 Certification", *The ISSA Journal*, February, 18-19.

KPMG (1998) *The Information Security Survey 1998*, Information Risk Management Group, KPMG, London.

KPMG (2006) The *Information Security Survey 2006: Six Important Signals*, Information Risk Management Group, KPMG, Amsterdam.

KPMG (2008) *European Identity & Access Management Survey: Status and Maturity of Identity and Access Management Projects in European Organisations*, IT Advisory, KPMG, Amsterdam.

Kritzinger, E and Smith, E (2008) "Information Security Management: An Information Security Retrieval and Awareness Model for Industry", *Computers & Security*, 27:5/6, 224-231.

Kros, JR, Foltz, CB and Metcalf, CL (2005) "Assessing & Quantifying the Loss of Network Intrusion", *The Journal of Computer Information Systems*, 42:2, 36-43.

Kruger, HA and Kearney, WD (2006) "A Prototype for Assessing Information Security", *Computers & Security*, 25:4, 289-296.

Kvale, S (1996) *Interviews: An Introduction to Qualitative Research Interviewing*, Sage Publications, Thousand Oaks, California.

Kvanli, AH, Guynes, CS and Pavur, RJ (1996) *Introduction to Business Statistics: A Computer Integrated Data Analysis Approach*, 4th ed, West Publishing, St. Paul.

Kwok, L and Longley, D (1999) "Information Security Management and Modelling", *Information Management & Computer Security*, 7:1, p.30.

Labovitz, S (1970) "The Assignment of Numbers to Rank Order Categories" *American Sociological Review*, 35:3, 515-524.

Landry, M (2006) "Contingency Planning: A Process", *The ISSA Journal*, July, 26-29.

Leach, J (2003) "Improving User Security Behaviour", *Computers & Security*, 22:8, 685-692.

Lee, J and Lee, Y (2002) "A Holistic Model of Computer Abuse Within Organisations", *Information Management & Computer Security*, 10: 2/3, 57-63.

Lee, S, Luthans, F and Olson, DL (1982) "A Management Science Approach to Contingency Models of Organizational Structure", *Academy of Management Journal*, 25:3, 553-566.

Lee, S, Yoon, S, and Kim, J (2008) "The Role of Pluralistic Ignorance in Internet Abuse", *The Journal of Computer Information Systems*, 48:3, 38-43.

Levin, RI and Rubin, DS (1994) *Statistics for Management*, 6th ed, Prentice Hall, New Jersey.

Lewins, A and Silver, C (2007) *Using Software in Qualitative Research: A Step-by-Step Guide*, Sage Publications, London.

Lewis, GJ and Stewart, N (2003) "The Measurement of Environmental Performance: An Application of Ashby's Law", *Systems Research and Behavioural Science*, 20:1, 31-52.

Lichtenstein, S (1996) "Factors in the Selection of a Risk Assessment Method", *Information Management & Computer Security*, 4:4, 20-25.

Lin, PP (2006) "Systems Security Threats and Controls", *The CPA Journal*, 76:7, 58-66.

Lindberg, RS (2006) "Nimble Risk Management", *The ISSA Journal*, August, 12-15.

Lindup, KR (1995) "A New Model for Information Security Policies", *Computers & Security*, 14:8, 691-695.

Lindup, KR (1996) "The Role of Information Security in Corporate Governance", *Computers & Security*, 15:6, 477-485.

Lineman, DJ (2005) "The New ISO 17799: 2005. Security Policy Implications for Business", *Information Shield.* Available at: http://www.informationshield.com/papers/SecurityPolicyAndIso17799.pdf

Loch, KD, Carr, HH and Warkentin, ME (1992) "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly*, 16:2, 173-186.

Ma, Q, Johnston, AC and Pearson, JM (2008) "Information Security Management Objectives and Practices: a Parsimonious Framework", *Information Management & Computer Security*, 16:3, 251-270.

Ma, Q and Pearson, JM (2005) "ISO 17799: Best Practices in Information Security Management?", *Communications of the Association for Information Systems*, 15, 577-591.

Magklaras, G, Furnell, S and Brooke, P (2006) "Towards an Insider Threat Prediction Specification Language", *Information Management & Computer Security*, 14:4, 361-381.

Manrique, LG (2005) "The Enemy Within", *Accounting Technology*, Spring, 4-5.

Mattsson, U (2007) "Defending the Database", *Network Security*, 2007:7, 14-17.

May, T (1997) *Social Research Methods: Issues, Methods and Process*, Open University Press, Buckingham.

Messmer, E (2008) "Six Burning Questions about Security", *Network World*, 25:23, p.32.

Miles, MB and Huberman, AM (1994) *Qualitative Data Analysis*, 2nd ed, Sage Publications, London.

Mitchell, RB and Jones, T (2002) "Policies Controlling Use of Computer Based Resources in Small Businesses", *The Journal of Computer Information Systems,* 42:4, 77-83.

Mitchell, RC, Marcella, R and Baxter, G (1999) "Corporate Information Security Management", *New Library World*, 100:1150, p.213.

Mitnick, K (2003) "Are You the Weak Link?", *Harvard Business Review*, April, 18-20.

Mitropoulos, S, Patsos, D and Douligeris, C (2007) "Incident Response Requirements for Distributed Security Information Management Systems", *Information Management & Computer Security,* 15:3, 226-240.

Moses, R (1992) Risk Analysis and Management, in Jackson, KM and Hruska, J (eds), *Computer Security Reference Book*, Butterworth Heinemann, Oxford.

Moulds, R (2008) "Protecting Cardholder Data With Encryption", *Computer Fraud & Security*, 2008:6, 14-15.

Mouratidis, H, Jahankhani, H, and Nkhoma, MZ (2008) "Management Versus Security Specialists: An Empirical Study on Security Related Perceptions", *Information Management & Computer Security*, 16:2, 187-205.

Myler, E and Broadbent, G (2006) "ISO 17799: Standard for Security", *Information Management Journal,* 40:6, 43-52.

NCC (2007) *Security and Information Risk Survey: The View of UK Risk Professionals*, National Computing Centre, Manchester.

Neuman, WL (2000) *Social Research Methods: Qualitative and Quantitative Approaches*, 4th ed, Allyn & Bacon, Boston.

NIST 800-14 (1996) *Generally Accepted Principles and Practices for Security Information Technology Systems (GAASP)*, National Institute of Standards and Technology, Department of Commerce, USA.

NIST 800-30 (2002) *Risk Management Guide for Information Technology System*, National Institute of Standards and Technology, Department of Commerce, USA.

NIST 800-53 (2005) *Recommended Security Controls for Federal Information Systems: Information Security, Technology Administration*, National Institute of Standards and Technology, Department of Commerce, USA.

Nosworthy, JD (2000) "A Practical Risk Analysis Approach: Managing BCM Risk", *Computers & Security*, 19:7, 596-614.

Nota, P (1988) "Control Your Processing Power and Protect Your Information", *Management Accounting*, 66:4, 40-42.

NSTISSAM INFOSEC/1-99 (1999) *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Committee, National Security Agency, USA.

NSTISSI 4009 (2000) *National Information Systems Security Glossary* (INFOSEC), National Security Telecommunications and Information Systems Committee, National Security Agency, USA.

Nyanchama, M (2005) "Enterprise Vulnerability Management and its Role in Information Security Management", *Information Systems Security*, 14:3, 29-56.

OECD (1992) *Guidelines for the Security of Information Systems: Towards a Culture of Security*, Organisation for Economic Cooperation and Development, Paris.

OECD (2002) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, Organisation for Economic Co-operation and Development, Paris.

O'Hanley, R (2004) "Maintaining Security and Privacy Requires Getting Back to Basics", *Information Systems Security,* 13:5, p.2.

Olnes, J (1994) "Development of Security Policies", *Computers & Security*, 13:8, 628-636.

Onions, R (2006) Auditing in United Kingdom (UK) Small and Medium Enterprises (SMEs), *PhD Thesis*, University of Salford, UK.

Onwuegbuzie, AJ and Leech, NL (2005) "On Becoming a Pragmatic Researcher: The Importance of Combining Quantitative and Qualitative Research Methodologies", *International Journal of Social Research Methodology*, 8:5, 375-387.

Oppenheim, AN (1966) *Questionnaire Design and Attitude Measurement*, Gower, London.

Oppenheim, AN (1992) *Questionnaire Design, Interviewing and Attitude Measurement*, 2nd ed, Continuum, London.

Orlikowski, WJ and Baroudi, JJ (2002) Studying Information Technology in Organisations: Research Approaches and Assumptions, in Myers, MD and Avision, D (eds), *Qualitative Research in Information Systems*, Sage Publications, London.

Osborne, K (1998) "Auditing the IT Security Function", *Computers & Security*, 17:1, 34-41.

Pallant, J (2007) *SPSS Survival Manual: A Step by Step Guide to Data Analysis Using SPSS Version 15*, 3rd ed, Open University Press, McGraw-Hill, Maidenhead.

Parker, DB (1981) *Computer Security Management*, Reston Publishing, Virginia.

Parker, DB (1984) "The Many Faces of Data Vulnerability", *IEEE Spectrums*, 46-49.

Parker, DB (1991) "Restating the Foundation of Information Security", *Proceeding of 14th National Computer Security Conference*, Washington, 480-493.

Patton, MQ (1990) *Qualitative Evaluation and Research Methods*, 2nd ed, Sage Publications, California.

Peltier, T (2001) *Information Security Risk Analysis*, Auerbach Publications, Boca Raton, FL.

Peltier, T (2005) "Implementing an Information Security Awareness Program", *Information Systems Security*, 14:2, 37-49.

Peterson, RA (2000) *Constructing Effective Questionnaires*, Sage Publications, Thousand Oaks, California.

Pfleeger, CP and Pfleeger, SL (2007) *Security in Computing*, 4th ed, Prentice Hall, Upper Saddle River, NJ.

Pironti, JP (2005) "Key Elements of an Information Security Program", *Information Systems Control Journal*, vol.1. Available at: http://www.itgi.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=23540

Poore, RS (1999) *Generally Accepted System Security Principles*, GASSP Committee, International Information Security Foundation, USA.

Post, G and Kagan, A (2007) "Evaluating Information Security Tradeoffs: Restricting Access can Interfere With User Tasks", *Computers & Security*, 26: 3, 229-237.

Post, RS, Kingsbury, AA and Schachtsieh, DA (1994) *Security Administration: An Introduction to the Protective Services*, 4th ed, Butterworth - Heinemann, MA.

Posthumus, S and Von Solms, R (2004) "A Framework for the Governance of Information Security", *Computers & Security*, 23:8, 638-646.

Punch, KF (1998) *Introduction to Social Research: Quantitative & Qualitative Approaches*, Sage Publications, London.

Purpura, P (2002) *Security and Loss Prevention: An Introduction,* 4th ed, Butterworth-Heinemann, Boston.

Qureshi, AA and Siegel, JG (1997) "The Accountant and Computer Security", *The National Public Accountant*, 42:3, 12-40.

Rainer, KR, Charles, AS and Houston, HC (1991) "Risk Analysis for Information Technology", *Management Information Systems*, 8:1, 129-147.

Rainer, K, Marshall, T, Knapp, K, and Montgomery, G (2007) "Do Information Security Professionals and Business Managers View Information Security Issues Differently?", *Information Systems Security*, 16:2, 100-108.

Richardson, R (2007) *The 12th Annual CSI Computer Crime and Security Survey*, Computer Security Institute, San Francisco.

Richardson, R (2008) *The 13th Annual CSI Computer Crime and Security Survey*, Computer Security Institute, San Francisco.

Robson, C (1993) *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, Blackwell, Oxford, UK.

Rocco, TS, Bliss, LA, Gallagher, S and Prez-Prado, A (2003) "Taking the Next Step: Mixed Methods Research in Organisational Systems", *Information Technology, Learning, and Performance Journal*, 21:1, 19-29.

Rodetis, S (1999) "Can Your Business Survive the Unexpected?", *Journal of Accountancy*, 187:2, 27-32.

Romney, MB and Steinbart, PJ (2003) *Accounting Information Systems*, 9th ed, Prentice Hall, New Jersey.

Ross, J and Weill, P (2002) "Six IT Decisions Your IT People Shouldn't Make", *Harvard Business Review*, November, 84-91.

Ryan, B, Scapens, RW and Theobald, M (1992) *Research Method and Methodology in Financial Accounting*, Academic Press, London.

Ryan, J and Ryan, D (2006) "Expected Benefits of Information Security Investments", *Computers & Security*, 25:8, 579-588.

Ryan, SD and Bordoloi, B (1997) "Evaluating Security Threats in Mainframe and Client/Server Environments", *Information & Management*, 32:3, 137-146.

Saleh, MS, Alrabiah, A and Bakry, SH (2007) "A STOPE Model for the Investigation of Compliance With ISO 17799-2005", *Information Management & Computer Security*, 15:4, 283-294.

Sarantakos, S (2005) *Social Research*, 3rd ed, Palgrave Macmillan, New York.

Saunders, M, Lewis, P and Thornhill, A (2007) *Research Methods for Business Students*, 4th ed, Prentice Hall, Harlow.

Schneier, B (2001) "Managed Security Monitoring: Network Security for the 21st Century", *Computers & Security*, 20:6, 491-503.

Schultz, E (2005) "The Human Factor in Security", *Computers & Security*, 24:6, 425-426.

Scott, JE (1995) "The Measurement of Information Systems Effectiveness: Evaluating a Measuring Instrument", *DATA BASE Advances*, 26:1, 43-61.

Scott, RW (2008) "Taking the Risk Out of IT", *Accounting Technology*, 24:4, 25-28.

Sekaran, U (2003) *Research Methods for Business: A Skill Building Approach*, 4th ed, John Wiley & Sons, New York.

Shaw, G and Daniels, S (2002) "Managing System Risk", *Management Services*, 46:9, 14-15.

Sherer, SA and Alter, S (2004) "Information System Risks and Risk Factors: Are they Mostly about Information Systems?", *Communications of the Association for Information Systems*, vol.14, 29-64.

Sherstobitoff, R and Bustamante, P (2007) "You Installed Internet Security on Your Network: Is Your Company Safe?", *Information Systems Security*, 16:4, 188-194.

Shih, SC and Wen, HJ (2005) "E-Enterprise Security Management Life Cycle", *Information Management & Computer Security*, 13:2, 121-134.

Sieber, SD (1973) "The Integration of Fieldwork and Survey Methods", *American Journal of Sociology*, 78:6, 1335-1359.

Siegel, S and Castellan, J (1988) *Nonparametric Statistics for the Behavioral Sciences*, 2nd ed, McGraw-Hill, USA.

Singh, K (2007) *Qualitative Social Research Methods*, Sage Publications, Thousand Oaks, California.

Siponen, M (2000) "A Conceptual Foundation for Organisational Information Security Awareness", *Information Management & Computer Security*, 8:1, 31-41.

Siponen, M (2006) "Information Security Standards Focus on the Existence of Process, Not its Content", *Communications of the ACM*, 49:8, 97-100.

Smith, GE (2004) "Information Security: Is Your Auditing Up to the Task?", *The Journal of Corporate Accounting & Finance*, 15:4, 13-19.

Smith, M (2003) *Research Methods in Accounting*, Sage Publications, London.

Smith, S and Jamieson, R (2006) "Determining Key Factors in E-Government Information System Security", *Information Systems Management*, 23:2, 23-32.

Sprent, P (1989) *Applied Nonparametric Statistical Methods*, Chapman and Hall, London.

Spurling, P (1995) "Promoting Security Awareness and Commitment", *Information Management & Computer Security*, 3:2, 20-26.

Steele, S and Wargo, C (2007) "An Introduction to Insider Threat Management", *Information Systems Security*, 16:1, 23-33.

Steinke, G (1997) "A Task-Based Approach to Implementing Computer Security", *The Journal of Computer Information Systems*, 38:1, 47-54.

Stiles, J (2003) "A Philosophical Justification for a Realist Approach to Strategic Alliance Research", *Qualitative Market Research: An International Journal*, 6:4, 263-271.

Straub, DW (1986) "Computer Abuse and Computer Security: Update on an Empirical Study", *Security, Audit, and Control Review*, 4:2, 21-31.

Straub, DW and Welke, RJ (1998) "Coping With Systems Risk: Security Planning Models for Management Decision Making", *MIS Quarterly*, 22:4, 441-469.

Swartz, N (2007) "Protecting Information from Insiders", *Information Management Journal*, 41:3, p.20.

Sweren, B (2006) "ISO 17799: A Closer Look", *The ISSA Journal*, January, 16-19.

Tchankova, L (2002) "Risk Identification: Basic Stage in Risk Management", *Environmental Management and Health*, 13:3, 290-297.

TCSEC (1985) *Trusted Computer Security Evaluation Criteria*, Department of Defence, Washington.

Teddlie, C and Tashakkori, A (2003) Major Issues and Controversies in the Use of Mixed Methods in the Social and Behavioural Sciences, in Tashakkori, A and Teddlie, C (eds), *Handbook of Mixed Methods in Social & Behavioural Research*, Sage Publications, Thousand Oaks, California.

Theoharidou, M, Kokolakis, S, Karyda, M and Kiountouzis, E (2005) "The Insider Threat to Information Systems and Effective of ISO 17799", *Computers & Security*, 24:6, 472-484.

Thomson, ME and Von Solms, R (1998) "Information Security Awareness: Educating Your Users Effectively", *Information Management & Computer Security*, 6:4, 167-173.

Thorp, C (2004) "Implementing ISO17799: Pleasure or Pain?", *Information Systems Control Journal*, vol.4. Available at: http://www.itgi.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=21318

Tracy, R (2007) "IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards", *Information Systems Security*, 16:2, 114-122.

Trcek, D (2003) "An Integral Framework for Information System Security Management", *Computers & Security*, 22:4, 337-360.

Trites, G and Lavigne, A (2006) "Top Tech Issues", *CA Magazine*, 139:7, 26-33.

Tryfonas, T, Kiountouzis, E and Polymenakou, A (2001) "Embedding Security Practices in Contemporary Information Systems Development Approaches", *Information Management & Computer Security*, 9:4, 183-197.

Tsiakis, T and Stephanides, G (2005) "The Economic Approach of Information Security", *Computers & Security*, 24:2, 105-108.

Tsohou, A, Karyda, M, Kokolakis, S, and Kiountouzis, E (2006) "Formulating Information Systems Risk Management Strategies Through Cultural Theory", *Information Management & Computer Security*, 14:3, 198-217.

Tushman, ML and Nadler, DA (1978), "Information Processing as an Integrating Concept in Organisational Design", *The Academy of Management Review*, 3:3, 613-624.

Vael, M and Neyer, VD (2006) "BCM Mismanagement", *The ISSA Journal*, August, 30-33.

Vermeulen, C and Von Solms, R (2002) "The Information Security Management Toolbox-Taking the Pain Out of Security Management", *Information Management & Computer Security*, 10:3, 119-125.

Vidalis, S and Kazmi, Z (2007) "Security Through Deception", *Information Systems Security*, 16:1, 34-41.

Villarroel, R, Fernandez-Medina, E, and Piattini, M (2005) "Secure Information Systems Development: A Survey and Comparison", *Computers & Security*, 24:4, 308-321.

Von Solms, B (2000) "Information Security - The Third Wave?", *Computers & Security*, 19:7, 615-620.

Von Solms, B (2001) "Information Security - A Multidimensional Discipline", *Computers & Security*, 20:6, 504-508.

Von Solms, B (2005) "Information Security Governance - Compliance Management vs Operational Management", *Computers & Security*, 24:6, 443-447.

Von Solms, B (2006) "Information Security - The Fourth Wave", *Computers & Security*, 25:3, 165-168.

Von Solms, B and Von Solms, R (2004) "The 10 Deadly Sins of Information Security Management", *Computers & Security*, 23:5, 371-376.

Von Solms, R (1996) "Information Security Management: The Second Generation", *Computers & Security*, 15:4, 281-288.

Von Solms, R (1998) "Information Security Management (1): Why Information Security is so Important", *Information Management & Computer Security*, 6:4,174-177.

Von Solms, R (1998) "Information Security Management (3): the Code of Practice for Information Security Management (BS 7799)", *Information Management & Computer Security*, 6:5, 224-225.

Von Solms, R (1999) "Information Security Management: Why Standards are Important", *Information Management & Computer Security*, 7:1, 50-57.

Vroom, C and Von Solms, R (2004) "Towards Information Security Behavioural Compliance", *Computers & Security*, 23:3, 191-198.

Walker, ST (1985) "Network Security Overview", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, 62-76.

Wang, G (2005) "Strategies and Influence for Information Security", *Journal Online*. Available at: http://www.isaca.org/Template.cfm?Section=JOnline&Template=/ContentManagement/ContentDisplay.cfm&ContentID=23548

Ward, P and Smith, CL (2002) "The Development of Access Control Policies for Information Technology Systems", *Computers & Security*, 21:4, 356-371.

Warigon, S (1999) "Preparing and Auditing an IS Security Incident-Handling Plan", *The EDP Audit, Control and Security Newsletter*, 26:10, 1-13.

Wass, VJ (1994) Minimizing and Managing Bias in a Mail Survey: A Study of Redundant Miners, in Wass, VJ and Wells, PE (eds), *Principles and Practice in Business and Management Research*, Dartmouth, Aldershot.

Wass, VJ and Wells, PE (1994) Research Methods in Action: An Introduction, in Wass, VJ and Wells, PE (eds), *Principles and Practice in Business and Management Research*, Dartmouth, Aldershot.

Webb, S (2000) "Crimes and Misdemeanours: How to Protect Corporate Information in the Internet Age", *Computers & Security,* 19:2, 128-132.

Weitzman, EA (2000) Software and Qualitative Research, in Denzin, NK and Lincoln, YS (eds), *Handbook of Qualitative Research*, 2nd ed, Sage Publications, London.

White, GW and Pearson, SJ (2001) "Controlling Corporate E-Mail, PC Use and Computer Security", *Information Management & Computer Security*, 9:2/3, 88-92.

Whitman, ME (2003) "Enemy at the Gate: Threats to Information Security", *Communications of the ACM*, 46:8, 91-95.

Whitman, ME (2004) "In Defence of the Realm: Understanding the Threats to Information Security", *International Journal of Information Management*, 24:1, 43-57.

Whitman, ME and Mattord, HD (2003) *Principles of Information Security,* Course Technology, 153-90.

Whitten, D (2008) "The Chief Information Security Officer: An Analysis of the Skills Required for Success", *The Journal of Computer Information Systems*, 48:3, 15-19.

Wiant, TL (2005) "Information Security Policy's Impact on Reporting Security Incidents", *Computers & Security*, 24:6, 448-459.

Wilkinson, JW (1989) *Accounting Information Systems: Essential Concepts and Applications*, John Wiley & Sons, USA.

Williams, P (1995) "Safe, Secure and up to Standard", *Accountancy*, 115:1220, p.60.

Willison, R (2006) "Understanding the Offender/Environment Dynamic for Computer Crimes", *Information Technology & People*, 19:2, 170-186.

Willison, R and Backhouse, J (2006) "Opportunities for Computer Crime: Considering Systems Risk from a Criminological Perspective", *European Journal of Information Systems*, 15:4, 403-414.

Wilson, M (1996) Asking Questions, in Sapsford, R and Jupp, V (eds), *Data Collection and Analysis*, Sage Publications, London.

Wood, CC (1997) "Policies Alone Do Not Constitute a Sufficient Awareness Effort", *Computer Fraud & Security*, 1997:12, 14-19.

Wood, CC (1995) "Writing InfoSec Policies", *Computers & Security*, 14:8, 667-674.

Wood, CC and Banks, WW (1993) "Human Error: An Overlooked but Significant Information Security Problem", *Computers & Security*, 12:1, 51-60.

Woodman, P (2007) *The Chartered Management Institute's 2007 Business Continuity Management Survey*, Chartered Management Institute, London.

Woodward, D (2000) "Smart Security", *The British Journal of Administrative Management*, January/February, 18, 22-23.

Wright, S (2006) "Measuring Security Effectiveness With ISO 27001", *The ISSA Journal*, September, 34-37.

Yang, SM, Yang, MH and Wu, JTB (2005) "The Impacts of Establishing Enterprise Information Portals on E-Business Performance", *Industrial Management & Data Systems*, 105:3, 349-368.

Yeh, Q and Chang, A (2007) "Threats and Countermeasures for Information System Security: A Cross-Industry Study", *Information & Management*, 44:5, 480-491.

Zambroski, R (2006) "E-Mail Security for Small Businesses", *The CPA Journal*, 76:7, p.51.

Zhou, L, Vasconcelos, A and Nunes, M (2008) "Supporting Decision Making in Risk Management Through an Evidence-Based Information Systems Project Risk Checklist", *Information Management & Computer Security*, 16:2, 166-186.

Zikmund, WG (2000) *Business Research Methods*, 6th ed, Dryden Press, Harcourt College, Orlando, FL.

Appendix 1
Covering Letter and the Questionnaire

Date

The IT Manager

Dear Sir / Madam

I am a full-time PhD student in the Accounting and Finance Section at Cardiff Business School, Cardiff University. I am currently conducting a research for my PhD thesis under the supervision of Professors Roy Chandler and Maurice Pendlebury.

The objective of my research is to evaluate the nature of accounting information systems currently used in UK firms and to investigate the security threats facing these systems and the security controls employed by firms to reduce such threats.

You have been selected to be one of the respondents of the attached questionnaire since your firm is listed on the London Stock Exchange. The questionnaire aims to obtain your opinions regarding the security of the accounting information system in your firm, the security threats facing this system and the security controls employed to reduce security threats. I would be extremely grateful if you could please spare me a few minutes of your valuable time by completing the questionnaire. Your opinions are extremely important to me.

I confirm that the information and opinions provided in the questionnaire will be treated as strictly confidential and will be used only for the purpose of academic research. Under no circumstances will any information be disclosed that will identify respondents and their firms.

Thank you very much for your co-operation, time and support. Please kindly return your completed questionnaire in the "Free Post" envelope provided.

Yours faithfully

Nancy Ibrahim Riad
PhD Student
Cardiff Business School
Aberconway Building
Colum Drive
Cardiff CF10 3EU
E-mail: RiadNI@cardiff.ac.uk
or riadnancy@yahoo.com
Telephone: 078 94 54 93 24

Questionnaire on the Security of Accounting Information Systems

Conducted by
Nancy Ibrahim Riad
PhD Student in Accounting

Under the Supervision of
Professor Roy Chandler and
Professor Maurice Pendlebury
Cardiff Business School
Cardiff University
UK

This questionnaire consists of 4 sections. Please answer all questions in all sections by ticking the appropriate box or bracket, or by providing other relevant information.

Section 1: The management framework of the accounting information system (AIS) security

This section aims to collect your opinions concerning the management framework of the AIS security within your company i.e. security policy, training and awareness program, risk assessment, incident handling, standards and certification, and the AIS security effectiveness.

1.1 The AIS security policy:

1.1.1 Does your company have a written security policy covering its AIS?

Yes	No	Don't know

1.1.2 If yes, approximately how often is this policy updated?

Less frequently than every 3 years	Every 3 years	Every 2 years	Every year	Every 6 months	Don't know

Other, please specify .....

1.2 Training and awareness program:

1.2.1 Does your company have a formal AIS security awareness and training program for its management team, employees and other users?

	Yes	No	Don't know
Managers			
Employees			
Other users			

1.2.2 Please indicate your level of agreement with the following statements:

Statements	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Your company communicates security awareness issues to its managers and employees regularly					
Your company communicates security awareness issues to its managers and employees in response to specific incidents					
Your company supplies its managers and employees with security awareness materials e.g. staff handbook, brochures, posters, intranet pages					
Your company conducts regular testing of the security awareness					

1.3 Risk assessment:

1.3.1 Does your company have an AIS risk assessment program?

Yes	No	Don't know

1.3.2 If yes, approximately how often does your company undertake this risk assessment for its AIS security?

Less frequently than every 3 years	Every 3 years	Every 2 years	Every year	Every 6 months	Don't know

Other, please specify .....

1.3.3 Please indicate the extent to which you agree or disagree with the following statements regarding the risk assessment activities within your company:

Statements	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Risks are assessed and threats to the AIS security are identified regularly					
Controls are defined and provide sufficient protection against threats					
Assets are identified and ranked by their value, sensitivity and criticality to the company					
The company undertakes risk assessment when a significant change in the company's environment occurs					

1.4 Incident handling, disaster recovery and business continuity plan:

1.4.1 Has your company experienced any AIS security incidents in the last year?

Yes	No	Don't know

1.4.2 If yes, what is the average number of security incidents your company experienced in the last year?

1-5	6-10	11-15	More than 15	Don't know

1.4.3 If yes, what was the worst security incident faced by your company in the last year?
Please specify .....
.....

1.4.4 Does your company have formal security incident handling procedures?

Yes	No	Don't know

1.4.5 How long did it take to restore normal business operations after the worst security incident?

A day	Between a day and a week	Between a week and a month	More than a month	Don't know

1.4.6 After a security incident, what actions are undertaken by the company to reduce future incidents?

- Updating the security policy [ ]
- Improving security awareness and training at all levels [ ]
- Improving the back-up system [ ]
- Improving the disaster recovery and business continuity plan [ ]
- Updating the detection software [ ]
- Undertaking security audit [ ]
- Allocating sufficient budget and resources to security [ ]
- No actions were undertaken [ ]
- Other, please specify [ ]

1.4.7 Does your company have a formal business continuity plan?

Yes	No	Don't know

1.4.8 If yes, approximately how often does your company test and review the business continuity plan?

Less frequently than every 3 years	Every 3 years	Every 2 years	Every year	Every 6 months	Don't know

Other, please specify .....

1.5 Security budget:

1.5.1 Does your company have a separate budget for security?

Yes	No	Don't know

1.5.2 If yes, approximately what percentage of your company's overall security budget was spent on AIS security in the last year?

None	Less than 1%	1%-5%	6%-10%	11%-15%	16%-20%	More than 20%	Don't know

1.5.3 Please rank your company's top 3 areas of spending on AIS security where 1 represents the most important:

Spending Areas	Rank
Security staffing	
Security consultants/outsourcing	
Employees' awareness and training	
Software security controls	
Hardware and physical security controls	
Incident response and business continuity	
Audit activities, compliance and certification costs	
Other, please specify.....	

1.6 Security standards and certification:

1.6.1 In terms of its content, please indicate your awareness level of the British Standard for Information Security Management BS 7799:

The British Standard BS 7799	Low	Moderate	High
Part 1: Code of Practice for Information Security Management i.e. BS 7799-1: 2005 or ISO/IEC 17799			
Part 2: Security Techniques: Information Security Management Systems i.e. BS 7799-2: 2005 or ISO/IEC 27001			

1.6.2 In your opinion, what is the overall awareness level of your company's managers and employees regarding the British Standard BS 7799?

	Low	Moderate	High
Managers			
Employees			

1.6.3 Has your company become certified under the ISO/IEC 27001 Information Security Management Systems Standard?

Yes	No, but plans to	No, and no plans to	Don't know

1.7 AIS security effectiveness:

1.7.1 Please indicate the techniques used by your company to evaluate the effectiveness of the AIS security:

- External security audits [ ]
- Internal audits of security procedures [ ]
- Penetration testing [ ]
- Network monitoring software [ ]
- Vulnerability scanners [ ]
- Other, please specify ..... [ ]

1.7.2 Please rank the top 3 critical success indicators of the AIS security management within your company where 1 represents the most important:

Success indicators	Rank
Information security assurance	
Reduction in internal policy breaking	
Reduction in frequency of AIS security incidents	
Increased ability to recover from disasters	
Successful defences against AIS security attacks	
Increased budget for AIS security	
Other, please specify.....	

1.7.3 In your opinion, how effective is the AIS security management in your company?

Not effective at all	Somewhat ineffective	Neither ineffective nor effective	Somewhat effective	Extremely effective

Section 2: Security threats to the company's AIS

This section aims to investigate the most common types of security threats that are currently facing the company's AIS and the sources of those threats.

2.1 Please rank the top 3 users who in your opinion represent the common sources of security threats to your company's AIS where 1 represents the most common source:

Sources of security threats	Rank
Authorised users/employees	
Former employees	
Suppliers of goods or services	
Customers	
Competitors	
Computer hackers	
Other, please specify.....	

2.2 Please indicate the frequency with which your company has faced each type of the following threats in the last year:

Security Threats	None	Once a year	Once a month	Once a week	Once a day	More than once a day
Unauthorised access to the data/systems by disgruntled employees						
Unauthorised access to the data/systems by hackers						
Unintentional destruction of data by employees						
Intentional destruction of data by employees						
Theft of physical information e.g. printed output, computer disks, tapes						
Introduction of computer viruses, bombs or worms to the system						
Spamming attacks						
Malware (spyware, adware) programs						
Sharing of passwords						
Theft of software						
Technical software failures or errors						
Sabotage or intentional destruction of computing equipment e.g. PCs and laptops						
Natural disasters e.g. fire, floods, earthquakes, etc.						
Other, please specify.....						

Section 3: Security controls of the company's AIS

This section aims to investigate the security controls of the company's AIS that are currently implemented and employed to reduce security threats.

3.1 For each of the following security controls please indicate whether your company is currently using it, is planning to use it, or there are no plans to use it:

Security Controls	Yes	No, but plans to	No, and no plans to
Administrative/Organisation Security Controls:			
Reorganised AIS security functions			
Continuous auditing techniques			
Real time security awareness/incident response			
Disaster recovery and business continuity plan			
Personnel Security Controls:			
Background investigations/reference checks			
Signing of confidentiality agreement by employees			
Security training and awareness programs			
Segregation of duties			
Mandatory vacations			
Software Security Controls:			
Testing software before use			
Off-site storage of original software			
Safeguards against unauthorised access to software			
Software audit alert tools			
Virus protection software			
Cancelling passwords for terminated employees			
Intrusion prevention/detection software			
Insurance coverage for software			
Hardware/Physical Security Controls:			
Back-up for hard disks			

Firewalls			
Penetration testing			
Restricting access to the main computing facilities			
Security alarm system			
Biometric techniques			
Storing unused laptops in secure/locked cabinets			
Placement of authorisation/database/accounting servers in secure location			
Protecting computers from natural disasters e.g. air conditioners, fireproof installations, waterproof installations, smoke detectors, etc.			
Insurance coverage for hardware and computer devices			
Input/Data Security Controls:			
Off-site storage of data back-ups			
Encryption of sensitive data			
User access controls/authorisation			
Output Security Controls:			
Restricting access to sensitive information for authorised users			
Storing sensitive output in secure/locked cabinets			
Network Security Controls:			
Network encryption			
Content and e-mail filtering software			
Malware (spyware, adware) detection tools			
Spam filtering software			
Other, please specify			

Section 4: General and Background Information

This section aims to collect general information about yourself and the company that you represent.

4.1 Please state your job title: .....

4.2 Please state the number of years of experience in your current job in this company:.....year (s)

4.3 Please state the most recent educational qualification you have obtained: ....

4.4 Please state the academic field of study of your most recent educational qualification: ....

4.5 Do you have any professional security qualification?

YES [ ] **NO [ ]**

If yes, please specify.....

4.6 Please select the industry group, which most closely corresponds to your company's line of business:

Education		**Health care**		**Pharmaceuticals**		**Telecommunications**	
Energy & Utilities		**Insurance**		**Property & Construction**		**Travel**	
Financial Services		**Manufacturing**		**Retail Merchandising**		**Wholesale Merchandising**	
Government		**Media & Entertainment**		**Technology**		**Other**	

Other, please specify .....

4.7 For how long has your company been established?

Less than 5 years	5-10	11-20	More than 20 years

4.8 How many employees are in your company?

Less than 100	100-500	501-1000	1001- 5000	5001-10000	More than 10000

Finally, if you have any further comments or suggestions you think relevant to the issues addressed in this questionnaire, please use the space below:

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Are you willing to spare me a few more minutes of your valuable time in a follow-up face-to-face interview concerning your views on the security of the accounting information system in the UK in general and in your company in particular?

YES [ ] **NO [ ]**

If yes, please provide your title, name, address, telephone number and e-mail address in the box below:

Title:.....

Name:.....

Address:.....

Telephone number:.....

E-mail address:.....

Do you wish to receive a copy of the results of this research?

YES [ ] **NO [ ]**

If yes, please provide your name and address in the above space

THANK YOU VERY MUCH FOR YOUR TIME AND EFFORT IN COMPLETING THIS QUESTIONNAIRE
YOUR CONTRIBUTION IS VERY MUCH APPRECIATED

Please kindly return this completed questionnaire in the FREE POST envelope provided.

Appendix 2
Covering Letter and the Semi-Structured Interview Schedule

The IT Manager
Company Name
Address

Date

Dear Sir/Madam

Thank you very much for your time and effort in completing the questionnaire regarding the security of accounting information systems. I really do appreciate your response a great deal. Thank you again for your agreeing to allow me to interview you concerning your views on the security of accounting information systems in the UK in general and in your company in particular. I attach an interview guide to give you notice of the indicative questions that I would like to discuss with you. Please note that, of course, I will not press you if you choose not to answer a particular question.

You may recall that I am a full-time PhD student in the Accounting and Finance Section at Cardiff Business School, Cardiff University. I am currently conducting research for my PhD thesis under the supervision of Professors Roy Chandler and Maurice Pendlebury.

The objective of my research is to evaluate the nature of accounting information systems currently used in UK firms and to investigate the security threats facing these systems and the security controls employed by firms to reduce such threats.

I confirm that the information and opinions provided in the interview will be treated as strictly confidential and will be used only for the purpose of academic research. Under no circumstances, will I disclose any information that will identify respondents or their companies.

Thank you very much for your cooperation, time and support.

Yours faithfully

Nancy Ibrahim Riad
Cardiff Business School
E-mail: RiadNI@cardiff.ac.uk
Telephone: 078 94 54 93 24

Semi-Structured Interview Questions

Section 1: Introductory discussion

- Introducing the researcher
- Thanking the interviewee for participation in the research
- Explaining the aims and importance of the current study
- Assuring interviewee of absolute confidentiality

Section 2: General and background information

- Company name
- Industry group
- Number of employees
- Position of interviewee
- Years of experience in the current position
- Professional security qualification (if any)
- Is there a separate department for security in the company? If yes, for how long has this department been established? How many employees are in this department? To whom do they report?

Section 3: The management framework of AIS security

3.1 AIS security policy

- Does your company have a written security policy covering its AIS? If yes, how old is it? Who is responsible for establishing this policy? How often is this policy updated? How is this policy distributed among employees?
- In your opinion, what is the most important element of your company's AIS security policy? Why?
- How often does your company check compliance with the security policy? How is compliance checked? Are consequences of non-compliance with AIS security policy clearly communicated and enforced?
- How do you rate the overall effectiveness of this policy?

3.2 Training and awareness program

- Does your company have a formal AIS security training and awareness program for its managers, employees and other users?

- Have you received formal security training? If yes, please state the most important topics covered in the training you received.
- In your opinion, what are the most common media for security training and awareness in your company?
- In your opinion, what are the most effective techniques used in your company to make staff aware of AIS security issues?
- Does your company undertake annual testing of security awareness? How does your company measure and monitor staff security awareness?
- In your opinion, what is the overall security awareness level in your company?

3.3 Risk assessment

- Does your company have an AIS risk assessment program? If yes, how often does your company undertake this risk assessment?
- Do you remember the last time your company undertook this risk assessment?
- Who is responsible for undertaking this risk assessment? How do you assess AIS risk in your company?
- In your opinion, what is the overall risk level of AIS security in your company?

3.4 Incident handling, disaster recovery and business continuity plan

- Has your company experienced any AIS security incidents in the last 2 years? If yes, can you remember the average number of these incidents?
- Can you remember the last security incident that occurred in your company? How was the incident discovered? Was the cause of this incident internal or external? What were the costs of this security incident to your company?
- What is the worst security incident that you could possibly imagine happening in your company?
- Does your company have formal security incident handling procedures?
- If a serious security incident happened in an area in which you have some responsibility, what are the steps you think would have to be taken to deal with this situation?
- Does your company report security incidents to external authorities? If yes, to whom does your company report these incidents? If no, what are the reasons for not reporting these incidents?

- In your opinion, is your company prepared to recover from a serious security incident?
- After a security incident, what changes were made by the company to reduce future incidents?
- Does your company have a formal business continuity plan? If yes, how often does your company tested and updated this plan? Do you remember the last time your company tested and updated this plan? Who is responsible for establishing this business continuity plan?
- How would you rate your company's effectiveness in detecting and responding to security incidents from insiders and outsiders?

3.5 Security budget

- Does your company have a separate budget for security? If yes, approximately what percentage of your company's security budget was spent on AIS security in the last year?
- How does your company decide what to spend on AIS security? Who approves this budget?
- What are the top areas of spending on AIS security in your company?
- How would you characterise your company's overall spending on AIS security?
- What do you expect your AIS security budget will be in the next year?

3.6 Security standards and certification

- In your opinion, what is the overall awareness level of your company's managers and employees regarding British Standard BS 7799?
- Where does your company stand in formally adopting or becoming certified under ISO/IEC 27001 Information Security Management Systems Standard?
- In your opinion, what are the benefits of complying with this standard?

3.7 AIS security effectiveness

- Does your company evaluate or measure the effectiveness of AIS security? If yes, what techniques are used for this evaluation?
- In your opinion, what are the most important success indicators of AIS security management within your company?

- In your opinion, what are the top obstacles to effective AIS security in your company?
- In your opinion, how effective is AIS security management within your company?

Section 4: Security threats to the company's AIS

- Security threats have become much more sophisticated in the last few years. Can you explain your point of view?
- In your opinion, what are the most serious security threats to AIS in general and AIS in your company in particular? What is the most frequent threat facing your company's AIS?
- In your opinion, what are the most common sources of security threats to your company's AIS?
- In your opinion, what are the most likely AIS security threats your company will be concerned about over the next two years?

Section 5: Security controls of the company's AIS

- Do you think your company is more secure today than a year ago?
- What are the most recent AIS security controls employed by your company?
- From your point of view, are there any gaps that exist between AIS security threats in your company and the scope of controls actually used?
- If you are asked to plan for some new AIS security controls in your company, what are the controls you feel are important and must be employed?
- What are the AIS security controls your company is planning to use in the next year?
- What are the AIS security controls your company is not using and is not planning to use? Why?
- Do you think AIS security will be much better next year than it is today?

Section 6: Uncovered issues

Would you like to add other issues not covered but you feel are important for the current study?

THANK YOU VERY MUCH FOR YOUR TIME AND COOPERATION

Appendix 3
Consent Forms - Confidential and Anonymous Data

CARDIFF BUSINESS SCHOOL
RESEARCH ETHICS

Consent Form - Confidential Data

I understand that my participation in this project will involve providing my opinions and views concerning some AIS security issues regarding the UK in general and my company in particular in an interview which will require approximately 90 minutes of my time.

I understand that participation in this study is entirely voluntary and that I can withdraw from the study at any time without giving a reason and without loss of payment (or course credit).

I understand that I am free to ask any questions at any time. If for any reason I experience discomfort during participation in this project, I am free to withdraw or discuss my concerns with **Professor Roy Chandler**.

I understand that the information provided by me will be held confidentially, such that only the researcher - **Nancy Ibrahim Riad** - *can* trace this information back to me individually. The information will be retained for up to *2 years (or until finishing the current research)* when it will be deleted/destroyed. I understand that I can ask for the information I provide to be deleted/destroyed at any time and, in accordance with the Data Protection Act, I can have access to the information at any time.

I also understand that at the end of the study I will be provided with additional information and feedback about the purpose of the study.

I, _____ (*NAME*) consent to participate in the study conducted by Nancy Ibrahim Riad of Cardiff Business School, Cardiff University with the supervision of Professor Roy Chandler.

Signed:

Date:

CARDIFF BUSINESS SCHOOL
RESEARCH ETHICS

Consent Form - Anonymous Data

I understand that my participation in this project will involve providing my opinions and views concerning some AIS security issues regarding the UK in general and my company in particular in an interview which will require approximately 90 minutes of my time.

I understand that participation in this study is entirely voluntary and that I can withdraw from the study at any time without giving a reason and without loss of payment (or course credit).

I understand that I am free to ask any questions at any time. If for any reason I experience discomfort during participation in this project, I am free to withdraw or discuss my concerns with **Professor Roy Chandler**.

I understand that the information provided by me will be held totally anonymously, so that it is impossible to trace this information back to me individually. I understand that, in accordance with the Data Protection Act, this information may be retained indefinitely.

I also understand that at the end of the study I will be provided with additional information and feedback about the purpose of the study.

I, _____ *(NAME)* consent to participate in the study conducted by Nancy Ibrahim Riad of Cardiff Business School, Cardiff University with the supervision of Professor Roy Chandler.

Signed:

Date: