The Implications of Economic Cybercrime for Policing

RESEARCH REPORT CITY OF LONDON CORPORATION **OCTOBER 2015**

CITY OF LONDON

CITY OF LONDON POLICE

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

The Implications of Economic Cybercrime for Policing

RESEARCH REPORT CITY OF LONDON CORPORATION **OCTOBER 2015**

www.cityoflondon.gov.uk/**economicresearch**

CITY OF LONDON

CITY OF LONDON POLICE

CARDIFF UNIVERSITY

PRIFYSGOL CAERDYDD

The implications of economic cybercrime for policing is published by the City of London Corporation. The lead author of this report is Cardiff University.

October 2015

PO Box 270
Guildhall
London EC2P 2EJ

www.cityoflondon.gov.uk/business/researchpublications

Authors

This report was prepared for the City of London Corporation by Cardiff University.

Dr Michael Levi, Professor of Criminology, School of Social Sciences, Cardiff University (lead author)

Mr Alan Doig, Visiting Professor, Newcastle Business School, Northumbria University

Mr Rajeev Gundur, School of Social Sciences, Cardiff University

Dr David Wall, Professor of Criminology, School of Law, Leeds University

Dr Matthew Williams, Reader in Computational Criminology, School of Social Sciences, Cardiff University

Acknowledgements

Many people have given their time to this project, especially in the City of London Police (not least former Commander Stephen Head), but also in the National Crime Agency, EC3 at Europol, Police Scotland and in the 'family of policing' around Great Britain, which includes Trading Standards officers, Get Safe Online, and cyber security firms in the private sector, as well as the Intellectual Property Office and private sector anti-counterfeiting bodies. However, we would like to express particular thanks to Dr Steve Strickland, formerly of the City of London Police, for his time and skills in marshalling a variety of collaborators, and for his thoughtful commentary; to Sabrina Basran and her colleagues at the City of London Corporation for their editorial contributions and for their efforts to keep us on the right lines, balancing the academic and the practical; and to EC3 staff and Professor Alan Woodward for their comments on an earlier draft.

Contents

List of abbreviations

ABI	Association of British Insurers
ATM	Automated teller machine (a cashpoint)
BCS	British Crime Survey
CERT-UK	UK National Computer Emergency Response Team
Cifas	Credit Industry Fraud Avoidance Service
CiSP	Cyber-security Information Sharing Partnership
CNP	Card-not-present
CPNI	Centre for the Protection of National Infrastructure
CSEW	Crime Survey for England and Wales
CVS	Commercial Victimisation Survey
DCPCU	Dedicated Card and Payment Crime Unit
DDoS	Distributed denial of service (attack)
DWP	Department for Work and Pensions
FACT	Federation Against Copyright Theft
FFA UK	Financial Fraud Action UK
GDP	Gross domestic product
HMRC	Her Majesty's Revenue & Customs
ICT	Information and communications technology
IFED	Insurance Fraud Enforcement Department
IP	Intellectual property
IPO	Intellectual Property Office
IRC	Internet Relay Chat
ISBS	UK Information Security Breaches Survey
ISP	Internet Service Provider
IT	Information technology
MMOG	Massive multiplayer online game
MMORPG	Massive multiplayer online role playing game
MOPAC	Mayor's Office for Policing and Crime
NCA	National Crime Agency
NFIB	National Fraud Intelligence Bureau
OCG	Organised crime group
ONS	Office for National Statistics
PBX	Private branch exchange
PCSP	Police Community Support Officer
PIPCU	Police Intellectual Property Crime Unit
PPP	Purchasing power parity
PSP	Payment service provider
SAR	Suspicious activity report
SCADA	Supervisory control and data acquisition
SME	Small to medium-sized enterprise
SMS	Short message service (text message)
Tor	The Onion Router
URL	Uniform Resource Locator
VAT	Value added tax
VoIP	Voice over internet protocol
WAPOL	West Australian Police

Foreword

London, as one of the world's leading financial centres, had a daily turnover in the foreign exchange market of £2,626 billion in April 2013 - all dependent on a highly interconnected electronic infrastructure and supporting technology. Yet this same technology that underpins and enables these global transactions also opens up businesses and individuals to new risks, in particular relating to cybercrime.

The introduction of sophisticated technology has brought about a step-change in the way economic crime is committed – enabling frauds to be perpetrated at scale, at great speed, and at a distance, with no physical contact necessary between criminal and victim. It can be much harder to identify the individuals initiating crime, and often the location will be outside UK jurisdiction. These factors have resulted in a sharp escalation of such activities in recent years, bringing new challenges for policing and industry in preventing and tackling such crime.

The City of London Police is the National Policing Lead for Economic Crime, and is playing a key role in proactively addressing these challenges including developing a national strategy. One major challenge has been coordinating information about criminal activity where this can be geographically widely dispersed. In addition to investigating some of the most serious frauds in the country, the City of London Police hosts the national reporting database – Action Fraud. This current research piece undertakes new analysis of data held by Action Fraud and its partner unit, the National Fraud Intelligence Bureau (NFIB) also hosted by the City of London Police. It finds that between October and December 2014 alone there were 106,681 reported fraud cases, a third of which related to banking and credit industry frauds. The median amount lost to fraudsters across all fraud types ranged from £112 lost through misuse of contracts in the telecom industry, to £38,974 lost from pension fraud. However the annual 250,000 crime reports received present only a limited view of several million crimes that are taking place within the UK annually to the cost of some £30billion. Under-reporting presents a challenge both in terms of research and policy responses.

City of London Police initiatives to reduce fraud include training both the private and public sector in specialist skills through their Economic Crime Academy, piloting a focused victim care unit in London – the Economic Crime Victim Care Unit - and working closely with law enforcement across the UK to share information and co-ordinate action. Most importantly they include the formation of new national police fraud and cyber strategies focused on prevention at a national and local level.

This research report highlights the necessity of working in partnership, both around primary prevention and building in security protection, and working with other agencies to disrupt criminal activities and pursue and prosecute offenders.

Even with these initiatives, there is much more to do. Economic cybercrime is evolving rapidly, at a scale and speed never before seen. This report provides new data and analysis around the scale of this activity and offers a comprehensive view of the challenges facing the policing and law enforcement responses. It appraises the success of different approaches to preventing and addressing crime, and presents practical suggestions with a focus on partnership working, education and awareness-raising, information-sharing across industry, and intelligence-led policing. As such it is a timely piece of valuable research that can help to shape future policies focussed on combatting the growing threat of cybercrime.

Mark Boleat
Chairman of Policy & Resources
City of London Corporation

Commissioner Adrian Leppard QPM
City of London Police

1. Executive summary

The use of the internet and technology to commit economic crime has been escalating sharply in recent years, bringing new challenges in preventing and tackling such crime. This research, commissioned by the City of London Corporation with the support of the City of London Police, and prepared by Cardiff University, sets out what we know about the rising role of the internet in economic crime; the variety, incidence and cost of economic cybercrime; who (as far as is known) the main actors are – victims, attackers, actual and potential protectors, and the facilitators or criminal actors themselves; and the implications of these findings for business, government and the public in terms of policing economic cybercrime. The report goes on to use this analysis as a basis for evaluating current policing models and approaches to economic cybercrime. It discusses some of the challenges faced in policing and the strategies developed to cope with economic cybercrime, as well as the varied responses available within the parameters of the 'Four Ps' of government strategy (Pursue, Prevent, Protect, and Prepare).

1.1. What is economic cybercrime?

There are three main forms of economic cybercrime:

- **Cyber-dependent crimes** in law rely on networked information and communications technology (ICT), largely via the internet. Without the internet, the offending would not be possible.
- **Cyber-enabled crimes** are facilitated by these same ICT-connected technologies, but are not dependent on them, and therefore can exist in some non-cyber form. If the networked technologies were removed, the crime could still take place but locally and more likely on a one-to-one basis. Being cyber-enabled allows these crimes to be carried out at scale for less capital and sometimes with fewer criminal staff than would be needed for similar crimes offline.
- **Cyber-assisted crimes** are differentiated from cyber-dependent and cyber-enabled crimes, and use networked digital technologies (such as mapping applications) in the course of criminal activity which would take place anyway. The nature and volume of criminal activity are essentially unaffected by its involvement (i.e. if the internet involvement was removed, the crimes would be organised in different ways).

Both the cyber-dependent and cyber-enabled forms of economic cybercrime provide criminals with a globalised reach in a distributed and informational way. If the networked technologies are removed, then the crimes still take place but both victim and perpetrator are much more likely to be located in the same country, or adjacent countries, when crimes are undertaken offline. The number of victims per criminal attempt is also likely to be lower and the means employed – in person, telephone, advert or letter – can be more amenable to investigation.

The cyber element can occur in different forms at any stage, from the planning of a crime through to its execution, to the expenditure and/or laundering of its proceeds.

The Crime Triangle theory[1] teaches us that crime is the product of would-be offenders, targets/victims and guardians, including those professionally paid to

[1] For a brief summary, see Felson & Clarke (1998: 4).

protect the public or whose routine activities serve to reduce opportunities for particular forms of crime. The virtue of this model is that it is dynamic, and can include insiders (some of whom may need or use ICT to complete their crimes), outsiders, and combinations thereof. So at any given time, economic cybercrimes are affected by the technologies available, those who are capable and motivated to exploit them and the vulnerabilities of the targets/victims. Some targets are deliberately selected for attacks (known as 'spear-phishing') whereas others are indiscriminately selected in mass attacks.

1.2. What is the scale of the challenge?

Criminal statistics and business and individual victim surveys show that fraud is on the rise, while the crime rates for other types of acquisitive crime are falling.[2] However, the evidence base for how 'cyber' has contributed to economic crimes is incomplete and weak, both today and historically. Other than cyber security vendor data, we depend on victims, or other parties, identifying and communicating their experience of an economic crime and their understanding of how it was carried out, within the existing framework of data recording and capture. While limiting, this does allow us to see both the increase in economic cybercrimes and the varied levels of cyber-involvement and reported losses from different types of such crimes. The Action Fraud and National Intelligence Fraud Bureau (NFIB) databases are two such examples and represent important steps in developing an evidence-based response to a growing area of criminal activity.

We can tell a certain amount about offenders from investigating the circumstances and techniques for criminal activity, but there is no evidence that large numbers of cyber-dependent perpetrators are primarily focused on financial gain, or that traditional criminals – particularly drug traffickers, burglars and robbers – are turning to cyber-enabled frauds in significant numbers. Relatively few cyber-enabled economic crimes are prosecuted, especially if suspects are based abroad, which means little is actually known about how criminals conduct their economic cybercrimes.

In terms of what we do know, and identifying trends based on the data available, this report estimates that of the fraud-related crimes reported to Action Fraud by individuals and businesses in the last three months of 2014 (Q4 2014), well over half were significantly cyber-related: 43% were cyber-enabled, and 13% were cyber-dependent, while a further 29% of them simply used technology (cyber-assisted).

1.3. What is the nature of economic cybercrime?

Data breaches and identity frauds have been rising steadily. E-commerce fraud losses increased rapidly in the early 2000s, especially after the rise of botnets, reaching a peak of £181.7 million in 2008 before falling until 2011. Losses totalled £217.4 million in 2014, when they accounted for 45% of all card fraud and 66% of total remote purchase fraud. Losses to the banking sector from online banking fraud rose in 2009 to £59.7 million, and peaked to a new high in 2013/14, at £60.4 million. Criminals also appear to be targeting businesses more, reflected in a higher average loss per online fraud case during 2014. It is, however, worth highlighting some of the

[2] ICT platforms have become central to the way business and social life are organised, and crime follows these changes when it is allowed to. This report, however, would point to a distinction between cybercrime intended to harm (e.g. hacking and some traditional malware) and acquisitive cybercrime.

challenges of the data – for example, the risks of looking only at year-on-year changes, and missing the impact of new technological security measures. This is illustrated by the fact that, though losses to the banking sector from online banking fraud first peaked in 2009 at £59.7 million, the new recorded high of £60.4 million in 2013/14 was only slightly above 2009 levels and less in real terms.

1.4. What are the practical implications for policing?

Based on the literature and analysis of Action Fraud data (covering Q4 2014), this report raises and considers some important questions for the policing of economic cybercrime. When answered, these will assist the police and partner agencies, businesses and individuals in their responses to the Four Ps Model where:

- **Pursue** is about following up organised criminals by prosecution and disruption;
- **Prevent** is about stopping people from becoming criminals (rather than about crime prevention);
- **Protect** is about primary prevention for business and the public against serious and organised crime; and
- **Prepare** is about post-event resilience for attacks and reducing the impact of crime, as well as future prevention.

While law enforcement bodies have developed a number of relevant strategies, these strategies and their implementation by type of cybercrime and victim need to be reconsidered in the light of the data now available. For example, the 'cyber' involvement can vary in the course of a crime: many cyber-enabled crimes begin online to hook victims, but offenders may take victims offline (sometimes assisted by technology) in order to extort money; even if the victim (or purchaser of crime-as-a-service software) pays in cryptocurrency, there may be a pay-out that is made offline (i.e. not connected to ICT) at a later stage when the criminals want to realise their gains. Thus Prepare strategies need to be flexible in order to increase resilience, and Pursue strategies need to find intervention points over the spectrum of economic cybercrime, from organising the crimes to money laundering, whether their aim is prosecution, asset freezing and recovery, and/or crime disruption.

1.4.1. The implications for Protect and Prepare

Protect spans a wide range of individuals and organisations. General improvements in cyber-protection methods are required to effectively reach all of these potential victims. Ideally, Protect methods would be built in with minimal effort or administered 'bottom-up' through peer groups, community-level bodies and charities, to help individuals and small to medium-sized enterprises (SMEs) adopt simple security processes, such as two-factor authentication and antivirus auto-updates that do not require complex attention or regular effort; otherwise they will be bypassed by staff or not completed at all.

Larger businesses can and should promote good security practice in the organisational frameworks already established, paying attention to insider as well as outsider threats. In addition to catastrophe risk reduction, more effort should be undertaken via segmentation exercises to identify those individuals and businesses who are at risk of repeat victimisation; a quarter of mass marketing fraud victims have been victims previously. This should focus Protect and Prepare efforts on the most vulnerable, preferably with the participation of community-level bodies and peers as well as technology firms and Police Community Support Officers (PCSOs) or Community Officers. (Arguably, a similar approach could also be employed for identifying potential offenders, with a greater focus on Prevent and Pursue motives.)

Additionally, whether undertaken by police or civilians, initiatives to provide reassurance and practical help for those affected by economic cybercrime are of value in themselves, irrespective of their impact on the Prepare strategy. This is due to the negative psychological elements of being a victim of fraud – such as self-blame or shame, particularly if we think ourselves complicit or gullible. This can make the experience worse for victims of fraud than for victims of theft and burglary (where most people take standard precautions and where the offence often occurs beyond our control). In addition, frauds tend to generate higher financial losses (and profits to organised criminals) than other predatory crimes.

1.4.2. The implications for Pursue

Much can and must be done to raise general cyber-awareness and digital capabilities in the police nationally, for general crime investigation as well as economic cybercrimes. One of the problems with the data to date is the lack of material on offenders and their engagement in cybercrime. For example, there have been few prosecutions under the Computer Misuse Act 1990 for cyber-dependent crimes, with some 339 prosecutions and 262 persons found guilty at magistrates' courts between 1990 and 2013.[3] Of those prosecutions, unauthorised access to computer material is by far the most enforced offence. However, the prosecution data only covers cases where computer offences were the most serious charge, so in most economic crimes in which networked computers are used, the cyber component is largely omitted from the public record. Determining options – whether investigation, asset recovery, disruption or restorative justice – is thus problematic.

Unless there are special liaison efforts (as in parts of West Africa and Eastern Europe) in which the 'host' jurisdictions and the UK work in partnership, there are limits to the feasible prosecutability of all but the most major offenders who are overseas. Where mutual legal assistance is very unlikely, police pursuit can seem pointless except to show victims that something is being done. A more controversial policy issue is whether one criterion for police investigation should be the degree of effort that victims have put into protecting themselves. The development of cyber insurance in protecting against catastrophic and lesser degrees of risk is also a subject of much debate in business and government.

In collaboration with partner agencies such as Trading Standards and the Intellectual Property Office (IPO), and with private sector collective and individual bodies, both criminal and administrative sanctions can be pursued. In doing so, it is vital that we avoid separating 'cyber' from the crimes and from the offender groupings that it facilitates. Disruption strategies – including take-downs of websites, botnets and dark markets – are valuable for harm reduction, especially if websites are taken down early, which require policing resources and/or internet service provider (ISP) proactivity. However, we know little about the medium and long-term effects of these measures, since scam websites and exchange forums may spring up again, as they are low cost and easy to form. These often reappear with improved security/encryption measures in place, having learned from past take-downs, making future take-downs more difficult. There is scope for experiments involving warning 'pop-ups' on screen for those who fall victim to offers that could be

[3] www.parliament.uk/business/publications/written-questions-answers-statements/written-question/Commons/2015-01-27/222192/.

fraudulent, though this would require careful management of the user experience. There is a need for more focused internet governance to deal with these challenges, but the politics of international opportunity reduction are very hard to achieve.

1.4.3. The implications for Prevent

Finally, with regard to Prevent, our research indicates that intelligence leads for the Pursue strategy should be closely linked with the Prevent strategy, in order to stop offenders descending into more serious criminality. For some early-stage offenders, warnings and advice would be appropriate, thus avoiding the development of a career-inhibiting criminal record, which would be aggravated by mixing with more mainstream serious offenders in the criminal justice system.

1.5. Concluding remarks

This report aims to provide a snapshot of where this important area of criminality is now, how it got here and how well we are organised against its various dimensions. There is no quick fix for these issues and we need to pay more attention to behavioural cues in order to develop security more in tune with the likely responses of individuals and businesses, rather than treating 'cyber' as a separate technical category. To improve the effectiveness of cyber security, there needs to be co-working towards a shared goal between the various members of the 'family of policing', business and civil society; though partnership policing alone is not a silver bullet solution. However, as the head of the National Police Chiefs' Council said recently,[4] we may also need to acknowledge that some degree of 'cost' or 'trade-off' is required; we lack the resources to investigate and/or the skills/technology to prevent every type of economic cybercrime. In acknowledgement of where some of the challenges lie, this report goes on to look at how possible policing responses may be developed and what the future of policing might look like when addressing economic cybercrime.

[4] See: www.telegraph.co.uk/news/uknews/crime/11767419/Police-chief-warns-that-officers-may-no-longer-respond-to-burglaries.html.

2. Introduction

The purpose of the research is to identify, define and examine some of the key issues and complexities surrounding cyber-enabled and cyber-dependent economic crime. By analysing the implications of these for policing, the report shows how businesses and individuals are affected by economic cybercrime and presents practical suggestions on how they may be supported within the context of the ongoing Pursue, Prevent, Protect and Prepare agendas.

The research that underpins this report has been commissioned by the City of London Corporation, with the support of the City of London Police. It explores cyber-enabled and cyber-dependent economic crimes, and their implications in relation to impact, policing and prevention, in accordance with government strategies for combating organised crime and terrorism. The research involved interviews with key UK and international stakeholders including the principal agencies for economic crime control, financial services and industrial firms, cybercrime prevention bodies in the public and private sectors, and police officers (retired and current), underpinned by an extensive secondary research review.[5]

2.1. Context

It is important to recognise that economic crimes of huge scale and impact occurred long before the internet. Serious economic crime has never required a cyber-dimension. The impacts of such activity have always included victims in both domestic and international jurisdictions. However, the presence of ICT in daily life has changed markedly over the past two decades. Every day there are more people and, more significantly, devices connected to the internet, spawning the term 'the internet of things' (van Kranenburg et al., 2011). The interconnectivity between people, machines and cyberspace is growing exponentially so that many areas of our lives, and increasingly so, are organised and undertaken through connected technology. This makes a large proportion of our working and non-working lives vulnerable to exploitation, with the potential for significant harm. Some predict that by 2020 there will be upwards of 50 billion devices connected to the internet (Cisco). Annual internet protocol traffic is projected to triple between 2014 and 2019 to a record 2 zettabytes,[6] adding trillions of dollars to global GDP (Accenture, 2015). An unintended consequence of this will be to extend the range of important, if not 'critical', infrastructure which is vulnerable to cyber-attack.

This routinisation and pervasiveness of internet use has made certain types of crime possible (cyber-dependent crimes), and has facilitated immensely the scale of others (cyber-enabled crimes), by enhancing offender productivity and widening the scope for crimes to be undertaken. The 'crime scene' today can be part of ICT platforms with multiple uses, from social media to confidential financial transactions. Current technologies offer speeds 500 times greater, sometimes more, than the dial-up modems of the 1990s. Technology and cyberspace have lowered the entry costs for mass frauds and eased their penetration within and across international borders, both in terms of the scale of this penetration and the speed with which it can be accomplished. In terms of cyber security, however, the necessity for, and types of,

[5] Individual sources have not been identified. Interviews were recorded by note rather than tape-recorder and no direct quotes are used which could identify individuals or specific agencies.
[6] See: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1644203.

protection has often lagged behind such developments (marketing strategies, volume of traffic, speed and ease of access, and the reliance on automated controls). One of the unintended consequences of the massive growth in connected technologies has been to make it more complex for those individuals who are not 'cyber-savvy' to understand and act upon the different security risks presented by technical devices such as computers, mobile phones and tablets. Similarly, they may not appreciate the level of interconnectivity or proactivity by or between devices that do not require human intervention or authorisation, or even necessarily be able to identify updates or interactions that take place automatically.

This has increased the difficulties of identifying, investigating and prosecuting offenders as much as it has increased vulnerabilities in businesses and individuals (including the general public) when undertaking routine transactions. For example, actions previously considered trivial (for example clicking on a URL link) can now initiate adverse consequences. It is difficult to develop plans that effectively respond to technological changes before the negative consequences of accidental or intentional misuse manifest themselves. In other words, making judgements about who or what the threats are, why, and how far they can be anticipated and pre-empted, requires innovative thinking and also practical action.

Cyberspace and, subsequently, cybercrime, have created a need to think through the nature of the threats and risks they pose and to understand what types of responses are most likely to be more or less effective, and under what circumstances. In addition, such developments have reinforced the need to better understand perpetrators and their motivations (for example, through online profiling). This report aims to contribute to that process, reviewing government strategy – adapted from its CONTEST counter-terrorism strategy – which has four components (Home Office, 2014, 2015a):

- **Pursue** organised criminals by prosecution and disruption;
- **Prevent** people from becoming criminals;
- **Protect** business and the public against serious and organised crime; and
- **Prepare** for attacks by building post-event resilience to reduce the impact of crime and improve resilience for future prevention.

In so doing, it is our view that finding the right term to describe the various threats posed by 'cyber' is important, because the wrong terminology encourages us to adopt unsuccessful strategies. So, for example, while the language of 'cyberwarfare' may stimulate a sense of urgency, it carries with it the expectation that the issue can be addressed as a distinct series of events or 'battles'. In reality, the security challenges posed by economic cybercrime are more of a permanent struggle, and cannot be solved by conventional attack strategies alone.

2.2. What does 'economic cybercrime' mean for this research?

Economic cybercrime largely involves obtaining, or initiating dialogue to obtain, data, goods and/or money by deception, misrepresentation or straightforward fraud from individuals, businesses and government through the medium of the internet. Some of these crimes involve no direct personal contact but are purely electronic, including financial transfers. Intellectual property (IP) can also be duplicated or transferred, significantly lowering product value and with potential negative consequences from using the 'faux' product. However, most damage takes the form of private economic transfer, domestically or internationally. While we recognise that nearly all crimes which involve ICT can be considered economic

cybercrimes, since most are intended to achieve some sort of economic gain, this understanding is neither practical nor particularly helpful.

Action Fraud[7] applies a typology of frauds including, but not restricted to, their cyber component – money laundering, for example, is not included because it is an enabler of and consequence of economic crimes, not a fraud in itself. This typology highlights the broad range of economic crime offences and, by implication, the range of people and business activities that need to be considered for prevention purposes, including:

- Advance fee payments;
- Financial investments;
- Non-investment fraud;
- Charity fraud;
- Banking and credit industry fraud;
- Insurance fraud;
- Telecom industry fraud (misuse of contracts);
- Corporate fraud;
- Pension fraud; and
- Computer misuse crime.

This research restricts itself to focusing on cyber-dependent and cyber-enabled crimes where the intention of the crime is economic gain. It thus excludes online child exploitation, terrorism, violent extremism, computer misuse (where no financial gain is sought or achieved) and other social threats. It also excludes 'service' forms of organised crime (such as drugs or human smuggling/trafficking) that are facilitated by using digital technologies as forms of communication.

2.3. What are cyber-dependent economic crimes?

Cyber-dependent crimes require ICT in order to be executed (McGuire & Dowling, 2013); they are 'true' cybercrimes and dependent upon the internet (Wall, 2007a). Some, such as malware and distributed denial of service (DDoS) attacks which crash websites and reduce their functionality, do not have easily identifiable offline equivalents. Other forms do – such as ransomware, a form of blackmail. They would simply not exist without the internet. The vast majority of research conducted on ICT and deviance focuses on the cyber-dependent types of crime, in part because of the cost of securing against them (Garvey & Patel, 2014). Examples of such crimes, which are recorded by Action Fraud, include:

- Computer virus/malware/spyware;
- Denial of service attack;
- Denial of service attack extortion;
- Hacking – server;
- Hacking – personal;
- Hacking – social media and email;
- Hacking – PBX/ dial through; and
- Hacking extortion.

[7] Action Fraud is the national fraud and internet crime reporting centre for British law enforcement hosted by the City of London Police. In calculating, for example, the volume of reports, it is worth noting the work of other centres such as Cifas and FFA UK. The latter coordinates information from and preventative approaches for some sectors of the financial services industry. In its analysis of crime data, the National Fraud Intelligence Bureau (NFIB), receives and collates data from all three sources.

Cyber-dependent crimes are often profit-motivated, but may take the form of ideological or political attack (such as the Russian-inspired DDoS attack on the Estonian financial services system in 2007 and, though still strongly contested as to motivation, attacks on Sony in 2011 and 2014) or cultural rebellion (as post-Assange/Pirate Bay/Swartz/Snowden), as well as hacking into corporate and governmental websites to acquire commercial, military and political knowledge not available to the wider public. For the purposes of this research, these crimes are addressed only when they involve identified financial gain. In the case of the Action Fraud data, we find, for example, that computer misuse crimes account for around 4% of recorded fraud and fraud-related crime. Of that proportion, the severity levels are high but the financial losses accruing to the victim are lower per incident than are losses from, for example, dating scams or online shopping fraud.

2.4. What are cyber-enabled economic crimes?

A variety of crimes are, at least in part, facilitated by digital means (Lavorgna, 2013, 2014a, 2014b). For instance, the networked component of ICT can aid in the procurement and selling of an item, communication between actors, or the transfer of funds at a distance, making such interactions more efficient and/or increasing their scale (both in terms of perpetration and impact).

Cyber-enabled crimes are 'traditional' crimes that exist in law, whose scale or reach is increased by use of computer networks or other internet platforms, although they can be still be committed without the use of ICT (in which case they cease to be 'cyber-enabled'). We thus understand cyber-enabled crimes as crimes which can take place in two realms, both online and offline, often simultaneously, or at different phases in the commission of the crime. These include, from Action Fraud data:

- Fraudulent sales through online auction sites or bogus retail websites. Once paid for, goods or services are not delivered or buyers unknowingly purchase counterfeit products (as with online ticketing fraud);
- Consumer scams such as advance fee payments, for example '419 fraud', inheritance or lottery frauds;
- 'Online dating' frauds where individuals are persuaded to part with personal information or money following a lengthy online 'relationship' via dating sites;
- E-commerce frauds, involving the fraudulent use of plastic cards for online purchases; and
- Online banking fraud, where fraudulent access to online bank accounts is gained.

2.5. Report structure

Chapter 3 considers the current policing landscape in the context of economic cybercrime, identifies which issues require consideration from a policing perspective, and where some of the key areas of challenge lie, to assess targeted responses, whether in terms of prevention or criminal investigation.

Chapter 4 presents an analysis of Action Fraud data, and considers which groups are most affected by economic cybercrime, such as individuals/the general public and businesses, and some of the key issues these groups face. It also explores efforts being made to support these groups, drawing on the existing evidence base.

Chapter 5 considers the implications of the issues explored in chapters 3 and 4 for policing approaches to economic cybercrime, in particular reviewing Protect and Prepare efforts against economic cybercrimes.

Chapter 6 draws these themes and issues together and considers what needs to be done, given the dynamics of these crimes and our uncertain understanding of victims, offenders and methodologies of offending, and looks at the impact of our efforts to date.

This report draws upon an extensive range of secondary and primary material, as well as interviews with key stakeholders. There is an accompanying Technical Annex to this report which considers the different secondary resources available in further detail.[8]

This report contributes to the early stages of a conversation about rational and effective management of this issue, rather than presenting a conclusive resolution, given the rapidly evolving environment. We believe this report complements the existing evidence base on economic cybercrime and identifies thought-provoking questions and issues for consideration when tackling economic cybercrime.

[8] The Technical Annex is available online at the City of London research webpage: www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Pages/default.aspx.

3. The modern role of policing and economic cybercrime

This chapter considers how evolving changes in crime control have implications for the policing of cyber-enabled and cyber-dependent economic crime. Where crime control in the UK was once widely seen as the sole responsibility of law enforcement, the past two decades have widened the range of actors, with an emphasis on partnership and prevention. At the same time, those involved in criminal activity have also changed, due to enhanced crime reduction capabilities and technological developments. The latter has had multiple impacts such as expanding the scale and speed of economic cybercrime, widening the range of potential people involved in committing crimes as well as the volume and types of crimes possible. This has implications for policing responses to economic cybercrime.

This chapter seeks to review these different aspects to identify and understand the gaps in policing that need to be addressed. The shift in the nature of the policing problem is not specific to the UK – it is shared by all countries, with varied degrees of acknowledgement and response – but the focus here is the UK context.

3.1. What does 'policing' mean in this context?

The evolving policing approach to fraud very much reflects the wider changes in crime control over previous decades. Traditionally, crime control was widely seen as the sole responsibility of law enforcement, with those involved – namely, police and prosecutors – investigating and prosecuting breaches of the criminal law. Today, crime control involves other agencies, emphasising partnership and information sharing, and responses to crime are framed in terms of harm, disruption, prevention and reduction, as well as in the more traditional tasks of investigation and prosecution. Much attention is given to analyses of crime patterns and trends, and to the application of intelligence-led policing, as means to strategize responses and target resources.

Another key dimension of crime control today is the role played by those affected by crime and potential victims, by third parties, and by policing and criminal justice agencies. The latter include the police (with the City of London Police holding National Lead Force status for fraud and economic crime), the National Crime Agency (NCA) and Trading Standards. Third parties include an array of for-profit and not-for-profit bodies ranging from financial services institutions and vendors of antivirus and forensic/social network analysis software and prevention and post-event consultancy services, through to anti-counterfeiting intelligence and policing bodies. The latter may or may not pursue their own investigations and sanctions approaches without law enforcement involvement such as the Federation Against Copyright Theft (FACT), Get Safe Online and Cifas (the UK's fraud prevention service). It also includes organisations that have regular contact with the public, such as Citizens Advice.

There are essentially three drivers which have transformed the problems of economic cybercrime that the police and fraud control face. These are:

1. The **volume** of crimes that can be committed;
2. The **speed** and instantaneousness with which crimes can be committed and completed, and at which new or different types of crime can evolve through technology; and
3. The **distance or scale** at which crimes can be committed, often without it being obvious where the offender is operating from, meaning the actual offence can

take place thousands of miles away from where its impacts are felt or the victim is based.

Though these issues were all manifest historically before the internet age (Levi, 2008), their scale has overwhelmed traditional police models of reaction to crime, and their technicalities challenge the police role in protecting citizens globally. The growth of cybercrime and internet capacity generates multiple targets for economic crime; as the 2011 'UK Cyber Security Strategy' noted: "cyberspace is also being used as a platform for committing crimes such as fraud, and on an industrial scale" (Cabinet Office, 2011:15). Anyone can be affected and most can be inadvertent enablers of victimisation, from the least to the most sophisticated individuals, businesses, third sector bodies and government departments.

Policing itself has been subject to continuing efficiency reviews, budget reductions, performance measurement, management approaches and external reviews. The popular emphasis on 'front-line policing' has led to forces reviewing the retention of central units, including levels of resource, what type of organisational structures to apply to those that are retained, and which policy agendas should influence the focus of those structures. In parallel developments, corporate entities have assumed responsibility for fraud prevention and detection, often as a consequence of perceptions that a readily available enforcement and investigative deterrent is absent (Brooks, Button & Frimpong, 2009), while public sector organisations have expanded their own anti-fraud functions and taken on responsibility for investigating fraud themselves (Doig & Macaulay 2008). Alongside these activities has been a diminishing police resource for addressing individuals' victimisation. A recurring challenge raised by fraud reviews and research is the limited resources available for the policing response to fraud and to economic crime.

This understanding of policing – whether applied reactively or proactively – informs this research and particularly our focus on how to prevent economic cybercrime.

3.2. The policing landscape for economic cybercrime

Policing around the world is being challenged by evolving patterns of crime, especially economic crimes and the cyber-forensic aspects of police investigations. Subsequently, the last decade has seen an increasing focus on research mapping the amount of economic crime (Levi et al., 2007) and, more recently, measuring economic cybercrime. A better understanding of economic cybercrime is a necessary prelude to making decisions as to what to do about it.

The cost of fraud has risen significantly. The first contemporary cross-sector examination into this, the 2000 report prepared for the Home Office and the Serious Fraud Office (National Economic Research Associates (NERA), 2000), argued that discovered fraud and undiscovered fraud could each range from £5 billion to £9 billion, giving an overall upper range of £18 billion. It also included staffing and other costs associated with the prevention, detection, investigation and prosecution of fraud, assessed at: criminal justice system costs – £500 million; public sector organisation costs – £521 million; and private sector organisation costs – £114 million. Though a vital contribution to understanding the nature and costs of fraud, the NERA figures were collated from material published by various agencies in both the public and private sectors, with no review of the methodology used or the data's robustness. Furthermore, it overlooked fraud policing costs and the cost of fraud dealt with by the police (but not the Serious Fraud Office – the 1998 and 2000 surveys on behalf of the National Working Group on Fraud proposed a self-assessed value of cases handled by police fraud squads at £3 billion to £4 billion).

Research sponsored by the Association of Chief Police Officers (Levi et al., 2007) estimated the overall cost of fraud at a minimum of £13.9 billion. Subsequent National Fraud Authority cost estimates have risen over time, from £30 billion in 2009 to over £38 billion in 2010, and substantially higher still to £73 billion in 2012, before falling to £52 billion in 2013. Although the quality of the underlying data is variable and much extrapolated rather than based on actual losses (which themselves would be affected by under-reporting), this rise also reflects a broadening in the coverage of the Annual Fraud Indicator,[9] so year-on-year data does not entirely compare like with like. Nevertheless, the work on losses associated with fraud has identified that fraud is, as an economic crime, a significant area of criminal activity.

On the other hand, staffing resources (in terms of numbers) for the pursuit of fraud have been declining over the past two decades compared with those devoted to other policing priorities (Button, Blackbourn & Tunley, 2014; Doig & Levi, 2013; Doig, Johnson & Levi, 2011). Resources devoted to fraud have been in decline, partly because of competing priorities and partly because government agendas prioritise economic crime by organised crime groups (Gannon & Doig, 2010). In 2015, the total figure of full-time equivalent police staff for fraud was at least 1,000, out of a total police complement of 127,000 for England and Wales. Around half of these are in London, limiting the scope for the investigation of difficult cyber-enabled cases in the capital and, especially, elsewhere.

However, there have been some significant achievements and progress in policing fraud and economic cybercrime, most of which followed from the 2006 Fraud Review. These have included the designation of the City of London Police as the National Lead Force on fraud, covering both traditional and cyber forms of economic crime, with increased resources and a training academy for officers (the Economic Crime Academy); a National Fraud Strategic Authority (later renamed the National Fraud Authority but abolished in 2014, with some of its functions transferred to the Economic Crime Command of the NCA) with responsibilities for comprehensive measurement of fraud and a national strategy for dealing with it; a National Fraud Reporting Centre as the sole central reporting point for fraud (later renamed Action Fraud and managed by the City of London Police); and an intelligence resource (now the National Fraud Intelligence Bureau (NFIB) reporting to the Lead Force). In 2013, Action Fraud was rolled out nationally; since 2014, all fraud complaints, unless immediate action is required, are recorded through Action Fraud. The NFIB's role has been to synthesise and analyse all Action Fraud reports, to assess patterns and trends, and to direct intelligence packages (with variable intelligence enhancements) to the most relevant police force.

Reporting to the police for crimes other than fraud remains local, even though some offenders may target victims in different police force areas. In the case of economic cybercrime – which, as mentioned, spans geographical areas and police force jurisdictions – localised reporting is not appropriate. The City of London Police has worked with stakeholders to centralise fraud reporting at a national level, through Action Fraud.

There have been challenges – for example, some citizens prefer to report frauds physically to their local force, and it can be difficult for reporting tools to keep up with the technological developments. However, the national reporting mechanism

[9] Discontinued - produced previously by the National Fraud Authority, which has since been abolished.

offered by Action Fraud and the filtering process of the NFIB have produced a much more organised mechanism for handling frauds, including those that have multiple victims and/or cross police force boundaries. Though there remains some resistance and challenge to the take-up of a new system where tradition has so long prevailed, much City of London and NCA effort has successfully gone into outreach. At the same time, in response to specific threats, specialised squads have been funded by the private sector and government to provide a coordinated and more efficient approach to the policing of payment card fraud, organised insurance fraud and intellectual property crimes.

A modest regional approach has also developed, with regional enforcement teams (such as the Eastern Region Special Operations Unit) which cover, from an organised crime perspective, asset recovery, financial intelligence, covert surveillance and so on. Economic crime or fraud is a part of this, but the level of staffing is influenced by regional priorities. The City of London Police and many other forces work on cyber-related frauds as an integral part of their main role. However, in terms of cyber fraud specifically, the only significant targeted identification of resources outside the NCA's Cybercrime Command and the City of London Police's focus has been the Metropolitan Police's Operation Falcon (Fraud and Linked Crime ONline) Command. As of April 2015, of the 300-plus posts in Falcon, some 18% were for civilians. They mostly deal with lower level cybercrime and volume fraud. Falcon also includes a dedicated Metropolitan Police Cyber Crime Unit which deals with complex and high-value cybercrime.[10]

Specifically, Operation Falcon responds to government strategy for the policing of economic cybercrime. This strategy has been to adopt and to adapt to organised crime generally and cybercrime in particular, the four dimensions of the CONTEST counter-terrorism strategy (also known as the Four Ps Model[11]): Pursue, Prevent, Protect and Prepare – defined in chapter 2.

As the terminology is borrowed from counter-terrorism, it is unclear where repeat victimisation – a key issue for economic cybercrime – sits in this model; arguably, somewhere between Prepare and Protect. As we shift from consideration of the protection of individuals to the protection of businesses, Prepare lessons can be learned from patterns of victimisation to improve protection and reduce the impact of economic cybercrime.

Finally, there is also a draft national Protect strategy (City of London Police, 2015) which intends to:

- Maximise the effective use of the variety of tactics and techniques available to policing under the Four Ps Model, including doing more to 'protect' communities;
- Integrate national, regional and local resources and capabilities;
- Tackle both volume crime and support the NCA in tackling serious and organised crime; and
- Ensure that the focus remains on the key outcome – reducing the impact of fraud including supporting victims.

At the time of writing, the strategy is in draft form and has yet to develop an implementation timetable and performance measures or to set out how far police

[10] City of London Police resources are not separated out for such purposes.
[11] The model has not been without its critics – see, for example, Innes (2014).

forces will respond uniformly to the objectives. Nevertheless, subject to these caveats as well as resource capacity, which has not yet been calculated or allocated, the strategy aims to reduce the impact of fraud, the volume of crime and the value of the losses incurred, as well as the wider impact on quality of life for individual victims. It does this by:

- Putting in place a national economic crime prevention centre;
- Establishing a national fraud prevention network; and
- Integrating Protect activity within the overall strategy for the policing of fraud developed by the National Police Coordinator for Economic Crime.

The objective of the strategy is to deliver:

- An enhanced threat picture;
- Empowerment of individuals and organisations to protect themselves;
- More effective evidence-based 'designed-in' fraud protection bespoke to individuals and groups most at risk; and
- Engagement of the volunteering community.

In terms of Protect, the purpose behind the strategy is to promote or encourage the conditions in which crime prevention against fraud, particularly when cyber-enabled, mirrors the best aspects of physical crime prevention. This includes industry 'designing-in' crime prevention to their technologies and processes, and individuals being educated in those ways of thinking and to take responsibility for them. The police's role is then to identify and advise where they see poor application of crime prevention processes and to focus their proactive effort where the threat is greatest.

The challenge lies in the implementation of such policies, which require buy-in from bodies outside police or indeed government control. The history of designing-out crime risks from high-tech products that are normally rushed to market is not hugely positive, except where visible threats are readily attributed which would clearly lead to huge financial and reputational losses. So, for example, the recall by Fiat Chrysler in 2015 of 1.4 million Dodges, Jeeps, Rams and Chryslers with 8.4-inch touchscreens, following a demonstration that remote hacking could take control of their functions and its publication in 'Wired' magazine.[12]

These changes in policing impact on the two principal ways in which we might understand the policing landscape:

1. Reactive, in terms of following up what is reported (e.g. Action Fraud and data reported by the banks, Cifas and other businesses); and
2. Proactive, in terms of efforts to find out about and warn against unreported economic crimes – pushing further and seeking out acts not yet officially defined as frauds but which do include fraudulent aspects (for example, dating scams and other mass marketing frauds, or thefts by professionals from client accounts and estates that have not yet been identified by the victims).

Of course, a significant dimension in relation to new or emerging strategies is one of resourcing. While this report does not undertake a detailed review of interventions against economic cybercrimes,[13] the difference in approach for personal and

[12] See: www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[13] There is extensive existing research into this issue, for example: 'Net losses: estimating the global cost of cybercrime' (June 2014), Centre for Strategic and International Studies, www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf; 'The threat of cybercrime to the UK' (June 2014), RUSI,

corporate security expenditures is relevant for considering how to police crimes that have an impact on these groups. Both require assessments of future risks under conditions of uncertainty, and benefit from collective intelligence gathering. The difficulty is to work out what interventions to prioritise and how to get from where we are now to where we might plausibly be.

3.3. Data and measurement as challenges to effective policing

As highlighted in the previous section, there are both a number of challenges to the effective policing of economic crime, and new approaches being developed to address these. A key challenge to policing is the lack of accurate data and measurement of the nature, scale and impact of economic cybercrime.

Many of the data problems are due to the relatively recent emergence of cybercrime and its poor capture in crime surveys and datasets. The majority of non-government British and international studies lack rigour in this area. While large-scale government surveys – such as the Crime Survey for England and Wales (formerly the British Crime Survey); the Offending, Crime and Justice Survey; and the Commercial Victimisation Survey – adopt 'gold standard' methodologies, they have only recently begun to systematically include questions on cybercrime. This means that, currently, it is not possible to rigorously examine trends using this data.

Private security surveys are often based on breach data identified by vendor software, so they show only part of the picture. Official criminal justice-related datasets rely on both reported and officially recorded incidents of cybercrime, which is often insufficient as this relies on (i) the crime being reported by the victims and (ii) accurate recording of the nature of the crime. In the case of the former, there is often reluctance on the part of businesses to report security breaches, due to the anticipated negative financial and reputational impacts they might suffer if the damage becomes public knowledge and is picked up by the media. Individual victims similarly may report online fraud to their bank, but not to the police. In the case of the latter, as already mentioned, recording of cybercrime tends to be poorly reflected in traditional data capture methods. Even robust administrative data in the private sector (such as that provided by Financial Fraud UK and Cifas fraud prevention service) cannot include unidentified cyber-enabled frauds (for example in the category of 'bad debt'). However, there are some good practice examples. In the UK, the Oxford Internet Survey and the Information Security Breaches Survey[14] have produced cybercrime data that is of 'gold standard' methodologically over a significant amount of time. In Europe, the Eurobarometer Cyber Security Special Surveys arguably provide the most robust evidence internationally.

Briefly, some of the core aspects and issues associated with these surveys are as follows:

- These surveys tend to work on the basis of identifying an organisation or individual as a potential victim of cybercrime. That is to say, an employee (usually the person with responsibility for ICT security) is asked about security issues and

---

www.rusi.org/downloads/assets/201406_BP_The_Threat_of_Cyber-Crime_to_the_UK.pdf; and Kshetri (2010).

[14] Excluding 2010 to 2013 where a self-selecting sampling methodology was used in place of a random probability sampling methodology.

attacks in relation to their organisation, or a member of the general public is asked similar questions in relation to their home.

- These surveys therefore capture instances of 'known' victimisation where the respondent directly experiences a cybercrime attack or has been made aware of the attack by software (e.g. antivirus) or by another person (such as a payment card firm which telephones the victim about a suspect transaction). Circumstances in which victims are not yet aware that they have been targeted are not captured by the survey.
- In terms of sampling strategies adopted for surveys, random sampling yields the most representative data but the majority of surveys on business cybercrime adopt non-random or 'self-selecting' approaches, which can produce partial and biased results. This is due to the high cost of the alternative random probability approach. The resulting data pool on business cybercrime is therefore biased towards knowledgeable victims from sectors where ICT security is well embedded (i.e. there is an ICT security manager to answer the survey questions). Those who are reluctant to respond, due to a lack of knowledge or interest or fear of reputational damage from notification of a breach, are absent from the dataset, leaving a skewed picture of the cybercrime problem. Unlike in some American states where security breach notification is required by law, thus creating an accurate account of breaches (see Anderson et al., 2008) to the extent that there is compliance, the UK picture, based on surveys adopting non-random samples, is incomplete.
- Even those surveys that adopt random probability approaches to surveying cybercrime are problematic. There are conceptual issues with question wording and the assumption of knowledge on the part of the respondents, which can undermine the reliability and validity of the data produced. Such problems led the European Commission i2010 High Level Group, for example, to conclude that many of the questions in the Community Surveys on ICT Usage relating to business cybercrime attacks were unreliable.
- Similar problems have also been reported in relation to domestic surveys. A European Commission-sponsored review into cybercrime questions in the annual Information Society Surveys found questions relating to businesses were likely to be unreliable because: (i) SMEs lacked expertise with technical terms; (ii) the outsourcing of security to specialists resulted in a lack of technical details; and (iii) the general reluctance of businesses to admit a problem in their own ICT systems. In relation to domestic respondents, the review concluded that answers to some cybercrime questions may be unreliable due to: (i) a lack of expertise with technical terms such as 'virus', 'firewall', etc.; (ii) the inability to trace back any incident to a specific cause (virus/adware/spyware/fraud); and (iii) the ambiguous or vague wording of the questions (Empirica, 2007).

Large-scale random probability national surveys, such as the Crime Survey for England and Wales (CSEW), the Scottish Crime and Justice Survey, the Offending Crime and Justice Survey, and the Commercial Victimisation Survey, have included cybercrime victimisation and perpetration in their questionnaires. However, surprisingly few respondents reported cybercrime experiences, and, in the light of other data on anxiety about identity theft and the prevalence of security breaches, this leads us to question the validity of the responses to these questions. Furthermore, questions on e-victimisation have only recently become included as standard.

Given the problems outlined, it is apparent that the cybercrime data pool is currently unsatisfactory, both in terms of quality and quantity. The largest databases produced by vendors are likely to be partial and biased, while the best quality data from national surveys adopting random probability sampling techniques can suffer from poor conceptualisation and a lack of historical questions on the topic. This represents a key challenge to developing an effective policing response.

A detailed exploration of surveys of cybercrime victimisation relevant to the UK (excluding vendor statistics) is provided in the Technical Annex accompanying this report.

3.4. Key considerations and issues for policing economic cybercrime: innovation

There are three broad developments within economic cybercrime which have implications for how policing is thought about and implemented. The first (discussed in this section) concerns innovation; the second involves the offenders; and the third development concerns the defences used by economic cybercriminals.

Without attempting to reflect on the entire landscape within which cybercriminals operate, we note three examples where innovative changes are taking place that facilitate economic cybercrime. These are new opportunities, exploitation of existing opportunity and developments in how the proceeds of cybercrime are used.

3.4.1. Innovation change: new opportunities

The first innovation development is that the cyber landscape has changed dramatically as networked technologies have transformed the way that cybercrime is organised. Cyber security threats have been further escalated in recent years as cybercrime has become more professional, harder to identify and/or recognise (via rootkits, Zeus, botnets), and provides anonymity for offenders, at least under normal conditions without significant forensic investigation efforts. Cybercrimes have also become more automated,[15] and much larger and more complex with the advent of social media and 'cloud' technology, where data is stored on servers rather than computer hard drives and is accessed by users remotely, online. These trends are compounded by emerging networked technologies that are currently being planned or in progress, such as mesh technologies which join devices together, developing lateral networks, self-deleting (Tiger) texts which eradicate evidence, and cryptocurrencies (explored in section 3.4.3). The latter create alternative value systems.

Collectively, these technologies further challenge policing and attempts to impose governance, especially across jurisdictions as networked technology has increasingly enabled cybercrime to become borderless. To quote the Australian Crime Commission (n.d.):

> "the internet is particularly attractive to criminals and organised crime groups. It is globally connected, borderless, anonymous, fast, low-risk, easily accessible and has high volumes of rich data including financial data, personal information, military information and business information."

[15] For example, the fake antivirus and ransomware which lock the functionality of computers unless a ransom is paid to the offenders.

There are also new forms of service delivery and types of services. These include services supplied by reputable online suppliers to legitimate users. There is also the delivery of harmful services via more sophisticated versions of crimeware-as-a-service, where criminals require no knowledge of computers or systems because online specialists supply them with the means. This might include malicious software, supporting infrastructure or stolen personal and financial data. This makes it "relatively easy for cybercrime initiates – lacking experience and technical skills – to launch cyber-attacks not only of a scale highly disproportionate to their ability but for a price similarly disproportionate to the potential damage" (Europol, 2014: 20–21; see also Europol, 2015). The concern here is that the fear of crime that arises from such developments reduces incentives for businesses to invest in networked activities, while further encouraging the infiltration by offline organised criminals into the online markets. This widens the gap between the levels of security required by the public and business, and the levels of security that government and the police can realistically deliver.

Technology and market dynamics offer the potential for further criminalisation. For example, the new card-aggregation technologies that promise to unify payment cards on a single device could be misappropriated as tools that facilitate carding, fraudulently accessing goods or services with financial data including payment cards and bank account details. Other well-intentioned technologies that seek to streamline or enhance user experiences may carry similar risks – raising the question of the role of law enforcement and others in undertaking criminal impact assessments of such technologies to assess their exploitability by criminals and by law enforcement/intelligence bodies.

Further, it is important to recognise that the digital market is not one that is geographically restricted. As technologies become cheaper and more widely available, not only will there be an increase in global internet penetration in general, but new users and new activities and products will be incorporated into what is now a global online community, growing the pool of potential victims and potential criminal actors. Due to ease of access, a greater proportion of users than previously may be unfamiliar with technologies, which contributes to the insecurity of the internet; these users are 'easy targets' who inadvertently help facilitate criminal activity. Even large, otherwise sophisticated businesses may be vulnerable in this way, especially if they have merged component businesses with different ICT platforms. There will be both anticipated and unanticipated problems of patching vulnerabilities in the 'internet of things', through the hacking of technology products such as smartphones, which 'misbehave' as a result.

As well as these new opportunities for economic cybercrime, it is worth highlighting those innovative developments that require particular consideration from a policing perspective – the exploitation of existing opportunity and how the proceeds of cybercrime are used.

3.4.2. Innovation change: the exploitation of existing opportunity

The second innovative development in economic cybercrime is the exploitation of existing opportunity – such as intellectual property. This is a complex challenge, in that online sales and subsequent payments are recognised by the IPO as a major threat to legitimate manufacturers and retailers (IPO, 2014). Public attitudes are deeply ambiguous towards counterfeit products (Large, 2014), except in safety-critical and some health frauds. For example, the Police Intellectual Property Crime Unit (PIPCU) of the City of London Police launched its 'Wake up – Don't fake up!'

campaign in May 2015, warning consumers of the risks posed by fake beauty products. In the last 18 months, the PIPCU has suspended more than 5,500 websites selling fake luxury branded goods as well as seizing more than £3.5 million worth of fake goods, and in May 2015 made two arrests.[16]

Counterfeit goods sales can be reduced by third party economic pressures. As an example, Amazon's rules for hosted vendors – adopted after criticisms that they had a relaxed attitude to hosting counterfeits – place the onus on the vendor to source and sell only authentic products. The consequences of selling counterfeit goods include immediate suspension or termination of selling privileges, without reimbursement. Legal action may also be taken, including civil and criminal penalties.

Inter-agency collaboration is also effective, as in the UK Real Deal campaign. This was set up by the National Markets Group, consisting of industry groups and digital anti-piracy units, Trading Standards, the Department for Work and Pensions, the police and the UK IPO, to encourage business to commit to trading in legitimate goods and to refuse to sell illegal digital media including DVDs, music, games and software. Currently, 200 markets have signed the Real Deal Charter, which is supported by 50 local authorities, 34 Trading Standards services and 23 private operators.

Addressing insider theft of IP is more complex. In terms of information rather than products, ongoing efforts are being made to tackle this through detailed analysis of previous cases and identification of characteristic patterns of conduct ('signatures') that indicate an insider is attempting or is likely to exfiltrate data. Care needs to be taken by corporate boards as well as by security functions in large businesses, SMEs and public sector organisations to investigate the range of data held by the organisation, the risks of this data being sold, lost or stolen and the value of the data should this occur.

3.4.3. Innovation change: the proceeds of economic cybercrime

The third innovative development within economic cybercrime is the growth of virtual market currencies that fall outside normal financial systems. 'Cryptocurrencies' are a means by which online users can circumvent the money controls of the state and, in theory, may be traded anonymously. The regulation or prohibition of cryptocurrencies is open to debate. At present there is no legislation in European countries regulating their use. In July 2014, the European Banking Authority urged national policymakers to discourage payment institutions from buying or selling virtual currencies, pending a regulatory framework.[17]

The most popular virtual currency is Bitcoin, launched in 2009, which exists through an open-source software program. Bitcoins are stored entirely on computers, are not backed by any government or central bank and allow the owners to trade and move money from place to place almost as cheaply as sending email.[18] Bitcoin showed promise as a low-cost mechanism for e-commerce and money transfer, but can also be used for criminal purposes. The creation of a 'wallet' generates a Bitcoin

[16] For more information, see: www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Two-arrested-in-%E2%80%98Wake-up-%E2%80%93-don%E2%80%99t-fake-up!%E2%80%99-campaign.aspx.
[17] See 'European Banking Authority, Opinion on Virtual Currencies' (EBA/OP/2014/08).
[18] See Böhme et al. (2015) for a review.

address for the transactions and a personal key of 32 characters or more. Details are available online[19] about all transactions made from one Bitcoin address, and the internet protocol address from where a transaction was initiated. However, wallet owners can use many tools to hide their identity, such as the Bitcoin Laundry (designed to unlink Bitcoin addresses from each other) and the Bitcoin Fog (a wallet designed to mix up all funds transferred so they are indistinguishable from each other). When requested, funds are paid out in multiple randomised transactions for further anonymity of the source of the money. Some such 'tumblers'[20] even introduce delays and use random fees that they deduct from the incoming amount, making it difficult to link the incoming and outgoing transactions. Transferring Bitcoins without access to the personal code of the wallet owner requires sophisticated technical tools and complicated processes.

There is potential, then, for cryptocurrencies to be used for financial value transfers and money laundering. However, this presents problems of effort and liquidity. An additional obstacle is that cryptocurrencies cannot be used to buy licit items unless converted into legal tender. Converting cryptocurrencies into cash without a trace is more difficult; very few vendors currently accept cryptocurrencies for purchases, though the number is increasing. There are few Bitcoin ATMs, so most users have to convert their funds by bank transfer or going to a bureau de change. In reality, cryptocurrency is not as anonymous as initially envisaged.

Moreover, the market for cryptocurrencies has been extremely volatile. A meteoric rise in the value of Bitcoins and Litecoins[21] in the winter of 2013/14 was followed by a crash; at the time of writing, they are trading at about a quarter of the value of the early 2014 peak. The use of questionable markets that do not require much authentication to process transactions is exceedingly risky, with cryptocurrency wallets being hacked or the market potentially going bust. Consequently, while some people do try to store, transmit or launder wealth via cryptocurrency, market volatility coupled with security risks mean that it is not a reliable way of fulfilling those goals at scale.

The criminal potential of cryptocurrency technologies has yet to be determined and until cryptocurrencies have much more widespread expenditure opportunities, they will continue to be of limited value to criminals. On the other hand, in terms of markets and their functioning, it is important to anticipate trends and practices (see section 3.6) and to anticipate consequences. There are no obvious methods by which cyber-enabled money laundering can be reduced, beyond a continued focus on enhancing general anti-money laundering efforts. Some European investigations have led to seizure of Bitcoins and their transfer to the authorities. Speed in asset freezing is a particularly important factor in preventing serious economic crimes, but this is affected by the speed of identification and reporting to the authorities (or to a court for private action) as well as by the speed of response when alerted.

---

[19] See: http://blockchain.info.

[20] 'Tumblers' are services, often operating on Tor, which allow users to transfer their cryptocurrencies into a pool of funds and then receive them back (minus a small commission) into newly generated 'clean' addresses, thereby breaking the financial trail.

[21] Litecoin is another type of cryptocurrency, similar to Bitcoin – a peer-to-peer internet currency that enables instant, near-zero cost payments to anyone in the world. For more information, see: https://litecoin.org/.

3.5. Key considerations and issues for policing economic cybercrime: offenders

Evidently, innovation in economic cybercrime raises a range of issues and considerations for policing approaches. However, there are other areas of challenge that also require attention – the offenders themselves and the defence mechanisms used by cybercriminals for protection against policing (see section 3.6).

3.5.1. Types of offenders and offences

Table 3.1 presents a categorisation of the key types of offenders and offences in economic cybercrime and the main characteristics of each group (further detail can be found in the Technical Annex, available online).

The categorisation highlights both the range of threats and the divergence between ideological and political threats which fall within our definition of economic cybercrime (covering both cyber-dependent and cyber-enabled economic crime).

Table 3.1: Categorisation of the types of offenders and offences in economic cybercrime

Category	Target	Organisational type	Economic crime threat[22]
Amateur hackers	Security breaches	Individual/amateur	Low
Crackers and leechers	Software security, copyright piracy	Individual/amateur	Low
Pirates	Security, copyright piracy	Individual/ organised	Low
Attackers	IP theft, extortion	Criminal/organised	High
'Black hat' vulnerability scouts	ICT vulnerability	Individual/amateur	Low on performance; high on consequences if vulnerabilities sold or passed on
Professional malware developers and script kiddies	ICT vulnerability and means to exploit them	Individual/amateur	Low on performance; high on consequences if vulnerabilities sold or passed on
Carders and money mules	Data theft	Organised	High
Extortionists	Botnets and malware in order to set up extortion rackets	Individual/amateur/organised	Medium
Phishers and social engineers	Spam for data	Organised	High
'Black hat' fraudsters	Script attacks	Organised	High
Cheaters	Online gaming	Individual/organised	Medium

[22] Authors' assessment from the data.

Category	Target	Organisational type	Economic crime threat[22]
	and gambling cheating		
Click fraudsters	Cheating ad clicks and views	Individual/organised	High
Hacktivists	Political hacking	Individual/organised	Low

3.5.2. What about the role of organised crime?

One significant issue here is understanding how far the threats emanate from the same or different sources in terms of economic cybercrime. Another, concerning the general categorisation of offenders in Table 3.1, is to what extent 'organised crime' is involved: the latter would typically generate more interest from law enforcement. The term 'organised' is used for a multiplicity of forms of organisation, from small loose confederations to Mafia-type organisations. Those allegedly involved in the Libor and Forex rate-fixing scandals used ICT in their schemes, and their alleged activities might fit the definition of organised crime; but one might imagine such market manipulation occurring via hacking by unauthorised persons also, though it might be detected more quickly if repeated than if conducted by regular market participants. A key question here – and one particularly relevant to a law enforcement approach – is, 'What is organised crime?'

The Australian Crime Commission (n.d.) distinguishes between three types of organised crime groups:

- Traditional organised crime groups that use ICT to enhance their regular criminal activities;
- Organised cybercriminal groups that operate exclusively online; and
- Organised crime groups made up of ideologically and politically motivated individuals who use ICT to facilitate their criminal conduct.

The UK Serious and Organised Crime Strategy states that 'organised crimes' are serious crimes planned, coordinated and conducted by people working together on a continuing basis where the motivation is often, but not always, financial gain.

While there are claims that organised crime in this traditional sense is making a foray into cyberspace, the evidence indicates otherwise, at least in the classical sense of Mafia-type groups (Lusthaus, 2013). It is plausible that some organised criminal groups are taking advantage of ICT in order to facilitate their otherwise offline crimes. Moreover, it is possible that such groups are employing or bankrolling individuals or small groups that do engage in cyber-dependent crime. But the likelihood that these organisations have the intellectual capital necessary to navigate the internet as a conduit for criminal activity is, as yet, unproven. Setting aside economic crimes, evidence indicates that the use of ICT to execute criminal activity generally has been modest (Montoya, Junger & Hartel, 2013; Pyrooz, Decker & Moule Jr, 2013).

Of course, some organised criminal activity does take place online. It might involve a decentralised and/or networked group of actors who have never met outside cyberspace. This presents new challenges to law enforcement, particularly as it attempts to disrupt and disable complicated networks with horizontal and interchangeable command structures.

The innovation enabled by the internet allows criminal entrepreneurs to operate relatively efficiently. Currently, there are several technologies and forums that

criminal actors can take advantage of in order to anonymise themselves and facilitate criminal activity. This results in an arms race between criminal developers and those who try to foil them. The difficulty in protecting against unknown vulnerabilities is high, making it hard to stay ahead of criminal actors. Law enforcement has had some limited success in penetrating these technologies to identify and capture criminals, and/or has taken advantage of sloppy use of these technologies to find those who hide behind them.

However, the speed and capacity of cybercriminals to develop and guard what they do, how they do it and where they do it in cyberspace should not be underestimated. Law enforcement experiences have shown that cybercriminals are very efficient in learning from policing operations and responding to these with improved software security and encryption, and mechanisms for conducting criminal activity (as, for example, with the Darkode forum).[23]

3.6. Key considerations and issues for policing economic cybercrime: cyber defences

Semi-licit or illicit goods can be acquired in largely licit, grey and black markets; the label is a matter of degree, and it may be more helpful to describe them as 'underground' markets, with or without encryption. They provide access to products or host interactions which can be legal but which can also be exploited for criminal purposes: for example, a vulnerabilities market where vulnerabilities are identified and cyber security patches developed. A grey-marketer would use this information to sell an attack, knowing that most users would not be attuned to the available patch or fix to protect against it (Ablon, Libicki & Golay, 2014). Black markets, by contrast, trade exclusively in illicit products including vulnerabilities, attack frameworks, data, contraband, counterfeit items and stolen merchandise.

Cryptomarkets exist in a variety of locations and employ technologies not commonly used by average internet users, such as bulletin board systems, Usenet, the Tor network and internet relay chat (IRC) (Johnson, 2009). These markets have lifespans which date from months to a few years as law enforcement shuts them down. So far, new markets have consistently emerged to fulfil the demand left by the collapse of old ones, making prevention and implementation of Protect and Prepare difficult. Disruption does have an effect, however, as forcing such markets into short lifespans increases the risk of participants losing money even if they are not being successfully prosecuted. On the other hand, those operating in such markets are often effective at disguising or denying access to their markets using a number of cyber defences, including:

- **Bulletproof hosting:** These are crimeware services that protect cybercriminals from law enforcement, and are typically hosted at offshore locations which are difficult for law enforcement to access. If attacked, these services are designed to reroute in order to avoid interruption (Bradbury, 2014).
- **Anonymisation:** Experienced users who attempt to maintain online anonymity can change their user names and disguise their internet protocol address. Skilled cybercriminals continue to operate through forums with administrators who vet participants (Lusthaus, 2012).

[23] See: http://krebsonsecurity.com/2015/07/the-darkode-cybercrime-forum-up-close/ – which mutated into the Darkcode forum after arrests.

- **Alternative cyber networks:** In an effort to be anonymous, some internet denizens use platforms such as Usenet or, more recently, Tor and P2P networks such as OpenBazaar and I2P. Usenet groups have, in the past, facilitated black markets for viruses and child pornography (Ghosh & Turrini, 2010; Jaishankar, 2011). Participants are required to follow particular techniques rigorously to ensure that they achieve true anonymity (Dingledine & Mathewson, 2006).
- **Encryption:** Companies are starting to provide software and hardware that claim to be secure from prying eyes. Offenders who attempt to anonymise their actions risk discovery if anyone they communicate with does not engage in best practices. This is illustrated clearly in the FBI's take-down of Ross Ulbricht, better known as the former Silk Road administrator 'Dread Pirate Roberts', and the subsequent tracing of his Bitcoins to the cryptomarket he once managed. Information was recovered from his unencrypted computer after he was arrested while online (Oakford, 2015; Weaver, 2015).

3.7. What do these issues mean for the policing of economic cybercrime?

As the internet continues to become entrenched in our daily lives and we share increasing amounts of data, cyber-enabled and cyber-dependent crime will increase if only because the permutations of incentive, opportunity, and low risk of investigation and prosecution traditionally invite criminal activity. The task ahead is to manage the risks so as to devise and ensure Prevent and Protect interventions that complement patterns and levels of use as well as to minimise the negative socio-economic impact of such crimes. This inevitably involves making evidence-based judgements about trends in offending and impacts on different sectors of the population, directly and via business and government.

There are efforts to head off some criminal actors before they can make contact with their potential victims, such as applying spam filters, which are nearly universal throughout all email providers. Some companies which provide internet browsers, such as Google and Mozilla, and internet service providers have attempted to take on the role of guardians by providing software, free of charge, which alerts users to potential fraudulent websites or malware.

However, as the licit market moves towards standard anonymisation for all users as a privacy measure, it is important to pre-empt the vulnerabilities and legal difficulties that will present themselves (Blakeslee, 2012; Denning & Baugh, 1997). This task is much easier said than done. The evolution of botnets and the sophisticated attacks that emanate from them are also daunting problems. Given the central role that botnets play in attacks, it is worth attempting to combat them so long as they remain a significant means of conducting cybercrime (Amoroso, 2012; Bleaken, 2010).

The speed at which the internet and internet behaviour evolve is also an ongoing challenge when attempting to keep up with the threats and risks posed by economic cybercrime (Calderoni, 2010). Accordingly, there is a need to improve levels of proactive as well as reactive responses and focus to match those that policing has achieved in other areas such as organised crime and corruption. It is worth noting here the objectives of the 2011 'UK Cyber Security Strategy',[24] which set

[24] "Objective 1: The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace; Objective 2: The UK to be more resilient to cyber-attacks and better able to protect our interests in cyberspace; Objective 3: The UK to have helped shape an open, stable and

out a vision for 2015; these reflect the continuing need to review and refresh that vision and strategy.

Given that the internet is an important driver of economic growth (Manyika & Roxburgh, 2011) it is clear that government actors need to take steps to ensure that criminal actors do not offset these gains. The speed of post-strike interventions is critical to reducing harms – the time lag between implementing new criminal strategies and the effective countering of those strategies leads to economic losses. However, given the disadvantages of being attacked, and the costs required to minimise the impact of such attacks, the problem that law enforcement, organisations and governments will continue to face is the 'cost-to-pay-off' analysis vis-à-vis cybercrime.

As it is the sovereign responsibility of the state to protect its citizens, it is arguably reasonable to demand that government provide the necessary policing responses to economic cybercrime, although these responses must inevitably compete with other agendas and priorities. As noted earlier, the police are not required to be the sole player in the law enforcement landscape; rather, it is more about identifying specific roles and responsibilities in that landscape, as well as the role of other agencies, and the promotion of partnership and other collaborative arrangements.

The crux of the challenge lies in the speed and volume of economic cybercrime, the global nature of the internet, and the scale at which this allows crimes to be committed. Subsequently, responsibilities for global protection and the pursuit of offenders lie with a plethora of national governments, requiring strong and effective collaborative networks.[25] Differences in political regimes and economic success raise the risk of 'free-rider' governments that refuse to participate in a global protection regime against online criminal actors. This is an issue that has been rising up the political agenda, though it is somewhat undermined by the politics surrounding allegations of state-sponsored hacking for economic and political intelligence and to cause damage. In this context, frauds against individuals and SMEs are normally subordinated.

3.8. Summary

This chapter has explored the current policing landscape and approach to economic cybercrime, and has identified some of the key challenges linked to the nature of economic cybercrime.

In the face of competing priorities and agendas, the general approach to fraud by the English and Welsh police forces has tended to focus on and reflect one particular significant policy agenda as identified in the 2011 government strategy 'Fighting Fraud Together'. This prioritised organised crime and fraud committed by organised crime groups (OCGs). Where fraud squads have not been abolished, they have merged with Serious Crime Units or been rebadged as Economic Crime Units in order to align existing expertise and resources with government priorities to address OCGs, corrupt professionals and asset recovery. At the same time, and as a consequence of a number of initiatives that emerged from the 2006 Fraud Review,

---

vibrant cyberspace which the UK public can use safely and that supports open societies; Objective 4: The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives."

[25] These currently include Europol's European Cybercrime Centre (EC3), the FBI's Strategic Alliance Cyber Crime Working Group, and the Interpol Global Complex for Innovation.

there has been a national approach to the reporting and recording of intelligence relating to fraud that has recently culminated in a national strategy.

Until issues of local priorities and resourcing are addressed, there may be a gap between a national strategy and local delivery; the regional response appears at present to address primarily the organised crime dimension of economic crime (in both senses of the term 'organised'). However, the strategy itself acknowledges that:

> "while fraud is rising in its current volumes, it cannot be satisfactorily dealt with by the police alone, and its volume needs to be kept at a manageable level – crime prevention. Furthermore, the first obligation of the police is to prevent crime and given that much, if not most, fraud relies on some degree of participation by the victim, this holds particularly true for this crime type." (City of London Corporation, 2015: 28)

Certainly, taking government, business and individuals as a whole, the dominant thrust of policy and action is in the Protect and Prepare sphere. Policing plays a complementary role in that space and has potential for a greater role (possibly with a tighter focus on the types and perpetrators of crime) in terms of Pursue.

Such a response has, however, to understand the specific issues associated with cybercrime. These include the range of victims and crimes, which can be committed from a single source or by a number of perpetrators; the ability to insert or disguise the criminality as part of legitimate cyber activity; the speed and instantaneous nature of the criminality itself; and the exploitation of jurisdiction and territorial boundaries in terms of perpetrator, means or mode of delivery and location of victim. All of these considerations throw up a number of strategic questions pertinent to any response to economic cybercrime, such as who else should be involved and in what capacity, and what should be the specific roles and responsibilities of the police:

- Cybercrime is an evolving law enforcement issue which requires clarification of the roles and responsibilities of a range of agencies and stakeholders, determining the specific foci of law enforcement responses and the deployment of appropriate resources to do this properly.
- Policing resources are reducing, driven as they are by competing priorities and agendas in a time of economic stringency. Those initiatives that are in place are emerging rather than comprehensive and established.
- Cyberspace is constantly evolving, for an extensive range of functions, services and products, while also providing platforms for aggregation and innovation. Most of these outstrip preventative and other measures for control protection.
- Cyberspace has multiple actors whose typologies, levels of engagement in criminality and particular types of criminality and methods of organisation and operation do not lend themselves easily to existing definitions or ways of understanding.
- Cyberspace is developing its own marketplaces and financial arrangements that require specialist awareness and access if they are to be addressed.

These are just some of the issues that a future approach to the policing of economic cybercrime needs to consider. The following chapter explores the impacts of economic cybercrime on different groups, considering the existing evidence base to explore the responses to the issues discussed in this chapter. The meaning of these developments for trying to tackle and police economic cybercrime is then explored in chapter 5.

4. The impacts of economic cybercrime: who, what and how much

This chapter explores in detail how different types of economic cybercrime affect certain groups, focusing in particular on individuals/the general public and businesses, with some consideration of government entities also. The analysis draws largely on the existing evidence base and the chapter goes on to consider what is currently being done to help police the impacts of economic cybercrime for each group, and to identify where the gaps are. This analysis is central to developing preventative and investigative policing responses.

This chapter is divided into two main parts. In the first part (sections 4.1 and 4.2), the report draws on a literature review to identify key themes and threats to business and individuals, and analysis of Action Fraud data, while noting that the evidence base is not as robust as it should or could be.

In the second part (sections 4.3 to 4.6), we address the issues facing the police if they wish to respond to specific categories of victims and potential victims. We do not specify what the police should do in strategic, policy or operational terms but simply identify areas of possible response; the specificity is addressed in chapters 5 and 6.

4.1. The main themes of economic cybercrime

As identified in chapter 3, the key barrier to a better understanding and tackling of cybercrimes is the lack of reliable data on their frequency and the nature of their impact on businesses, the national infrastructure and the general public.[26] These data issues include (i) inconsistencies in the information held by various stakeholders; (ii) lack of data sharing protocols; (iii) confidentiality and anonymity of respondents; (iv) failure to adopt 'gold standard' data collection practices, linked to under-reporting; and (v) knowledge and perception of victimisation. This combines with a failure to report (or decisions not to report) identified crimes in the first place in some instances, and therefore results in significant under-reporting of economic cybercrime.

Despite these issues and areas of challenge, the available research and data, if treated with due care, play an important role in understanding economic cybercrime. In this section, we focus on themes drawn from the most 'satisfying' datasets in relation to two key groups affected by economic cybercrime: individuals and businesses. We also explore what data is held by police in the UK on economic cybercrime through Action Fraud.

4.1.1. Malware and virus attacks

The main perceived threat or risk associated with cyberspace for both businesses and individuals is the prevalence of malware and virus attacks (these can be cyber-dependent and/or cyber-enabled).

Data from the UK Information Security Breaches Survey (ISBS) shows that, in 2010, the reported prevalence of malware infection, insider misuse and unauthorised access

[26] Several papers provide insightful reasons why existing data is flawed: see, for example, Anderson et al (2008, 2013); Casper (2007).

had a sharp increase, and there was a slightly modest increase in reports of theft and fraud. Reports of insider misuse and unauthorised access peaked at new all-time highs (42% and 49% respectively), while malware attacks returned to near their peak prevalence in 2004, having declined between 2004 and 2008.

In a 2015 report by PwC, 90% of large organisations said that they had suffered a security breach, up from 81% in 2014. Small organisations recorded a similar picture, with 74% reporting a security breach, up from 60% in the previous year (HM Government, 2015). Of these, 11% of respondents changed the nature of their business as a result of their worst breach. The average cost of the worst single breach suffered by organisations surveyed has gone up sharply for all sizes of business. For companies employing over 500 people, the starting point for breach costs - – which includes elements such as business disruption, lost sales, recovery of assets, fines and compensation – commences at £1.46 million, up from £600,000 the previous year. For small businesses, the lower end for security breach costs increased to £75,200, up from £65,000 in 2014. Malicious software affected nearly three-quarters of large organisations and three-fifths of small organisations, for whom there was a substantial rise. Three-quarters of large organisations suffered a staff-related breach (up from 58% in 2014) and nearly one-third of small organisations had a similar occurrence (up from 22% the previous year).

The 2012 and 2014 UK Commercial Victimisation Survey (CVS) found that computer viruses were the most common type of online incident among UK businesses. The 2014 CVS estimates that there were 136,000 incidents of online crime against businesses in the wholesale and retail sector in the 12 months prior to interview. This is a notable decrease compared with 2013 (234,000 incidents), but an increase compared with 2012 (69,000 incidents) (Home Office, 2015b).[27] Around 10% of all wholesale and retail premises experienced at least one type of online crime in the last year, with 9% experiencing a virus and 2% experiencing hacking in the 12 months prior to interview. Computer viruses accounted for 87% of all online crime (although the low levels of other types of online crime may be because these crimes do not come to the attention of victims; for example, in the case of phishing, the offending email may be caught by spam filters, or victims may not know that their computer systems have been hacked).

Similarly, there is an upward trend in recorded domestic phishing attempts, indicating, as with business-recorded cybercrime, that cyber-enabled fraud is on the increase.

4.1.2. The volume of economic cyber-related incidents

Fraud is not currently covered by the CSEW. However, additional analysis by the Office for National Statistics (ONS) on existing questions in the 2012/13 CSEW suggests that plastic card fraud and building society fraud taken together could potentially have contributed between 3.6 and 3.8 million crime incidents in 2012/13 – almost half the total crimes against individuals (7.3 million in the year to September 2013) (ONS, 2015: 89). CSEW data does show that, for the year ending September 2014, 5.2% of payment card owners were victims of card fraud. This is an increase of 4.6%,

[27] We would propose a caveat, here: it may be surprising that so few businesses did suffer from viruses but the percentage that were not actual victims doubtless owe much to their investment in cyber security measures rather than to their lack of vulnerability to attack. Attempts in such cases are likely to be unknown except to the cyber security vendors.

and reverses the trend of small reductions in payment card fraud over the last few years.

It is also worth noting that the financial services industry is not alone in being subject to significant levels of economic cyber-related incidents. Although over half of UK adults are aware of mass-marketing frauds, approximately 2.6 million individuals have fallen victim to these scams in some way – some 800,000 UK adults in 2012 alone (Whitty, 2013; ONS, 2013). Data collected by a YouGov survey in April 2013 found that, in their lifetime, approximately 500,000 UK adults had fallen victim to a dating scam; around 900,000 had been conned by a boiler room scam; 700,000 by a charity scam; 900,000 by a 'need funds for an emergency' scam; 700,000 by an inheritance scam; and 800,000 by a lottery scam. There is also a significant repeat victimisation problem, as a quarter of those scammed had been subsequent victims of another or a similar scam. This is consistent with earlier surveys commissioned by the Office of Fair Trading showing high victimisation and repeat victimisation risks (Levi et al., 2007).

4.1.3. Financial losses to victims

There is also a need to establish the financial losses to victims as a consequence of economic cybercrime. Given that many datasets record significant levels of and concerns about cybercrime, it is necessary to distinguish crimes where the primary intentions are disruptive and malicious rather than financial, and where the associated costs are more to do with recovery and resilience than losses. While useful, the number of cases tells only part of the story. To get a more realistic idea of the actual impacts or losses of such frauds on business or individuals, it is better to think about losses as a proportion of turnover or (more difficult to obtain and analyse) as a proportion of profit. Industry data has now been released showing some fraud rates per capita card expenditure: the loss to fraud was 0.7p per £100 spent via contactless payments. In 2014, card fraud losses were 7.5p per £100 spent, compared with a peak of 12.4p per £100 spent in 2008. The overall UK e-commerce fraud-to-sales figures equated to 9.2p per £100 spent in 2014. Online banking fraud losses were marginally greater in 2014 than in 2008, but e-commerce fraud went up from £181.7 million in 2008 to £217.4 million in 2014. For online banking, although the sterling value of losses was greater in 2014, the rise in online banking volume means that the effect on the industry was significantly less than in 2008 (setting aside any effects from changing industry profitability rates) (FFA UK, 2014).

4.1.4. Targeted prevention strategy and risk areas

Is there a correlation between a targeted prevention strategy and risk areas? The main losses to the banking sector between 2003 and 2014 related to internet-enabled CNP[28] fraud, offline CNP fraud (i.e. by telephone) and internet banking fraud, as counterfeit card frauds declined due to the introduction of Chip and PIN. Offline CNP fraud declined in the early 2000s with the growth of internet shopping (and related fraud). Losses from internet-enabled CNP fraud (i.e. e-commerce fraud) increased rapidly in the early 2000s and totalled £217.4 million in 2014, when they accounted for 45% of all card fraud and 66% of total remote purchase fraud.

[28] CNP (card-not-present) fraud involves transactions where the merchant, retailer or other service provider does not have physical access to the payment card; examples are transactions by telephone, mail order or internet.

Overall, losses on purchases made using a card remotely – those made online, over the phone or by mail order – rose 10% in 2014 to £331.5 million, while the number of fraud incidents rose 7% in the same period. In recent years, losses to UK retailers have remained stable and this rise has been almost entirely the result of UK cards being used fraudulently abroad in those countries (like the US) which do not have Chip and PIN or other security measures applied to online orders. Internet-enabled CNP declined between 2008 and 2010 with the introduction of security measures such as American Express SafeKey, MasterCard SecureCode and Verified by Visa, but then began to rise again (FFA UK, 2014).

There is also an element of customers being scammed, for example in investment scams, dating scams and wine scams. Typically, not all of these cases are reported to the victim's bank and are therefore also excluded from the numbers. Via Financial Fraud Action (FFA) UK – the fraud coordination body for the UK financial services industry – the banking industry is working to educate customers to protect themselves against this type of scam and report it to their bank. In future press releases, FFA UK will also be expanding the data provided to include attempted/prevented fraud, which will help demonstrate more fully the scale of attack being mounted against UK account holders via their financial institutions.

4.2. The current UK situation

The analysis in section 4.1 identifies four key themes that emerge from official research. We now cross-reference these findings with incident reporting data for the UK, to Action Fraud (see 4.2.1) and other UK industry bodies (section 4.2.2).

4.2.1. Action Fraud

Action Fraud collects data for reported frauds by UK individuals and businesses, excluding reports for 'plastic crime' which is collected by Cifas and FFA UK, to avoid double counting (see section 4.2.2). Analysis of data from Action Fraud covering October to December 2014 (Q4 2014) shows, overall, a considerable rise in reported fraud in the UK.[29] On the other hand, the data indicates both divergence and convergence with the material reviewed in section 4.1, in terms of victims reporting a loss or an attack.

First, the types of frauds reported: overall, there were 106,681 reported incidents,[30] 4,062 (4%) of which involved computer misuse crime, a much smaller proportion than might have been expected. The two largest components of computer misuse crime involved viruses or malware, and hacking of emails and social media. By volume, the single largest types of reported fraud are banking and credit industry frauds (33%), a large proportion of which (18%) are cheque, plastic card and online bank account frauds. This is followed by non-investment frauds (29%), which include online shopping and auctions (12%) and also computer software service frauds (8%). The latter may include, for example, fake antivirus and ransomware. Advance-fee payments (and their different forms) follow (14%). Specific technology-related

[29] Caution should be exercised when talking about earlier periods, since reporting and recording standards have changed in the interval ('Crime in England and Wales', ONS, 2015).

[30] There are some inconsistencies in the Action Fraud data relating to the total number of cases, due to missing data. For the purposes of this research we have worked with the available detail for each issue. Totals match up closely wherever possible. It is also worth highlighting that the analysis presented in this report is not comparable to ONS analysis of Action Fraud data due to different datasets covering different time periods.

offences are less prevalent, covering telecom industry fraud (misuse of contracts) at 5%. The remainder of the offences are relatively small in volume. Table 4.1 presents data for reported crime by volume by category (including the two largest sub-categories within each).

Table 4.1: Typology of reported frauds, Q4 2014

Fraud type	No. of frauds	Proportion of total reported frauds
Banking and credit industry fraud	**34,913**	**32.7%**
Cheque, plastic card and online bank accounts (not PSP)	19,127	18%
Application fraud (excluding mortgages)	10,091	9.5%
Non-investment fraud	**30,490**	**28.6%**
Online shopping and auctions	12,405	11.6%
Computer software service fraud	8,455	7.9%
Advance-fee payments	**15,065**	**14.1%**
Other advance-fee frauds	7,498	6.7%
Lender loan fraud	2,078	1.9%
Telecom industry fraud (misuse of contracts)	4,817	4.5%
No identified category	**12,404**	**11.6%**
Categories as % of total	**92,872**	**87%**
Total	106,681	100%

Second, the data highlights that the internet has not always been the source of or medium for the initial contact that leads to a fraud. The single most common way that offenders contacted their victims was by phone or text (35%). Almost a fifth (18%) were contacted after visiting a website, 12% in person, 11% by letter or fax and 8% by email. From these figures, the overall degree of involvement of network technologies can be estimated, though with some caveats.[31]

[31] Percentages are indicative rather than absolute; adjusted for cyber-involvement (email+visit to a website+web forum+(0.66) of TV, radio or online advert, or flyer) ('in person' and 'other' have been excluded); classification depends on when the victim feels the fraud began, e.g. at first contact, or the point at which money was being requested. With most frauds today, online usually goes offline to get the money; blanks are excluded and percentages are based upon total known information; 'simplified' means main offence and information are joined.

Table 4.2: First contact method (offender), Q4 2014

Contact method	No. of frauds	Proportion of total reported frauds
Phone call, text message or similar	31,088	35%
Visit to a website	15,587	18%
Other	11,625	13%
In person	10,932	12%
Letter or fax	10,159	11%
Email	6,859	8%
Web forum, chat room or similar	1,582	2%
TV, radio or online advert, or flyer	462	1%
Newspaper, magazine	179	0%
Total	**88,473**	**100%**

The data in Table 4.2 suggests that reported fraud offences using networked technologies are actually relatively low as a proportion of the total. However, it is likely that the data underestimates the extent of cyber-involvement throughout the crime, because reporting reflects only first contact by the offender. Many economic crimes involve a cyber-element at a later point – for example, a phone call generated via voice over internet protocol (VoIP) might be used to make initial contact and 'hook' a victim, after which a fraudster will take over. Subsequently, it is not always clear for classifiers (and victims) from the data when the fraud actually began. This relates to a wider challenge of defining fraud: is it with the initial contact or later on when an attempt to extract money takes place? Some victims are carefully groomed and often will not realise the fraud until well after the event.

Nevertheless, the data does provide a clear indication of the different levels of cyber-involvement in the different offences. Though, at this point, the data does not reveal whether it is cyber-enabled or cyber-dependent (or indeed cyber-assisted, or not relevant); this can only be seen when it is cross-tabulated by fraud type.

From another perspective and although offences that use networked technologies are relatively rare – a fact that may reflect the newness of Action Fraud, different reporting patterns of individuals and businesses, and different victimisation profiles – the differentiation by crime and the cyber-involvement is important. When the data is ordered according to the level of estimated cyber-involvement, it cuts across[32] a number of the Action Fraud data headings (see Table 4.3). The data presented in Table 4.3 highlights the degree of estimated cyber-involvement for specific types of fraud and helps to better understand where cyber technologies are involved. For example, advance-fee payments are not generally indicative of cyber-involvement, but specific forms of advance-fee payment fraud offending are. Traditional 419 advance-fee payment frauds are very low in cyber-involvement (15%), whereas

[32] Our analysis orders the fraud types in terms of cyber-involvement via first contact. Including all of the types of cybercrime (assisted, enabled and dependent), it is calculated from the combination of the following values (email+visit to a website+web forum+(0.66) of TV, radio or online advert, or flyer) ('in person' and 'other' have been excluded).

others, such as dating scams (88%) and online shopping and auctions (86%) are the most cyber-involved.

Table 4.3: Level of cyber-involvement, first contact method (offender), Q4 2014

Action Fraud category/sub-categories	Total n=	Cyber-involvement	% of cyber-involvement
Dating scam	835	737.6	88%
Online shopping and auctions	11,350	9,754.2	86%
Counterfeit cashiers' cheques	559	428.4	77%
Rental fraud	773	572.8	74%
Ticket fraud	910	655.0	72%
Computer virus/malware/spyware	1,370	975.2	71%
Denial of service attack	47	26.0	55%
Mandate fraud	966	520.4	54%
Hacking – social media and email	1,047	524.0	50%
Denial of service attack extortion	10	5.0	50%
Hacking extortion	106	53.0	50%
Mortgage-related fraud	144	69.0	48%
Fraudulent applications for grants from charities	9	4.0	44%
Hacking – server	86	29.6	34%
Hacking – personal	428	132.0	31%
Business trading fraud	124	38.0	31%
Other regulatory fraud	72	22.0	31%
Prime bank guarantees	12	3.6	30%
Other consumer non-investment fraud	4,703	1,358.0	29%
Fraud by failing to disclose information	160	46.0	29%
Pension fraud by pensioner (or their estates)	7	2.0	29%
Charity fraud	238	63.2	27%
Insurance broker fraud	39	10.0	26%
Pyramid or Ponzi schemes	164	38.6	24%
Other fraud	11,553	2,250.8	19%
Cheque, plastic card and online bank accounts (not PSP)	13,437	2,449.4	18%
Consumer phone fraud	352	61.6	18%
Fraudulent applications for grants from government-funded organisations	41	7.0	17%
Other financial investment	1,017	170.8	17%
Bankruptcy and insolvency	18	3.0	17%
HM Revenue & Customs (HMRC) fraud	6	1.0	17%
Lender loan fraud	1,929	319.2	17%
Other advance-fee payments	6,794	1,017.6	15%
Inheritance fraud	743	109.6	15%
419 advance-fee payment	550	80.2	15%
Door-to-door sales and bogus tradesmen	1,242	170.2	14%
Banking and credit industry fraud – information (only)	3,637	495.6	14%

Action Fraud category/sub-categories	Total n=	Cyber-involvement	% of cyber-involvement
Share sales or boiler room fraud	387	44.0	11%
Dishonestly retaining a wrongful credit	32	3.6	11%
Corporate procurement fraud	33	3.0	9%
Pension fraud committed on pensions	24	2.0	8%
Insurance-related fraud	253	20.2	8%
Lottery scams	1,238	97.2	8%
False accounting	133	9.6	7%
Fraud recovery	368	26.0	7%
Time shares and holiday club fraud	219	15.0	7%
Application fraud (excluding mortgages)	6,350	428.8	7%
Retail fraud	1,660	109.6	7%
Fraud by abuse of position	500	29.8	6%
Pension liberation fraud	230	12.0	5%
Telecom industry fraud (misuse of contracts)	3,194	119.2	4%
Corporate employee fraud	451	12.6	3%
Computer software service fraud	7,813	167.0	2%
Hacking – PBX/dial through	100	2.0	2%
Department for Work and Pensions (DWP) fraud	9	0.0	0%
Passport application fraud	1	0.0	0%

Though useful in identifying what types of economic crimes most involve cyber technologies, there are a number of issues with the data. First, the level of cyber-involvement within categories varies significantly in terms of initial contact. For example, within advance-fee payments, first contact method for lottery scams suggests 8% cyber-involvement; dating scams involve fewer cases but suggest 88% cyber-involvement. Similarly, lender loan fraud represents nearly14% of all advance-fee payments but the data suggests only 17% cyber-involvement on first contact method.

The second issue is that it is not immediately apparent which offences are cyber-enabled and which are cyber-dependent. It also does not provide sufficient data to develop horizontal or vertical analyses of perpetrators, specialisms, networks or interactions, or information sources for exploitation (although this clearly does exist in terms of repeat victimisation).

It is possible to identify which types of fraud are most lucrative for the fraudster (i.e. where the most money is lost by the victim). From this data it is possible to calculate the median financial losses by the main categories of fraud (medians have been calculated as they generate less distortion of the data than the figures alone or mean averages, though there is still potential for inaccuracies). This data is presented in Table 4.4. It highlights that, in Q4 2014, the most money was lost to fraudsters through pension fraud, business trading fraud, financial investments, and bankruptcy and insolvency fraud.

These levels of reported losses confirm the earlier assessments that fraud continues to involve significant costs to individuals and business. However, the third issue highlighted by the data is that there is no direct correlation between the volume of

cases and the value of financial losses. Similarly, there is no correlation between either of these and the level of cyber-involvement in a fraud.

Table 4.4: Median amounts given to fraudster by victim (Q4 2014)

Fraud type	Estimated loss to fraudsters per victim[33]
Pension fraud	£38,974
Business trading fraud	£28,609
Financial investments	£21,534
Bankruptcy and insolvency	£20,000
Fraudulent applications for grants from government-funded organisations	£11,500
Fraud by abuse of position of trust	£8,100
Corporate fraud	£3,869
Department for Work and Pensions (DWP) fraud	£3,298
False accounting	£2,000
Other regulatory fraud	£2,000
Banking and credit industry fraud	£1,721
Insurance fraud	£1,084
Advance-fee payments	£784
Computer misuse crime	£536
Fraud by failing to disclose information	£440
None of the above	£420
All charity fraud	£390
HM Revenue & Customs (HMRC) fraud	£281
Non-investment fraud	£274
Telecom industry fraud (misuse of contracts)	£112

The fourth issue with the data concerns the level of impact and harm of the fraud. The data provides some useful graded indications of the impact upon the victim,[34] which provides an understanding of the victims' perspectives and thus helps to prioritise action. This analysis is presented in Table 4.5. It shows that the types of fraud with the most impact on the 'victims' are: Pyramid or Ponzi schemes, followed by dishonestly retaining a wrongful credit, fraud by abuse of position of trust and then pension frauds. By comparison, offline retail fraud has the lowest impact on victims. Again, the degree of cyber-involvement associated with each type of offence is highly variable.

[33] The table illustrates the amounts lost to fraudsters per victim. It is estimated by using the median because the averages are skewed by large standard deviations, and often estimations of loss. The advance-fee payments, for example, many of which are cyber-enabled, are numerous and yield relatively small amounts to fraudsters. The data field is skewed because of some large entries, so, to correct for these, the median has been used to demonstrate the difference.

[34] The range of data collected from reporters of crime is (i) 'Concerned about the fraud but it has not impacted on health or financial well-being'; (ii) 'Minor – only a small impact on either health or financial well-being'; (iii) 'Significant – impacting on health or financial well-being'; (iv) 'Severe – have received medical treatment as a result of this crime and/or at risk of bankruptcy'. There is an 'other' category, which is where the impact is either unknown or not deemed relevant to reporting the case.

Table 4.5: Fraud impact levels by severity, Q4 2014

Fraud type	% of severe	Harm factor	% cyber-involvement
Pyramid or Ponzi schemes	74%	2.87	24%
Dishonestly retaining a wrongful credit	73%	2.73	11%
Other financial investment	70%	2.77	17%
Fraud by abuse of position of trust	70%	2.76	6%
Rental fraud	68%	2.70	74%
Pension fraud committed on pensions	67%	2.80	8%
Lender loan fraud	66%	2.68	17%
Dating scam	64%	2.65	88%
Other regulatory fraud	62%	2.67	31%
Bankruptcy and insolvency	60%	2.80	17%

The fifth issue concerns where the emphasis of a cyber-related law enforcement response should be placed. Those categories reflecting the biggest losses – such as pension, business trading and financial investment frauds – are areas where cyber-enablement or cyber-dependency was not an obvious significant factor. Those offences with significant cyber-involvement seem to vary in both number of cases, average loss and likelihood of realistic levels of recovery (where such data is available), as shown in Table 4.6. The data also shows that much of the financial loss of frauds is unlikely to be recovered for the victims.

Table 4.6: Estimated median amounts lost to, and recovered from, fraudsters by highest levels of cyber-involvement,[35] Q4 2014

Fraud type (sub-categories)	% of cyber-involvement	Estimated median loss per victim	Estimated median recovery per victim
Dating scam	88%	£2,595 (n=528)	£1,700 (n=27)
Online shopping and auctions	86%	£210 (n=9,329)	£160 (n=483)
Counterfeiting cashiers' cheques	77%	Not known	£305 (n=36)
Rental fraud	74%	£980 (n=603)	£700 (n=28)
Ticket fraud	72%	£450 (n=897)	£528 (n=32)
Computer virus/malware/spyware	71%	£100 (n=191)	£132 (n=48)
Denial of service attack	55%	£605 (n=6)	£6 (n=1)
Mandate fraud	54%	£9,820 (n=682)	£3,845 (n=32)

[35] The number of cases may differ because: (i) the recoveries may be from a different time period to the losses; (ii) there are fewer recoveries than losses because there are simply fewer recoveries, recoveries from any given set of losses may arise in subsequent time periods, or there may be inaccuracies in the reporting process (e.g. the losses may be overestimated, or the person who lost the money may not know that it was recovered, say by someone else such as a bank).

Finally, and conversely, Table 4.7 shows that the data suggests that those areas where the greater (mean or median) amounts are likely to be recovered are in the business or public sectors (such as DWP, HMRC, business trading fraud or false accounting) where cyber-involvement is low (the highest level of cyber-involved first contact method was less than 16%).

Table 4.7: Average amounts (median and mean) recovered from fraudsters, Q4 2014

	Amount recovered		
Fraud type	**Median**	**Mean**	**N**
Financial investments	£7,107	£39,958	150
Banking and credit industry fraud	£1,621	£47,542	966
Corporate fraud	£988	£35,863	47
Pension fraud	£24,244	£30,904	10
HM Revenue & Customs (HMRC) fraud	£40,141	£40,141	2
Fraud by abuse of position of trust	£1,629	£20,882	30

Evidently, the picture is complex and the data highlights the different considerations that policing approaches need to make. However, overall, the data is useful in providing a clear indication of which crimes have the greatest levels of cyber-involvement and the relative scale of that involvement in contemporary fraud. This initial assessment of three months' reports to Action Fraud suggests that of cyber-related frauds reported, just over a third (34%) are cyber-assisted, half (50%) are cyber-enabled and just under a sixth (15%) are cyber-dependent (see Table 4.8).

Table 4.8: Cyber-involvement

	Numbers	% of all	% of cyber-involvement
Cyber-assisted	30,759	28.8%	34.2%
Cyber-enabled	45,293	42.5%	50.4%
Cyber-dependent	13,859	13.0%	15.4%
Not applicable	16,773	15.7%	
Total	**106,681**	**100.0%**	**100.0%**

4.2.2. Reported fraud by UK industry bodies

Data from industry bodies shows a considerable rise in reported fraud (though caution should be taken about earlier periods, since reporting and recording standards have changed in the interval).[36] Nevertheless, it is notable that the number of fraud offences reported by industry is greater in total than the number of recorded frauds (see Table 4.9), since they are reported direct to the NFIB rather than via Action Fraud.

[36] 'Crime in England and Wales', ONS, 2015.

Table 4.9: Fraud offences reported by UK industry bodies to NFIB, 2013/14[37]

Fraud type	Cifas	FFA UK	Total
Banking and credit industry fraud	181,737	100,462	282,199
Cheque, plastic card and online bank accounts (not PSP)[38]	121,565	100,462	222,027
Application fraud (excluding mortgages)	55,525	0	55,525
Mortgage-related fraud	4,647	0	4,647
Insurance-related fraud	9,484	0	9,484
Telecom industry fraud (misuse of contracts)	41,862	0	41,862
Business trading fraud	97	0	97
Fraudulent applications for grants from charities	30	0	30
Total	**233,210**	**100,462**	**333,672**

4.3. Key issues

4.3.1. Reviewing the data

The available data and various surveys contribute to our understanding by providing a 'snapshot' insight into economic cybercrime, rather than either a narrative or even a basic analysis. It does show that there are significant levels of non-economic cyber-attacks as well as economic, and significant but specific types of cyber-involved crimes; but that there is also a lack of information on the financial loss impacts of these attacks, as opposed to the number of incidents; and it shows differentiated patterns of cyber-involvement and the impact of targeted Prevent and Protect approaches (albeit primarily in the financial services sector) in reducing criminal attempts. There is also very limited information on perpetrator profiles and their organisation or interaction, information sources and approaches.

Nevertheless, the Action Fraud data – in relation to fraud and fraud involving cybercrime – shows that:

- Most reports (53%) were by a third party, followed by individual victims (32%) or businesses (14%).
- The largest number of reports relate to banking and credit industry frauds (33%) and non-investment frauds (29%). Technology-related offences are less prevalent. The proportion recorded as computer misuse crime was relatively small (4%), though this is partly an artefact of the data counting rules.
- Offenders mainly engaged with victims by telephone (35%), followed by websites (18%), in person (12%), letters or fax (11%) and email (8%).

[37] Source : National Fraud Intelligence Bureau. This data is not designated as National Statistics but, from 2012/13, the table presents fraud data collated by NFIB from Cifas and FFA UK only and does not include fraud offences recorded by Action Fraud, which are now represented alongside police recorded crime. The data presented here is therefore not comparable with past published NFIB figures.
[38] A PSP is a payment service provider (e.g. PayPal, World Pay) that is not a bank, dealing in electronic money transfers. Fraud offences perpetrated using PSPs fall under 'Online shopping and auctions' (not collected by industry bodies); the Cifas telecom industry fraud figure is substantially higher than that seen in the year ending September 2013 bulletin. This is due to a correction of an error that was caused by the NFIB system not accurately picking up certain Cifas fraud types.

- Cyber-enablers were identified in a fifth of cases and varied according to the modus operandi. They ranged from online sales (19%) to email (17%), hacking (11%) and social network media (9%). (We would expect some victims to have reported more than one fraud.)
- Offenders (96%) and victims (98%) were mainly located in the UK[39] with only a small percentage located outside the UK, distributed in small numbers globally (4% of offenders from 130 countries outside the UK and 2% of victims in 119 countries outside the UK).
- As the evidence highlights, broadly speaking there are two main groups affected by economic cybercrime: individuals or the 'general public', and businesses (which includes companies, banks and industries). A third relevant group is government entities, but they seldom report via Action Fraud and are not members of Cifas, so data pertaining to government entities is not explored here. Indeed, frauds against government departments are no longer collated or published centrally. In many cases, trust itself can be the 'victim' – which has broader social impacts, beyond the scope of discussion here.

4.3.2. Identifying financial losses

One of the issues in the Action Fraud data is, where does the materiality of losses occur? Cyber-enabled fraud reflects much greater financial loss than cyber-dependent crimes, whose losses are more likely to be incurred through payment for business disruption and recovery.

The definition and measurement of actual financial losses in the data require much greater refinement to provide an accurate measure, if any law enforcement response is to be predicated on cost as well as complexity. The main problem, however, is getting an accurate assessment; this is due to inconsistencies with data entry. First, it may be difficult to define and categorise the crime and to discover the actual loss. For example, there could be a reported loss which, upon examination, appears to be a crank call or a lottery scam rather than a real loss. In a few cases, victims have reported lottery scams where they have been told that they have won £10 million or more – which is recorded as the loss sum in some cases – but where the actual loss is usually a much smaller fee to release the monies, say £200. The fraud here is not the lottery winnings (which were always illusory) but the alleged fee extracted from the victim for (apparently) converting the currency and transferring the amount from the bank. The figures are not wholly representative of actual losses, but they are broadly indicative of the impacts of different forms of victimisation.

This highlights some of the complexities with accurately measuring financial losses from frauds, particularly where the data is taken from self-reporting mechanisms.

4.3.3. Identifying the cyber component

The Action Fraud reporting system, as the first centralised, national reporting structure for economic crimes, is undoubtedly pioneering and hugely important.

However, there are still a number of challenges raised by the system, not least because it is still in its early stages of implementation. The Action Fraud data is

[39] The victim location is explicable in relation to Action Fraud's role as a UK reporting body and the Home Office counting rules. The offender location may reflect (mistaken) victim perceptions of where they believe the offenders to be.

imperfect, primarily because it is intended to be used by law enforcement for tactical law enforcement purposes. Some refinement is needed so that a wider range of people (including social scientists) can use the data to explore its strategic implications for crime, intelligence and policy purposes. The data input fields appear to have evolved yet remain limited in places because of the (intentional) functional changes in Action Fraud since its inception. On the positive side, the data and its collection process do provide a good basis for refinement and improvement in quality and quantity. As it stands, the data contains some useful information that can be used for analysis. Although imperfect, the sheer volume of data (at least 300,000 reports per year) does mean that anomalies can be statistically eliminated, as long as they are not systemic.

In relation to identifying the cyber component of reported economic crime, this is largely missing from the current reporting process as a standalone data field. There could, for example, be a cyber-flag, but the problem in applying this is that the crimes/frauds that use network technologies and ICT do not always start off as such. They tend to have at least two stages: the engagement with the victim and the actual fraud, including its laundering. Hard to capture (even for the victim) are occasions when the fraud involves different types of networked technology, such as VoIP, to enable offenders to engage with victims online. So, for example, to infect a computer with a remote access Trojan (to connect it to a botnet or to steal financial and personal information); or to con the victim into thinking that they are speaking to a bank when they phone back. Later on in the process of the fraud, the fraudsters may also need to go offline in order to access the fraud money, for example through a money mule or financial transfer. There also seems to be a large difference in victim profile between businesses, single investors (SMEs through to pension plans) and everyday frauds linked to common purchasing practices. The figures here can skew findings, so arguably a filter of sorts is needed.

The volume of cyber-enabled or cyber-dependent economic crime indicated by the data is significant; when cyber-assisted crime is included, the vast majority of reports to Action Fraud show some degree of cyber-involvement. The problem is actually capturing the essence of the crime because many start online until a victim is hooked; then the fraud goes offline. Other crimes stay online all of the time, for example, many dating scams and some other advance-fee payments, and most computer misuse crimes.

4.4. The data: key questions for further consideration

Aside from the issues concerned with identifying actual losses or the location of multiple perpetrators, the data does emphasise a number of key considerations that will require greater attention as the basis for determining any law enforcement response under the Four Ps Model:

- There is a high level of cyber-involvement in reported cases of fraud but there is no established pattern of what crimes are cyber-involved or who carries them out.
- Cyber-involvement is an elastic term, given its role among a number of other media in initiating and perpetrating frauds.
- Cybercrime for gain is significant, much more significant than perceptions of non-economic cybercrimes but much less in terms of volume of attempts or reported cases.

- Financial losses are substantial by case and by crime, but there are significant variations – not all economic cybercrime results in significant losses and not all crimes involve ICT.
- Even in those industries with established Prevent and Protect approaches, such as financial services, the level of cybercrime remains high.
- The level of recovery of financial loss is relatively low.

The key point from the data is that what appears to be the main perception or fear of cybercrime relates to denial of access, disruption and loss of data and identifiers; few economic cybercrimes result in actual immediate and direct financial loss (other than time expended on putting things right). Action Fraud data by its nature addresses a very different dataset since nearly all involve financial loss. What we see is a significant level of high-volume, often low-value economic cybercrime with varying degrees of severity and harm but where the cyber component varies by crime. It is clear that the number of cases with cyber-involvement is significant but there are a number of gaps in the information; for example, we know little of who and where the perpetrators are, and the links between them and their crimes, degree of specialisation and targeting, etc. It is not always clear whether victims are businesses or individuals, and this makes it harder to plan responses on the basis of the data.

The data does address some significant policy- and police-related issues within in the volume-value-category-cyber matrix. While this does not offer a clear response focus, it does underline that volume economic cybercrime tends to target individuals, while organisations suffer the greater losses (although they are also more likely to recover some of those losses). It is clear that the current approach to non-cyber fraud would exclude investigations in a significant number of Action Fraud cases, in terms of volume and level of losses. We might hope that the data would tell us whether OCGs were involved, but unfortunately it is seldom sufficiently clear-cut to do so. Nor does it help us with the precise context of the use of cyber in the crimes. So it is not merely whether or not a differentiated response is required at national and local levels but also whether the main drivers of such a response require a technical-led investigative capability to determine the Four Ps emphasis by volume, loss, harm, perpetrator or deterrence. Certainly, the steady decline in police resources for high-volume, low-value fraud where there is no cyber component would imply that unless there is a good chance of conviction and confiscation, the effective pursuit of economic cybercrimes will not happen.

4.5. The impact of economic cybercrime on individuals/the general public

Individuals are often 'targeted' by criminals for two principal reasons. First, the level of technological sophistication required to defraud individuals is typically less than that required to attack an organisation or government. Second, the proceeds from these crimes are seldom enough on a crime-by-crime basis to merit a major investigative response, unless they are identified by the media or police as especially deserving such support (Blakeslee, 2012; Doig & Levi, 2012; Levi, 1992, 2013).

Though individual thefts often involve relatively small amounts in financial value, fraudsters who are successful 'en masse' can make significant financial gains if they are not stopped (Wall, 2007a:40). For example, in money laundering, 'smurfs' – who make several small transactions rather than one large one – are used to avoid the threshold amounts set up to identify suspicious transactions (Florêncio & Herley, 2010). Targeting several individuals is fairly low-risk in terms of the likelihood of action

being taken, especially if no systematic intelligence is gathered that links individual events and the highest common factors.

There are several techniques used to target individuals. Fake websites which mimic legitimate ones and malware, such as key trackers and Trojans, are used to covertly gather personal data, which can be sold on the underground market and exploited for further financial gain (Ablon et al., 2014; Asgher et al., 2014; Cross, Smith & Richards, 2014). Individuals may become targets of fraudsters through self-selection by responding to a phishing scam, a mule scam or a dating scam (McGuire & Dowling, 2013; Whitty & Buchanan, 2012). Personal attacks may make use of social engineering techniques, whereby the attackers manipulate targets psychologically, encouraging atypical behaviour such as sending increasing amounts of money to the attacker, providing the attacker with personal information, or with unauthorised access to accounts or computer systems (Ghosh & Turrini, 2010; Hutchings, 2013; Kshetri, 2010; Ståhlberg, 2008).

Finally, there is a need to consider the individuals who are vulnerable as a result of engaging in deviant behaviour online, and are thus selected as targets by others (Lauritsen, Sampson & Laub, 1991; Singer, 1986; Wolfgang, Ferracuti & Mannheim, 1967). This could include those who download pirated materials which are infected by malware; complacent actors, such as money mules, who are duped into facilitating a scam; and more malevolent actors, such as the botmasters who operate botnets, thus making themselves the targets of their competitors (Bossler & Holt, 2009; Dittrich, 2012; Gragido et al., 2012; Kikuchi, Matsuo & Terada, 2011).

4.5.1. How could policing help individuals?

Reports from software suppliers and computer security organisations highlight the issues arising from using no or little antivirus protection. Despite the simplicity of use, up to a quarter of UK computer owners do not have current antivirus installed. This should become a smaller problem over time as software packages integrate security systems, such as Windows 8/10 which come with Windows Defender. A number of antivirus packages are free, so cost alone should not be a factor. There have also been other initiatives, such as Blackfin's pop-up workshops with industry and law enforcement, and the local 'web constables' in Estonia and Finland.

However, the increasing use of internet-connected devices in addition to computers (tablets, e-book readers etc.), which seldom have countermeasures pre-installed, means that malware has become increasingly problematic. There is some recognition of these issues, for example Cifas[40] and FFA UK[41] offer useful advice to help individuals avoid becoming a victim of identity fraud and other scams.

While efforts to educate the general public about internet dangers have improved, individuals who fail to adhere to best security practices can become profitable targets for motivated and skilled offenders (Pratt, Holtfreter & Reisig, 2010). This is particularly true of relatively new internet users (Gragido et al., 2012), but it also applies to more experienced users, and to users who make their own assessment of what information is at risk or what type of security is suitable. Consequently, more effort needs to be made to create uniform, centralised or market solutions to encourage and support individuals, particularly novice users, into engaging in good

[40] See: www.cifas.org.uk/avoid_being_a_victim.
[41] See: www.financialfraudaction.org.uk/%5Cconsumer-landing.asp.

security practices, as well as providing them with guardianship against grooming and offering support if that guardianship fails.

A starting point is to educate individual internet users about the dangers they face, particularly with regard to scams that use social engineering techniques to hook victims, for example via offers made by email or on internet dating sites, as well as by telephone using VoIP (Hutchings, 2013). This might include the following areas of activity:

- A Cyber Security Protect Police Officer could identify and assess individuals who might be vulnerable, delivering appropriate awareness events to various communities and identifying partners. They could also act collectively as 'public interest' lobbyists, persuading banks and other financial services that provide online facilities to mandate the use of service provider software for all financial transactions; and they could offer to undertake impact assessments of new products or services from an individual user's perspective.
- While useful, having a single point of responsibility in itself is unlikely to make much impact on the public in general. Therefore, attention must be given to developing coherent strategies to warn individuals, drawing on issues relevant to them.
- When addressing the deeper challenge of individuals' susceptibility to social engineering, reducing levels of malware invasion is only the first stage of protection. Investment in crime prevention education does not have a good history in terms of serious evaluation, but the sheer variety of potential victims and enablers make it hard to target prevention efforts. Tailoring and targeting messaging to particular groups, picking up on their specific vulnerabilities, is key.
- There is a need to understand how and why different groups use the internet and for what purpose; targeted marketing and communication; persuading partners such as banks to require appropriate levels of installed controls; partnership working with associations already engaged with groups (from schools to Citizens Advice, to signal events such as university and college enrolment weeks etc.). Monitoring such delivery is vital and will require appropriate funding.
- At the same time, for those who fall victim to online scams or attacks, there needs to be a better system in place to provide them with support when they report the crimes. This should include those who have been reimbursed for their direct financial losses and are reported in bulk by FFA UK, and efforts (at a local or regional level) to go after those who engage in low-value but high-frequency crimes (Cross & Bradshaw, 2014; Jeffray, 2014).

4.6. The impact of economic cybercrime on organisations

Any business or organisation can become a target for cybercrime, though ICT security companies, financial institutions and online gambling outfits are particularly common targets due to the nature of their commercial and business activities (Botezatu, 2011, 2012; McMullan & Rege, 2010; Mickelberg, Schive & Pollard, 2014). The types of crimes which affect businesses vary considerably – often reflecting their business activities as well as their size – but include extortion (for example via ransomware); misrepresentation (such as bank mandate fraud); theft (of both data and money); illegal access; and system interference (Calderoni, 2010; Mickelberg, Schive & Pollard, 2014).

In 2012, 8% of business premises (covering the accommodation and food services, wholesale and retail, manufacturing, and transportation and storage sectors) had experienced at least one type of online crime during the past 12 months (McGuire &

Dowling, 2013). However, there are substantial variations in the nature of the cyber-attack for each sector and the reasons why, as well as whether financial gain is the sole or primary intention of the perpetrator. Some cyber-dependent crime against big business is to facilitate other economic cyber-enabled crime; data security in particular is a mainstream concern for large businesses and organisations (Jeffray, 2014).

Government entities often fall victim to the same crimes that businesses face. However, there is greater potential for economic disruption, and greater costs in responding to and/or repairing damage from attacks. Compromising or controlling the government infrastructure – particularly those services that make up the UK's 'critical national infrastructure'[42] – can result in large economic losses for the state and potential gains for the perpetrators, not only from monetisation of stolen data but also from the unauthorised use of government infrastructure (Brenner, 2010). There are also likely to be indirect, knock-on impacts such as hindrances to economic growth, and a reluctance to move operations online, thus reducing overall efficiency and opportunities for innovation (Detica & The Office of Cyber Security and Information Assurance, 2011).

It is difficult to estimate from data the prevalence and damage of economic cybercrimes to organisations, due to systemic under-reporting by victims who are reluctant to disclose breaches in their cyber security.[43] Organisations fear that disclosing security breaches will result in a drop in consumer trust (Brenner, 2010; Heinonen, Holt & Wilson, 2012; Wall, 2007b). Nevertheless, what data there is underpins the need for breaches to business to be taken seriously, given the value of financial loss, which is greater than for crimes against individuals. Businesses often lose the most in economic terms from cybercrime, particularly through high levels of intellectual property theft and espionage. Also of note is that the impact of economic cybercrime does not fall equally across industry sectors. Although government understandably continues to prioritise protecting the critical national infrastructure, providers of software and computer services, financial services, pharmaceutical and biotech, and electronic and electrical equipment are at particular risk from cybercrime, including corruption by and social engineering of insiders as well as hacking of sensitive commercial data. Detica &The Office of Cyber Security and Information Assurance (2011) argue that, without urgent measures to prevent the haemorrhaging of valuable intellectual property, the cost of cybercrime is likely to rise even further in the future as UK businesses increase their reliance on ICT. Since then, the hacking of IP in various forms has markedly ascended the political agenda.

We also acknowledge that, in addition to private actors, the cyber threat to governments may come from other states. While outside the scope of this research, the point highlights that the internet is a globally shared commodity yet there is no

[42] The Centre for the Protection of National Infrastructure (CPNI) comprises nine sectors: communications, emergency services, energy, financial services, food, government, health, transport and water. Criticality is determined by whether the loss or compromise of the sector would have a major detrimental impact on the availability or integrity of essential services, leading to severe economic or social consequences or to loss of life. For more information, see: www.cpni.gov.uk/.

[43] Although, in the US, but not yet in the UK, organisations whose security breaches result in personal data loss are legally mandated to inform individuals and offer them free protection via credit reference agencies.

clear-cut governance model for cyberspace, nor is there a dispute resolution mechanism.

4.7. How could policing help organisations?

4.7.1. Large organisations and businesses

Government and public sector organisations have recognised the importance of safeguarding against cybercrime in terms of protecting the integrity and confidentiality of both data and ICT portals. The government has allocated £860 million until 2016 to establish a National Cyber Security Programme following the 2011 UK Cyber Security Strategy. That funding has gone to government departments, agencies and some other non-governmental organisations. These include the intelligence agencies, the Ministry of Defence, the Foreign and Commonwealth Office, the Department for Business, Innovation and Skills and the Centre for the Protection of National Infrastructure (CPNI) which supports the organisations that provide essential infrastructure services. Modest sums have gone to the police and into protecting consumers, beyond substantial funding for Cyber Streetwise[44] (a government-funded campaign aimed at changing the way people protect themselves from falling victim to cybercriminals) whose impact remains to be evaluated.

Many of the frauds which affect businesses are fairly well understood as a result of analyses by the major financial consulting firms and membership organisations such as the Association of Certified Fraud Examiners. The difficulty for businesses is recognising the signs or risk areas, investing the resources and communicating them effectively to time-pressed staff. Although the consequences may fall in the first instance upon individual account holders, businesses (and sometimes governments) are generally liable for security breaches which lead to mass leaks of personal financial data.

Encouraged by the CPNI and the Computer Emergency Response Team (CERT) programme, but acting independently, some of the worst-affected sectors have already learned the advantages of pooling data and actions in response to the collective threat of economic cybercrime.[45] For example, this happened in the payment card sector in the 1990s following a large rise in offline and online fraud (Levi, Bissell & Richardson, 1991), though mobile payments remains an area of significant risk. The British Bankers' Association and groups within it have increasingly experimented (and continue to do so) with data integration and data sharing to

[44] See: www.cyberstreetwise.com/.

[45] In addition to informal, organic arrangements, the first formal information exchanges were established in 2003. As the CPNI notes, trust is built up slowly. Representatives at information exchanges are expected to attend all meetings, and generally only two named members from the same organisation are allowed. Substitutes cannot attend. Current (2015) information exchanges include: ADMIE – Aerospace and Defence Manufacturers Information Exchange; CIPSIE – Communications Industry Personnel Security Information Exchange; CNSSIE – Civil Nuclear Sector SCADA Information Exchange; FSIE – Financial Services Information Exchange; MSPIE – Managed Service Providers Information Exchange; NIXIE – Northern Ireland Cross-Sector Information Exchange; NSIE – Network Security Information Exchange; PIIE – Pharmaceutical Industries Information Exchange; SCSIE – SCADA and Control Systems Information Exchange; SPIIE – Space Industries Information Exchange; SRIE – Security Researchers Information Exchange; TSIE – Transport Sector Information Exchange; VSIE – Vendor Security Information Exchange; WSIE – Water Security Information Exchange (see more at: www.cpni.gov.uk/about/Who-we-work-with/Information-exchanges/#sthash.31lUdVan.dpuf).

enhance their speed of response to attacks in the form of DDoS, hacking and insider corruption/IP data theft. Similarly, major successes against volume fraud have been achieved following voluntary or organised data sharing and integration within the credit sector (particularly by Cifas), the insurance sector (via the Insurance Fraud Bureau) and local government (through the Audit Commission's National Fraud Initiative, before its disbandment). There are many other fraud reduction initiatives, omitted here as they are not cyber-related.

The growth of DDoS and malware attacks on relatively well defended banks has given impetus to cross-industry sharing, especially where there are genuine fears that the attacks might bring down the institution or have wider sector ramifications. There has been significant investment in analysis and protection services offered by financial consulting firms, and by a plethora of technology and consulting firms, pre- and post-cybercrime events.

Overall, the needs of large organisations are predicated on information sharing and police guidance – including the development and use of technical standards and common taxonomies to make information sharing easier and more efficient – on emerging threats and trends, around which they can develop their responses. We would expect major incidents to prompt a police response which should have an appropriate level of resource and expertise to provide assurance, in order to increase business confidence in the security of the internet and offer a credible deterrent to criminals.

4.7.2. Small to medium-sized enterprises (SMEs)

There has been less governmental and cross-sector investment in SME security as firms focus on those who are willing and able to pay for cyber security. This 'willingness to pay' model does not correspond to the impact of cybercrime as a ratio of profits, turnover or assets, which is likely to be more significant for smaller than larger businesses. A 2015 report by the London Assembly's Police and Crime Committee notes that banks are reluctant to refund SMEs money lost through online fraud, especially if linked to 'customer error'; though, of course, the estimated likelihood of crime against large versus small businesses is also relevant.

One of the significant challenges for SMEs is a lack of awareness, knowledge or understanding of the issue – unpublished survey research by Cyber Streetwise on 1,000 SMEs states that two-thirds do not consider their business to be vulnerable to cyber-attack, and just 16% say that improving their cyber security is a top priority for 2015. A quarter (26%) of respondents believe that only firms that accept online payments can be hacked; another 22% said they did not think that small companies were targets for hackers. A key problem for business in general, large and small, is staff not knowing how to identify easily when they ought to be suspicious of an email.[46] Research into good practice suggests that: (i) warning text should include a clear and non-technical description of potential negative outcome(s); or (ii) an informed direct warning should come from a credible position of authority. Concrete warnings are much more effective than vague ones; soft powers of persuasion work much better than harsh ones (Modic & Anderson, 2014).

[46] See, for example: www.cpni.gov.uk/advice/Personnel-security1/Social-engineering-Understanding-the-threat/; and: www.getsafeonline.org/information-security/social-engineering/.

The government has sought to counter this risk-taking through greater information provision, for example highlighting that the average cost of major breaches outweigh the costs of security.[47] There are an increasing number of short guides[48] and free training available for SMEs, though the impact of these is difficult to evaluate due to a lack of data. Though useful, this approach of information sharing is persuasive only if the organisation understands that it is likely to become a victim of such attacks. Of course, risk assessments of the likelihood and impacts of potential cyber-attack versus the costs of security will vary widely for each organisation. It may be hard to shift this subjectively estimated risk. However, irrespective of this, relatively cheap security measures are available and should be taken.

In addition to raising awareness and educating staff, a key step to helping SMEs address economic cybercrime threats is to make sure messaging is presented in an accessible way for employees. Those we interviewed agreed that SMEs were the most time-pushed to provide cybercrime advice to employees, especially for those without a dedicated ICT department, and it is therefore vital to frame such advice correctly for easy comprehension. Much of the effort made by Get Safe Online and Cyber Streetwise (both free government-funded online security advice services) has gone into creating relatively clear graphic communications, both for individuals and for SMEs, to drive home key messages more effectively.[49] One promising initiative was undertaken in connection with Research Council UK's Partnership for Conflict, Crime and Security Research. Young entrepreneurs were given some IP and other cyber-protection awareness training during a workshop, in addition to their regular management skills, and although the longer-term effects are unknown, building in this sort of practical cyber risk management at an early but salient stage appears to be the sort of initiative that is needed.

Providing effective solutions for SMEs is also essential. PROOF is a free online filing service via Companies House, which seeks to protect firms from the risk of identity theft. Once signed up, anyone not possessing authentication codes issued by Companies House will be unable to file documents for the company, for example changing addresses or bank accounts. Such websites can offer some cyber security assurance in terms of their own initiatives.

As well as these approaches, there is a trend for mandating cyber security measures as a private sector contract issue. For example, current procurement rules require those tendering for central government contracts to pass the CyberEssentials or CyberEssentials Plus certification, though this rule applies to only a modest proportion of SMEs.[50] Also salient is the growing awareness among larger companies of the need to secure their supply chain, as ICT vulnerabilities in the chain can compromise their own security. Nevertheless, Cyber Streetwise's study found that 22% of SMEs "don't know where to start". Rather than a shortage of information or advice sources, it is perhaps the wide range of advice sources, including overlapping official websites that poses challenges. Efforts to streamline sources and make advice consistent, to maximise effectiveness, may therefore be of value.

---

[47] See: www.gov.uk/government/news/cyber-security-myths-putting-a-third-of-sme-revenue-at-risk.
[48] One example is available here: www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know.
[49] For example, 'The Rough Guide to Online Safety'. See: www.getsafeonline.org/businesses/. There is no consensus among experts about which messages are accurate.
[50] Also see LCCI (2014) for some trenchant criticisms of how the scheme operated.

In terms of identifying gaps for law enforcement, a starting point for SMEs will be to replicate the information offered to individual internet users about the threats and risks they face, and the options available to them, including delivering appropriate awareness events to the various communities and to identify partners.

The police will also have a formal role in terms of coordinating the provision of protective security and preparedness advice as well as receipt of allegations of criminal activity. The key question, however, across all three 'victim' groups – individuals, large organisations and SMEs – is, where would targeted interventions have, in policing terms, the biggest impact? As we will explore later, there may also be issues of desert and need: some we interviewed suggested that those who cannot afford to adopt security measures should be prioritised for police help. However, where victims can cause social harm to others in the supply chain or to the nation's economic interests, they cannot be ignored for prevention, even if they are denied criminal investigation.

4.8. Summary

This chapter has drawn on an extensive literature review on economic cybercrime as well as Action Fraud data. It notes that the evidence base is not as robust as it should or could be in order to distinguish variations in the economic dimensions of cyber-dependent and cyber-enabled crime or to identify the frequency and the nature of their impacts on businesses, government and the public. Nevertheless, and despite these issues, the available research and data, if treated with due care, could play an important role in understanding economic cybercrime. The Action Fraud data has the potential to provide for an evidence-based law enforcement response. More work, however, is required to make this a reality.

This chapter has also highlighted that a very varied response to the threat of economic cybercrime is required of businesses, government and individuals, and thus to their engagement with law enforcement if they wish to respond to specific categories of victims and potential victims. While there are some similarities in terms of the challenges faced, there are differences in the ability of each of these three groups to address the challenges.

Larger organisations often have dedicated ICT departments and are better informed of the risks and threats. They are also likely to be able to afford the appropriate resourcing responses. For them, the issue is less of awareness and education, or even of having access to law enforcement resources to investigate and prosecute fraud, than it is an issue of access to guidance on threat and risk profiles and types so that they can design and deploy their own responses. Larger organisations can leave law enforcement agencies to take action against identifiable groups who initiate the more significant or recurring cyber-attacks against them (although whether this responsibility lies with technologically-savvy economic crime departments or dedicated cybercrime units requires further consideration). The insurance industry's Insurance Fraud Bureau, the City of London Police's Insurance Fraud Enforcement Department (IFED), and the Dedicated Card and Payment Crime Unit, in sharing information, joint working and targeted operations, are examples of added-value to a relatively well organised sector. However, they would be of much less use as a response for smaller organisations.

For SMEs, dedicated awareness and education are required. However, in an atmosphere in which many smaller businesses are suspicious of government (and to some extent of larger businesses, too), it may not be easy to find someone who is seen as having across-the-board credibility to issue such warnings.[51] A combination of experience to increase perceptions of risks and having mitigations/solutions in place is likely to help overcome the scepticism barrier for the majority (and would have equal relevance for individuals). It is important here to consider the need for 'knock-on' effects, such as through the supply chain, which can generate systemic weaknesses if not addressed. It may also be important to supplement such responses with specialist guidance and advice on a planned basis – but that raises questions about who else should be involved and what law enforcement's role should be. We turn to this issue in the next chapter.

[51] An issue in counter-terrorism and counter-drugs efforts also.

5. The implications of economic cybercrime for policing

This report has explored the nature of economic cybercrime and the impact it has had on two key groups, namely individuals and businesses (of all sizes). This chapter seeks to draw this analysis together and to explore how the various issues highlighted have implications for policing approaches to economic cybercrime, and what these might be. It goes on to review current policing approaches to consider how they can be developed to effectively reduce the risks of economic cyber-attack for individuals and businesses. This is done in the context of existing government strategy and, particularly, its CONTEST counter-terrorism strategy, which has four components (the Four Ps Model):

- **Pursue** organised criminals by prosecution and disruption;
- **Prevent** people from becoming criminals;
- **Protect** business and the public against serious and organised crime; and
- **Prepare** for attacks by building post-event resilience to reduce the impact of crime as well as improve resilience for future prevention.

5.1. Introduction

Policing economic cybercrime involves a multiplicity of national and transnational actors intervening both before (Protect and Prevent) and after (Pursue and Prepare) criminal activity. As highlighted in chapter 4, economic cybercrime affects a range of actors, principally individuals or the 'general public', businesses and government; it also often affects different groups in different ways. Although historically economic crime and its impacts have not always been recognised by these groups – particularly among corporate boards (Levi, Morgan & Burrows, 2003) – this has begun to change.

Following a spate of major cyber-attacks,[52] an increasing number of businesses, especially but not exclusively in financial services, have begun to take information security very seriously. This is reflected in the rise in the number of jobs in cyber security[53] and is evident from a study of CEO priorities,[54] as well as in the general

[52] For financial services, a key 'wake-up call' was the attack on JP Morgan in 2014; if a relatively well defended bank could be attacked, it was time to take cyber security more seriously. But the regularity of attacks on all financial institutions has played an important part, showing that it is both potentially serious and regular. Globally, since 2005, more than 75 data breaches in which one million or more records were compromised have been publicly disclosed. The attacks on Home Depot and eBay in 2014, and on Target at the end of 2013, illustrate an increase in attacks on retail and merchant data. The largest attacks have been on US retailers. In the US alone, over the period July 2005 to July 2015, over 853 million records (not individuals) were compromised from 4,569 data breaches made public (see: www.privacyrights.org/data-breach). The UK Information Commissioner's Office does not supply data in the same way, but 1,414 data breaches were notified to it in 2014. In the year to April 2015, British financial institutions were investigated 585 times for data privacy breaches (see: Financial Times, 2 June 2015), though it is not clear what such 'investigations' comprise. We are not suggesting that prosecutions are an appropriate measure of its performance, but the Information Commissioner's Office has prosecuted 21 persons and companies over its entire history.

[53] No reliable aggregate data on cyber security jobs is available for the UK (and media reports often cite US data without noting that it is not UK data), but the banks and major financial advisory firms interviewed for this project had all conducted a major recruitment expansion. See: www.scmagazineuk.com/more-jobs-but-cyber-security-skills-gap-widens/article/340103/; for US data to end 2013, see: Burning Glass (2014).

[54] For rising CEO concern, especially in North America, see: www.pwc.com/us/en/ceo-survey/secure-assets.jhtml.

attention being paid to cybercrime by academia and the media. Individuals in all social strata are fearful of direct scams such as identity crimes, and many are willing to pay for tools such as antivirus software and (to a lesser extent) identity theft monitoring to provide protection.[55] However, even simple messages about security are harder to apply in an online environment than offline (raising the question as to whether it is the message or the medium that is the issue),[56] and action often follows a negative experience rather than being taken proactively.

Cyber-enabled and cyber-dependent economic crimes harm the interests of all businesses, UK/regional government and individual consumers. The need for policing is unquestionable. In this context, the core issues now involve four questions:

- Who within and outside policing should be involved and in what capacity?
- What are the specific roles and responsibilities of the police and where should ownership lie in terms of tackling economic cybercrime?
- What resources (in money and effort) will be considered worthwhile for greater cyber security?
- How will that security be organised for and/or by the huge numbers of businesses and people that are (potentially) affected?

Both in principle and in practice, there is uncertainty about what is expected from the police – and what it is reasonable to expect from them – in tackling economic cybercrime. The response to this conceptual problem may determine the extent to which there is a gap between the emerging fraud strategy and its delivery.

Evidently, one strand of the effective policing of economic cybercrime involves Protect and Prepare measures, though the police are constrained from recommending particular products, and their specific skills as cybersecurity advisers are open to question. Another issue is whether the police should take on cybercrime roles where the objectives are less about preventing and investigating financial loss than they are about deterring those primarily involved in disruption, and so on, thus securing business continuity and delivery and supplementing in-house security arrangements.

Moreover, such measures may not solve or even mitigate the problems they are designed to address. A further strand for consideration is how far the police can investigate economic cybercrimes that have international dimensions and where offenders are beyond practical reach. Even where the police can arrest offenders and disrupt cybercrime markets – often via the FBI and/or Europol EC3 – the effects may be short term. Perhaps this is too severe a test of effectiveness for many, since many police interventions may be largely symbolic, but it is reasonable to ask what economic cybercrime control functions, on the basis of the available evidence, are necessarily performed by sworn officers (rather than by PCSOs, volunteers or by the private sector), and what the impact of such operations is on the levels, types and organisational forms of criminality. These issues are themselves linked to data collection, recording and measurement to inform practice; an area that, as

[55] For a sceptical view on US identity theft protection, see: http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/.

[56] It is instructive to note that the various websites giving guidance on identity theft/fraud – Cifas, Action Fraud, the Information Commissioner's Office, the Metropolitan Police, the BBC, Get Safe Online and commercial companies such as Equifax and Experian – appear to confirm that cyber-related fraud is a crime that continues to rise (see: www.cifas.org.uk).

discussed earlier in the report, faces a number of challenges and requires further consideration.

The emerging 2015 strategy is very much focused on centralised organisation, given that the City of London Police can allocate its resources in collaboration with a national economic crime prevention centre, a national fraud prevention network and the National Police Coordinator for Economic Crime. It has also, in terms of the two identified strands of volume and of serious, organised fraud, a much clearer direction through the Economic Crime Command of the NCA, the regional Special Operations Units and Economic Crime Units. Centralisation is also evident in the forthcoming national prevention and awareness campaigns, although they should be tailored to local circumstances in ways that need to be developed. Much less clear is the intersection of locale and volume. Here the strategy suggests, under the Four Ps Model, that, in relation to Pursue:

> "the nature of volume fraud, particularly when cyber-enabled, often from overseas, means that it will not always be feasible for the police to investigate and pursue an offender with the core aim of securing conviction and a custodial sentence... public expectations and the ambitions of investigators should therefore be managed accordingly."

In other components the strategy envisions roles for local forces that include victim support, local initiatives driven by local priorities and NFIB risk profiles, as well as delivery of locally tailored prevention campaigns, community engagement, championing prevention in force (e.g. all officers and staff with victim contact) and collaboration with local victim support services.

As with many public policy issues, there is a tension between coherence and localism, but the approach is predominantly a top-down one. This has yet to recognise the very complex picture of crime patterns and the level of cyber-involvement, the different ways in which individuals and businesses are affected by different types of economic cybercrime and under what circumstances. Understandably, there is a lack of clarity over offender types and interaction.

Building on the issues presented here, there also needs to be a much more comprehensive assessment of what is currently being done to address and tackle economic cybercrime, the range of efforts and organisations required, the level and ownership of the resources required, and the context in which the responses are presented. The language of the Four Ps Model, for example, was met with confusion by most business people we interviewed who were not security professionals (and by some police officers, especially overseas). In part, we feel, this is because the model is designed with counter-terrorism in mind as opposed to helping potential victims to avoid the consequences of criminal activity. This chapter thus looks at the Four Ps Model in some detail and considers how the strategy may be refined and realigned to respond more effectively to the issues – and the four questions – it has identified. Given the strategy's comments about the role of organised crime in cyber fraud, we also focus on volume cyber fraud.

5.2. The police role in Protect

The police currently play a fairly minor role in the Protect function against economic cybercrime. Given the range of potential victims in the general population and in business, they have no way of reaching this almost universal population of potential victims before they become actual victims. Government in general does play a role,

and the private sector seeks to make profits from advertising better cyber security, as it does in other spheres of offline crime prevention.

Clearly, this is both a marketing and service delivery issue. Governments have previously run campaigns in favour of specific safety requirements (whether the use of seat belts or the dangers of smoking) to ensure a general basic level of awareness. Such an approach may be essential to allow the police, as trusted guardians, to offer additional guidance on protective measures against economic cybercrime for business and individuals. Compulsory built-in antivirus with automatic updates on all ICT devices might be one way forward – but this would raise issues of whose security offerings are to be taken up, and by what criteria, as well as the fact that there are sometimes technical limitations to having built-in security. Understandably, banks have avoided engaging with this issue beyond providing free antivirus protection, due to the complexities. Despite such free offerings to their customers, a notable (though unpublished) proportion of individuals and businesses do not take it up (some, but presumably not all, because they already have other antivirus software installed). It could be argued that encrypted online banking and communications should be a compulsory precondition of internet banking as part of the reciprocity of the commercial arrangements.

In addition to the general sources of information and guidance on what to do about cyber security, Coventry et al. (2014) and Ashenden & Sasse (2013) offer some useful advice on how to embed better security practices in the general population and business respectively. Using behavioural insights, Coventry et al. (2014) present a target-hardening and educative framework (see Table 5.1).

Table 5.1: Setting up a preventative approach to economic cybercrimes 1

Approach	Actions
Defaults – is it possible to make the secure option the default option and design in security from the start?	• The UK cookie policy; the default should be opt-out • Security software should be installed and part of the initial set up not an optional extra • All programs with privacy and security access should be defaulted to secure • Websites should log out the user when they leave, not leave them open – or at least prompt the user to log out • Users should not go online with administration rights to prevent hidden programs executing without asking permission
Salience – how can the information be made noticeable and relevant to the target audience?	• Make security assessments easily visible and preferably at the point-of-vulnerability – a security monitor app • Personalise security messages – how has the individual improved, what risks are they open to (based on sites they visit)? • Give software ratings based on their security provisions – the UK has mandatory Security Performance Certificates for all websites operating within the UK
Priming – how can we subconsciously influence users?	• Build on the Internet Explorer anti-phishing green URL indicator and ensure that any insecure sites are more noticeable – actively interrupt the user • An active visual indicator of the current security level of the PC and the user – what is being downloaded on to their system etc.

Further, a gap analysis may be necessary to understand what some sectors do or do not do and how far that is a consequence of past experience, size and sensitivity of the product or activity. For example, for (usually large) businesses, there are growing numbers of full service security firms that take care of cyber-risks on all platforms. Official neutrality to avoid recommending particular firms or products makes consumer choice harder to undertake – on what basis do non-experts choose between technically complex options? – but there is some kite-marking process supported by government (for example, the two levels of the Cyber Essentials badge). More importantly, and a lesson that the Cyber-security Information Sharing Partnership (CiSP) has understood, is that voluntary arrangements, conversation sharing, speed of exchange, demonstration of added-value, hard data sharing in real time and, especially, trust in the arrangements are important as the basis for partnership and engagement. CiSP has over 1,000 members and 3,000 people involved.

5.3. The police role in Prevent

Prevent is the mechanism used to attempt to 'divert' potential criminals from committing crimes. Some potential offenders can be identified from their role in chat rooms, social media and other forms of internet presence, but the level of threat they pose may vary considerably.[57] If the evidence suggests that they may be reaching a serious threshold, then some disruption may be attempted. Some police officers interviewed for this project were sensitive to the risk of longer-term isolation from the labour market that might result from bringing minor offenders into the criminal justice system. Though HR and employee vetting functions may benefit from recent developments such as the Cifas Staff Fraud Database, the prediction of future harm from past conduct remains in an early stage of science at present. Though there is some security information in schools, colleges and universities, this is patchy, and issues around the morality of cyber-conduct or fraud, as well as the legal requirements for data protection under the Computer Misuse Act 1990 and the Data Protection Act 1998 receive little or no attention, either in general or in relation to ICT and other courses. However, resources available for a significant police or non-police role in reducing the risk of future cyber criminality are very modest, and since many of the threats come from regions overseas, those potential criminals or victims are not readily influenced by UK interests or by education here. This is an area of preventative intervention that needs to be worked on internationally if progress is to be made.

5.4. The police role in Protect and Prepare: information and awareness

The police are and need to remain partners with other organisations involved in both the Protect and Prepare roles. As with Police and Community Together (PACT), travel safety and other school- or community-based initiatives, the broader family of policing can both inform the agenda about threats and risks and also provide figures of authority to deliver the message to individuals and SMEs (larger organisations are already networked or have in-house expertise in this area). Proposed 'Cyber Security Protect Officers' will have specific roles in interventions, primarily in schools and colleges, to dissuade or divert individuals at risk of engaging

[57] As highlighted by preliminary research into the association between autism and cybercrime, and international law enforcement, following a rise in cybercrimes involving individuals with autism. See: www.emeraldinsight.com/doi/10.1108/AIA-05-2015-0003.

in cyber-related criminal conduct, but this should include economic cybercrime as well as anti-bullying, grooming and terrorism.

The key relationship will be their own networks with those agencies which are already engaged with specific sections of the community – whether Age UK, Citizens Advice or the Confederation of Small Businesses – or organisations such as the Fraud Advisory Panel or the North East Fraud Forum (NEFF). Such public/private partnerships are crucial as an approach; a point noted as far back as the 2006 Fraud Review. In 2015, the NEFF co-sponsored the North East Regional Cyber Crime Conference as a platform to bring businesses together to raise awareness of the current cyber threats and to explore means of preventing a cyber-attack within their organisations. The conference also promoted the North East Regional CiSP.

While this does not require significant staff input, it will require limited amounts of funding and a clear central source of information, material and, crucially, accessible sources of both online and offline support and guidance to address specific issues.

5.5. The police role in Protect and Prepare: increasing resilience and reducing repeat victimisation

5.5.1. Increasing resilience

Building cyber resilience involves a number of aspects. It is about being an 'intelligent' user of information on threats and responses; taking those actions or steps to mitigate and respond to cyber threats; and being able to prepare for, adapt to, withstand and rapidly recover and learn from, disruptions caused by cybercrime (see Scottish Government, 2015). Given that every individual and every organisation (whether a business or government entity) is a potential victim and that all have assets of some sort of worth, it is essential to have in place a risk management approach that involves thinking strategically and pre-emptively. Assessing the probability that an individual or organisation is likely to be the victim of a targeted or untargeted attack of a particular harm level, and thus needs basic or more sophisticated (and expensive/burdensome) security controls, is a key component of an holistic understanding of the role and importance of cyber security (GCHQ and CERT-UK, 2015).

The key issue is breaking down the nature of the threats and concerns at a macro-level to what it means in practice to develop and implement controls to protect and prepare for economic cybercrimes. While there is a range of initiatives – from standards such as ISO 27001, to the Cyber Essentials certifications, to government funding for SMEs (in the form of the 2015 £5,000 voucher scheme to obtain specialist advice) – there need to be more tailored and accessible sources of guidance and support that address the totality of the risk environment and effective responses (see Table 5.2).

Table 5.2: Setting up a preventative approach to economic cybercrimes 2[58]

Organisational information risk management regime	
Policy	**Components**
• Establish an effective governance structure and determine your risk appetite	• User education and awareness • Home and mobile working • Secure configuration
• Produce supporting information risk management policies	• Removable media controls • Managing user privileges
• Maintain the senior management's engagement with the cyber risk	• Incident management • Monitoring • Malware protection • Network security

5.5.2. Victimisation

Repeat victimisation has become very important as a focus of police and Prepare/Protect interventions. If those individuals and businesses who are most likely to become repeat victims can be identified and encouraged to improve their security and resilience, with support as required, they can be saved from harm and Pursue costs reduced (including policing and, if it gets that far, criminal justice and penal costs). Whitty (2013), for example, notes that a quarter of dating scam victims had been previous victims of fraud. Although this may not be generalisable to other forms of cyber-enabled fraud, it seems likely that there will be a concentration of victims in some demographic and business sectors, which the police may be well placed to identify via the Action Fraud database and thus use as the basis for part of the emerging strategy. It should also be noted that repeat victimisation help is not restricted to economic cybercrime: the telephone is a common method of communication for mass marketing and investment frauds.

Some progress has been made at a general level in some categories of fraud, such as mass marketing frauds, but more effort needs to be made across the range. While segmentation work has been undertaken for organised crime (including fraud) victimisation and enablers, there needs to be a concerted push to identify individuals and businesses particularly 'at risk' and to help them. This can be done for groups in advance of their becoming victims (or not) – as has recently been done to discourage frauds against those liberating occupational pensions – and/or after they first report a fraud, when people are more likely to be receptive to advice.

Primarily, the mechanisms for doing this to date have been websites and formal organisations. However, awareness measures may need to be supplemented by outreach by trusted (and trustworthy) persons. Peer influence and community-level bodies seem particularly well placed to perform this function and it is better that such bodies proactively seek out or arrange face-to-face sessions with representative organisations – Women's Institutes, senior citizen groups, etc. – rather than rely on vulnerable or poorly-informed individuals to use the internet for information. Age UK, Citizens Advice or even a vetted group of 'cyber-savvy' volunteers would be appropriate service deliverers, depending on the demographic. Victim Support has also expressed a willingness to become more

[58] Source: www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary.

involved than in the past (Button, Lewis & Tapley, 2009; Levi & Pithouse, 1992). This, however, would require a shift in skills from those used when dealing with victims of theft, burglary and violence, since the demographic of volunteers may itself need training in fraud victimisation and cyber-skills.

In short, people find advice more credible when it comes from their peers and people they can relate to, and they are more likely to follow security advice when it is very simple and requires little effort to implement; better still, when it is conducted on their behalf by third parties such as their internet service providers and social media service providers.

Finally, in addition to reducing repeat victimisation (and saving future policing and collateral costs), the dimension of care for victims has begun to receive more attention. The London Mayor's Office for Policing and Crime (MOPAC) recently established a Victim Care Unit; though important, this relatively expensive resource can be applied only to a small percentage of victims. Being a victim of fraud is sometimes accompanied by guilt and self-blame; counselling and help for both mental health and practical needs is an important and underdeveloped area, whether the individual or business person is a first time or repeat victim. Limited research has been conducted into the impact of different forms of face-to-face, cyber-enabled or mixed mode economic crimes, but there is no reason to suppose that fraud victims are any more resilient than the victims of other crimes. The fact that the individual might have been tricked into parting with their money voluntarily does not make them less in need of help, and the social benefits of reduced fraud are significant. Some will consider fraud victims to be less deserving of help, but this does not mean that they should not be equipped with the knowledge and skills to reduce repeat victimisation. Who is available to help with these tasks and how they will be paid for (if needed) and by whom, remains a difficult issue.

5.6. The police role in Pursue reassessed

Prepare, Protect and Prevent dimensions offer the police minor roles and, in light of resource constraints and expertise, these roles are possibly more suited to other institutions which can integrate these responsibilities into wider, complementary functions. Policing has in any case gradually shifted towards intelligence-led efforts to reach out and enhance sources of information (Levi and Maguire, 2012). Nevertheless, with fraud, the police are mostly dependent on what gets reported to them by victims or third parties with guardianship roles. Unless connected with already actively monitored OCGs or suspected terrorists, insider threats are reactively policed by law enforcement following reports by the private or public sector. Although recorded and victim-survey-measured property crimes have been falling, there are a host of other crime and non-crime demands on falling police resources, and newer or redefined issues requiring attention, which include counter-terrorism, child sexual exploitation online, modern slavery, online bullying, offline sexual grooming and racial harassment. Against this background, it is necessary to explore where to engage in terms of the Four Ps and how to integrate them into current policing plans and priorities.

5.7. Engagement and integration

We would argue that a number of initiatives should be undertaken, the first of which is to establish economic cybercrime as a policy and policing priority within the Four Ps framework, whether or not it is connected with formally defined OCGs.

5.7.1. Getting cybercrime from policy agendas on to policing agendas

The 2011 UK Cyber Security Strategy proposed helping law enforcement agencies to tighten up their operational response, and provide support to police forces. In the case of the latter, the Strategy sought "to drive up wider national capability on cybercrime, including through shaping the training for mainstream law enforcement on cyber issues", and to encourage all police forces to make use of NCA cyber-specialists – volunteers with specialist cyber-skills or expertise. It has been argued, however, that the commitment, performance measures and, particularly, resources has not followed; nor have they been sufficient to enable proactive as well as reactive policing, or been devolved to local police forces to address low-value, high-volume cybercrime. As the Home Affairs Select Committee (2013: 9) noted: "Ministers have acknowledged the increasing threat of E-crime but it is clear that sufficient funding and resources have not been allocated to the law enforcement responsible for tackling it."

This sort of critique is not unique to economic cybercrime – fraud in general has also seen this disconnect between policy and operationalisation – but policy, no matter how good, requires the means of implementation to have more than rhetorical impact. This disconnect is perhaps reinforced and exacerbated by the cyber element, given the issues of speed, scale and impact highlighted earlier in this report.

Economic crimes have never been a popular component of police work, for cultural reasons as well as pragmatic, due to the resource-intensive nature of investigation (Levi, 2013). In the aftermath of the government's 2006 Fraud Review, an attempt was made to address this, with modest results (Gannon & Doig, 2010; Button, Blackbourn & Tunley, 2014). Those we interviewed suggested that the term 'cyber' creates even more alarm, because it conjures up visions of technically difficult investigations that are unlikely to be fruitful in terms of a successful prosecution or recovery of assets, both of them key drivers of police resources. To date, progress has been slow; a critical HMIC (2014) report observed that only three forces of 43 (Derbyshire, Lincolnshire and West Midlands) had made 'comprehensive plans' in relation to potential cyber-attack. Furthermore, only 15 out of the 43 had considered cybercrime at all in their strategic threat and risk assessments.

Recent data suggests that less than half of the police forces in England and Wales included the impact of fraud within their last strategic assessments, and only a quarter include it regularly in their tactical assessments. Forces' assessments of the impact of crimes tend to focus on offender profiles (i.e. they are linked to crime disseminations) rather than on victim profiles and general levels of fraud in the area.[59] Indeed, our interviews helped highlight how pressure on police to give service to those who live in a particular area, systematically disadvantages those who are victims of geographically widespread multi-police force crimes, such as mass marketing frauds, especially when suspects are not within the jurisdiction, making the output or outcome of the Pursue role deeply uncertain. Evidential and extradition rules have always strongly affected the

[59] National reporting via Action Fraud does not include economic crimes in local crime maps based on postcodes.

handling of serious fraud cases (Levi, 2008, 2013), but with economic cybercrime, the need for cross-border evidence and mutual legal assistance is paramount.[60]

Unfortunately, due to capacity and resource constraints, around half of cyber-enabled frauds reported to Action Fraud are not distributed to forces if the offenders are deemed to be outside the UK. These cases are considered outside the scope of investigation, although some will be investigated by the City of London Police and the NCA. Nevertheless, discussions with a sample of police and crime commissioners' staff suggest that identity theft and other cyber-enabled economic crimes are now of major concern, and are important parts of current plans for combating business crime in London (MOPAC, 2014) and in many other regions, metropolitan and otherwise.

An important question is how to establish cyber-dependent and cyber-enabled economic crime on the policing agenda in ways that allow for a meaningful response. Taking the Pursue component of policing, for example, we can subdivide economic cybercrimes into those where (i) some or all of the suspect(s) are inside the UK, the EU or other areas that allow for extradition, and those where they are not; (ii) the offenders are part of networks that are susceptible to monitoring in advance of crimes, such as OCGs, and where they are not; and (iii) the crimes themselves can be known about in advance, or can only be investigated reactively. (In the former instance: Ponzi schemes, long firm frauds committed by OCGs, counterfeiting rings and payment card frauds; in the latter: corporate collapses, major misstatements of corporate earnings, insider dealing and dating scams.) Many of these are assisted by collaborations with the private sector, not only via information sharing but also via Cifas, FFA UK, the IPO, anti-counterfeiting bodies such as FACT and others, and the major financial advisory firms who play an increasing role in investigations and forensics. The NCA has become increasingly active in the cybercrime attribution and prosecution arena, in line with its mission to make the UK an unwelcome place for criminals to operate.

There is also a need for clarity in tasking and messaging from strategic and symbolic police actions as part of Pursue. Assessing the impact of prosecutions, disruption and asset recovery on domestic and foreign offenders remains in its infancy, but needs very careful consideration for each case. There is a need to show particular criminal networks and individuals that involvement in crime has its costs, even if the medium and long-term impact on limiting the online criminal opportunities available is modest, as has been shown, for example, in the rapid revival of alternative drug and identity data cryptomarkets following take-downs such as DarkMarket and Silk Road. Target audiences may include not just the immediate offenders but others at home and abroad, and also victims and potential victims who may need reassurance, but also Protect and Prepare lessons discussed above, via media reporting about how to handle risks.

5.7.2. Paying for the policing agenda

Another area of challenge for the medium term is the cost of policing economic cybercrime, both in terms of the availability of additional funding, where such funding should be placed and to what purpose, and who has ownership of it. High

[60] Our analysis of Action Fraud data suggests that the overwhelming majority of fraud suspects are UK-based; however, this finding is somewhat counter-intuitive, and may simply reflect victims' assumptions that their offender is in the UK.

travel and communications costs and time long pre-date the formation of police and crime commissioners and austerity policing, but are brought to the fore when 'non-essential costs' are considered. As noted above, although policing resource full-time equivalents for fraud now total at least 1,000 in England and Wales, half of these are in London. The consequence is that the scope for investigation of difficult cyber-enabled cases in London and especially elsewhere is constrained. No analysis is currently available of how many typical cases this resource could actually pursue to conviction, but when compared with reports to Action Fraud and Cifas/FFA UK, it indicates that those difficult cases that are not of the highest priority receive little police input and therefore are not prosecuted. Though desirable, good liaison arrangements alone will not solve this problem, since there are few resources available for leverage, especially given significant cuts in Trading Standards and other bodies. This risk-averse approach to expenditure on cases that may not lead to prosecution or conviction suggests that many cases are closed off at an initial stage without deep investigation. Challenging though this may be in the light of media criticism and individualised case reviews/victim demands, it can be considered irrational to spend time on cases that will 'lead nowhere'.

The cyber element of economic crime has put greater demand on policing. This has coincided with a drop in the general crime rate and in the profile of both crime and policing in contemporary Britain. One response strategy has been the growth of unconventional police funding from the private sector and government. Some of the police interviewed for this research from outside the UK were concerned that this constituted privatised policing, offering special access to state functions. However, we argue, considering trends in fraud policing resources, that provided care is taken with governance arrangements, special funding of police units cuts down inefficiencies in search time and persuasion time to help find officers willing to take on cases, for example in organised crash-for-cash insurance fraud[61] or payment card cases. The lead author's observation of these negotiations before formal arrangements suggests that previous efforts were often wasteful and unpredictable. However, the resources in these specialist units remain insufficient for the cases that exist, both cyber-enabled and not, and so even where they could be successfully prosecuted, they will not be. In these specialist areas, the principal direct victims are corporations which then pass on their losses and it may be argued that the preventative remedy lies mainly with their own efforts at reducing their vulnerability. If they find that cost-ineffective, or are unwilling to share data and efforts, then why should the taxpayer pay for the externalities thus created?

If cases are not pursued, then much of the pre-police investigative work is wasted, unless it can be turned to preventative or disruptive effect, or used for civil law measures. Interviewees from the City of London Police, the private sector and the IPO praised the ease of liaison and information transfer enabled by the creation of the 20-strong PIPCU, the IFED and by the Dedicated Card and Payment Crime Unit (DCPCU).[62] Interviewees outside London noted challenges of prioritisation between London and other UK regions. This evokes broader issues of relative crime seriousness, where what is relatively trivial in a major metropolis like London may be very serious to the public (and police) in a local constabulary, and vice versa (this is an important point of discussion, though outside the scope of this work).

[61] This refers to instances where OCGs stage car crashes in order to commit insurance fraud.
[62] In the case of the latter, DCPCU was the forerunner of these other units that began in 2002.

5.7.3. Learning from abroad?

This study does not examine in detail the experience of other countries in the broad components of economic cybercrimes. The closest parallels to the UK are in Australia, discussed in the next section. US federal agencies have a well-deserved reputation for the aggressive pursuit of transnational crime – including economic cybercrimes – with the aims of disruption and prosecution, and have played an active role in joint cases with the UK and others (in particular Europol), including infiltration and sting operations. However, there have been no independent evaluations and even prosecution data is difficult to find. Data in a recent Congressional study (Finklea, 2014) suggests that out of 12.6–16.6 million identity theft cases in the US in 2012, there were some 450 convictions for aggravated identity theft, and fewer than 800 for identity theft in 2013. Although there may have been many other charges brought (e.g. for wire fraud and racketeering), this shows that the US has a huge gap in bringing identity and other cyber-related fraudsters to justice.

The Dutch police High Tech Crime Unit has attracted top-level graduates to work on difficult cases, though retention is difficult when the cases become more routine. In addition there is the Dutch Electronic Crimes Task Force, an initiative of the main Dutch banks and the Dutch High Tech Crime Unit and Prosecution. The task force is about information sharing among banks and law enforcement bodies, and is located at the High Tech Crime Unit.

Estonia has a large pool of volunteer 'cyber-warriors' recruited in the aftermath of the Russian DDoS attacks of 2007, and (like Finland) street 'web constables' who dispense advice on cyber security at a very local level. Hong Kong and South Korea have very active policing agencies, but little is known about their effectiveness. Europol has begun to be more active in encouraging international days of action, collaborating for example with the international travel industry to combat airline fraud, such as through the Europol EC3's EU prevention strategy and the establishment of an EU network of prevention Points of Contact. In general, the relationship between policing inputs and outputs and outcomes has not been much investigated in this difficult sphere.

5.8. Targeting responses and integrating the Four Ps: combating economic cybercrimes against individuals

As the Action Fraud data suggests, the majority of economic cybercrimes (by volume) impact upon individuals – which presents a greater challenge than dealing with businesses. Thinking about how to address this challenge requires a careful assessment of resources, police priorities and engagement with other agencies to complement police roles. The effective implementation of the Four Ps will depend very much on the nature of the cybercrime. The key, we would argue, is an evidence-based approach drawing on the specific types of the main economic cybercrimes identified by Action Fraud and the NFIB. Each will require a tailored response that may or may not be applicable to other types of economic cybercrime.

To illustrate this, we look in detail at the possible responses to one fraud – dating scams – which has a very high incidence of cyber-involvement (88% as per our analysis of Action Fraud data – see chapter 4). This approach, modelling a framework for policing responses to specific types of economic cybercrime by risk,

severity, likely loss, methods of perpetration, and so on, could serve as guidance to forces.

Any strategy for policing economic cybercrime needs to have a significant educative component that is intelligible (i) to victims and intended victims and (ii) to those in a position to monitor behaviour and provide relevant advice. Such an approach also has to recognise and reflect the specific characteristics of the crime itself. Here we examine cyber-enabled dating scams to illustrate how we might apply the Four Ps Model and what could be added to this approach to increase effectiveness:

1. **Prevent:** Domestically, some effort has gone into encouraging people to use the internet safely and avoid dangerous activities, but this has focused more on protecting the victims than on discouraging potential offenders (especially when they are targeting foreign victims), or shifting them into less socially damaging activities. The Prevent component has not been seriously attempted, since people who operate primarily overseas – and many dating scams have an international dimension – are not considered susceptible to behavioural change in development. Early developments of serious and organised crime strategy had little focus on trying to re-orientate dating scammers, online or offline. There is some messaging about prosecution and imprisonment, most commonly from the US which puts more resource into international prosecutions.[63] Logically, this might lead to more reluctance among offenders to target US-based individuals, but there is no evidence to support this.
2. **Protect:** Here the approach has been to warn people about the dangers of dating scams. There is evidence that scam victims know about the risks but simply fail to register their own situation as an example of a scam (Professor Monica Whitty, informal communication). To protect customer relationships and reduce the costs of handling fraud complaints, some banks have developed schemes where the withdrawal of substantial sums in cash as a departure from normal behaviour in client accounts is considered an indicator of a scam of sorts. Once flagged, they try to talk the suspected victim out of doing so and/or identify why they are withdrawing the funds. In the case of bank transfers, such activity can be reported as a suspicious activity report (SAR) to the authorities in the hope of quick action. Nothing is known of how frequently such enforcement responses happen to what are suspected by the bankers to be crimes-in-action but are not yet formally reported by victims.

   The financial services sector is also seeking to develop software to spot patterns of scam victimisation. In the safeguarding space, there have been efforts to get (largely unregulated) online dating firms to share information about persons who have been barred from one website or firm for suspected misconduct, so that they do not just move to another website or another firm's books. Unlike child sexual exploitation online, where the card schemes have made it difficult for firms to get merchant authorisation once suspected of involvement, there is not usually much leverage for a collective market solution for economic cybercrime.
3. **Pursue:** There are some strategic efforts at selective prosecutions, and attempts by the private sector to identify patterns of receipt of bank and money service

[63] But still only prosecutes federally a small number of identity thieves annually – see Finklea (2014).

business transactions that are unusual and ought to be reported. Making SARs to the national financial intelligence unit (in the UK, the NCA) enables interception when funds are delivered or picked up, provided that there are mechanisms for prioritising them and ensuring they do not get lost in the morass of volume reports, and there are police available to make the arrests. In high-profile cases, UK and US authorities have developed good relationships overseas for cooperation with money transfer firms and police/prosecutors.[64]

This response can be developed and augmented through inter-agency working. For example, in Queensland and Western Australia, efforts have been made to develop a multi-pronged strategy for identifying and dealing with romance and other scams. Project Sunbird, a collaborative project between the West Australian Police (WAPOL) and the West Australian Department of Commerce (Commerce), which began in 2012, focuses on people who are sending money to five known high-risk countries in West Africa: Nigeria, Ghana, Benin, Togo and Sierra Leone. There are five stages to Project Sunbird:

1. **Identification:** In the context of data capture of all international wire transfers by AUSTRAC (Australia's anti-money laundering agency), WAPOL access financial intelligence about individuals who are sending money to the five high risk countries. They screen this list to generate a list of individuals they suspect are fraud victims.
2. **Intervention:** This list is passed to Commerce, which contacts each person, notifying them that they may be victims of fraud. The letter encourages the individuals to stop sending money and invites them to contact Project Sunbird staff to discuss it. If they continue to send money, they are contacted again in a more targeted effort, which outlines further details of their likely involvement in fraud and provides a fact sheet for fraud victims.
3. **Interruption:** This stage is focused on the interruption of payments, and funds transferred to West Africa, and is primarily undertaken by Commerce.
4. **Intelligence:** This involves gathering intelligence from letter recipients from both agencies which feeds into the fifth stage.
5. **Investigation:** The investigation is led by WAPOL and can focus on local offenders if relevant, or make the appropriate referrals to an overseas law enforcement agency. This final stage is quite problematic, given limited resources and the time and cost of mutual legal assistance and extradition.

Relating this back to the Four Ps Model, from a Protect perspective, initial results from Project Sunbird were positive (Cross & Blackshaw, 2014). Between March 2013 and July 2014, 1,969 first letters were sent to individuals. Financial intelligence indicates that approximately two-thirds stopped sending money, with a further 14% reducing the amount of money transferred. Of those who continued to send money and received a second letter, 44% stopped sending money and a further 33% reduced the amount being sent.

This suggests that there was some Protect and Prepare effect from these initiatives. The UK NCA and its predecessor, the Serious Organised Crime Agency, have been involved in significant collaborative initiatives in West Africa, but details of their

[64] For example, a Ghanaian fraudster was jailed in 2014 in Ghana for five years and ordered to repay (with what result is unknown) £800,000 conned from 19 British women.

impact are not available. In terms of the Prepare component, intermittent effort has been made so far to deal with repeat victimisation. In a southern UK force area, Trading Standards officers persuaded community police officers to visit victims at home and talk through their experiences, to help identify and manage social engineering. Observations suggest that some individuals respond well to this counselling, while others have difficulty. The MOPAC/City of London Police-funded Economic Crime Victim Care Unit is seeking to develop a more systematic approach as well as offering support services to individuals affected by economic cybercrime. Research on dating scams has shown that, unlike for many other crimes, friends and family often blame the individual rather than the criminal, so they are without the sympathetic support typically available to victims of crime. However, there is uncertainty over which type of support is most effective. Internationally, Action Fraud and the FBI sometimes suggest that individuals use specific online support groups; Australian police sometimes suggest they join a face-to-face group; the Royal Canadian Mounted Police sometimes suggest that victims use a telephone support service.

The ad hoc and uncoordinated nature of such responses suggests a more coherent, joined-up approach should be taken to addressing those economic crimes (if the analysis provides the basis – identified by volume, value and harm) which appear to pose the biggest risk to individuals, not only setting in place networks and partnerships but also providing the police with a model on which to base and build their responses. Their effects will require careful evaluation.

5.9. Targeting responses and integrating the Four Ps: combating economic cybercrimes against business

The role of the police and state in combating the impact of economic cybercrimes on business is more complex than it is for individuals. As discussed in chapter 4, it is up to businesses to make a risk-based decision on what cyber security measures to deploy. The question, then, is what resources should be put in place by the police, via intelligence-led policing, to reduce the risks to business and to investigate the crimes which have not been prevented.

Quite apart from the difficulties of implementing cybersecurity and the weak evidence base for the impacts of education and awareness campaigns anywhere in the world, there are considerations about how business should balance and prioritise its demands. For example, Sony has been criticised for its lax cyber security in the aftermath of the 2011 Sony Playstation hack which cost $171 million and the 2014 Sony hack estimated to cost $100 million. Jason Spaltro, then executive director of information security, made the point that, essentially, he would not pay the high costs of cyber security to avoid the risk of a cyber-attack, if the costs of being hacked were still significantly less than the cost of protection.[65]

Some commentators ridiculed his short sightedness in not including the risk of regulatory penalties, etc. and (with the benefit of hindsight) in underestimating the probability that violation would happen. Had the extra money been spent on security, then it would have been difficult to know whether or not this would have been money well spent, and the CIO might have found it hard to justify to the Sony board (if the expenditure proposal got that far). However, this underlying judgement

[65] See: www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-compliance.html.

problem is true of many risk decisions in business (and in government), and both risk from criminal threats and risk from regulatory action have become far more salient as well as prevalent in business today. Security is not a value that either does or ought to trump all others, and risk appetites reasonably may vary; the risks should be measured where possible in a human security context, depending on the type of business. It could be argued that if Sony had taken such a risk-based decision and decided to economise, the police (in this case, the FBI) should not waste US taxpayers' funds on investigation. But quite apart from (in)consistency with other police practices in theft, burglary and violence reports – where victim 'negligence' is not usually viewed as disqualifying them from police help – there may be other reasons to investigate: for example, the wider political conflict with North Korea associated with this particular case. If individuals or the government in North Korea had been demonstrated to be behind the hack, then genuine mutual legal assistance and extradition would not have happened. Hence the complexity of evaluating whether investigation is or is not a good use of public resources.

5.9.1. The current approach: the police

The existing strategy involves a combination of active and passive elements. The traditionalist model of policing is to take the cases that come in and handle them according to the resources available, discarding them if crucial evidence is unavailable or the suspect is unobtainable. When forensic and/or investigative resources are exhausted, the remainder of cases are queued until resources are freed up. Historically, a resource boost has seldom happened except when a fraud has exceptional political or media interest. The more active model is to try to increase policing capacity, either by demonstrating serious harm from crime/threat from offenders, or finding new sources of income, such as proceeds of crime funds or sponsorship.

The City of London Police has been proactively following the latter strategy. Three units have been created with financial support from the business sector to deal with organised frauds. These are staffed by police and civilians, with fairly hands-off governance arrangements so that the industry sectors can influence overall strategy but not individual cases. In the medium and longer term, the relevant business groups can reduce or increase support for the policing units if they consider that the latter are no longer meeting their needs or that their work merits more funding. These are areas where business and the police have moved towards working arrangements in terms of resourcing and information that address what each perceives as significant and organised threats.

These include:

- **Payment card and online fraud:** Immense progress has been achieved via cooperation between the industry-funded DCPCU, FFA UK and Cifas, but issues of individual responsibility remain. Police Scotland is currently outside Action Fraud but has strong relationships with the financial services sector across the UK. The Scotland Unit has developed good external relationships with foreign police forces through regular joint work.
- **Insurance fraud:** This has a relatively low cyber component, other than that ICT is used for communications and software for data analysis for the Insurance Fraud Bureau, which pools industry-wide data, and in other insurance fraud initiatives by the Association of British Insurers (ABI) and individual firms. There is also the police unit IFED which targets serious and organised attempts to defraud the insurance sector.

- **Intellectual property crimes:** There is strong inter-agency working between the IPO, the police and Trading Standards. However, they are working in an environment in which public attitudes are deeply ambiguous, except in safety-critical and some health frauds (Large, 2014; Wall & Large, 2010). Scotland is a good role model for inter-agency collaboration, but there are good initiatives elsewhere (for example, North Yorkshire) to disrupt IP and other consumer crimes, if not necessarily those with a strong cyber component.

Such collaborative efforts are to be praised and welcomed. This level of joint working responds to identified and co-resourced issues that balance organisations' concerns with a level of response in one particular area – Pursue – while leaving the Prevent and Protect element of risk management to organisations.

Quite apart from the practical difficulties of implementing cyber security through changing personnel, distributed workplaces and complex supply chains, and the weak evidence base for the impacts of education and awareness campaigns, this raises the question of how businesses should balance their security demands against other functions. However, these are wider issues for industry and business rather than policing.

On the other hand, and outside the three areas noted above, one of the weaknesses of the police response to economic cybercrime has been in the area of cross-force, national and international crimes below the level of seriousness to warrant the scarce resources of the Serious Organised Crime Agency and its successor, the National Crime Agency. The situation has been improved by additions to the regional Special Operations Units, but there remains the problem of fractured responses from individual constabularies and a need for national units to deal with the externalities exploited by criminal networks, cyber-enabled or not, and which have to be paid for. We would argue that three of the Four Ps should be less of a law enforcement concern, apart from the provision of intelligence and information, than for industry bodies, government bodies and collaborative arrangements. We would also urge that, in terms of resilience, governments, public organisations and local government might want to be more proactive in requiring demonstration of effective risk management systems from those with whom they do business, certainly as suppliers and contractors. We would also argue that business requires much more evidence of an effective deterrent, whether in terms of disruption or prosecution, and the emphasis should be on Pursue. Nevertheless, there still remains a challenge as to what type of Pursue efforts we are prepared to resource.

In such circumstances, law enforcement may have to develop a hierarchy of responses that takes into account not just the impact and economic losses suffered by victims but also the broader social impacts captured in the concept of 'signal crimes' (Innes, 2014). This would include robust evidence that the threat is taken seriously, judged by reassurance and commitment. It may be necessary to confiscate the ICT tools employed by some of those involved in hacking and other disruptive but non-acquisitive cybercrimes as a visible sign that, alongside Prevent and Protect, there is some attempt to stop offending: mechanisms may have to be found to stop offenders accessing the internet, as was done with the American hacker Kevin Mitnick, for example. For economic cybercriminals, it may be possible to request (through civil or criminal routes) a Serious Crime Prevention Order under the Serious Crime Act 2007 as amended by the Serious Crime Act 2015, which is available for offences including fraud, money laundering, public revenue cheating, corruption and bribery, counterfeiting, blackmail and intellectual property theft. This

creates civil contempt powers to regulate the number of offenders' mobile phones, their travel and business activities and contacts, etc. We consider that, given the small number of offenders convicted, restorative justice is not a particularly salient response, but this might serve as a way of reinforcing a message of harmfulness among younger offenders or potential offenders. (Though, we need to be aware that there are risks inherent in the different ways that such measures could be interpreted).

Of more importance would be the reliance within the Pursue framework on disrupting cyber-enabled crimes, which can be done either via surveillance/informants/covert human intelligence sources or by rapid reactions to crimes in progress which reduce criminals' 'take' from one victim or a run of victims.

On the other hand, disruption is a contested approach in terms of longer-term effectiveness. As noted previously:

> "Because the notion of disruption can be used to signify a wide range of acts, and can be applied to a variety of criminal actors, it is not at all clear how the effects of a specific disruption contribute to the overall systemic measure. Still less clear is how an annual increase in the number of criminal enterprises disrupted is a measure of the increasing effectiveness of the criminal justice system." (Innes & Sheptycki, 2004: 22).

Nevertheless, disruption does offer an extensive set of tools which are used against a number of other areas, from child sexual exploitation to organised crime groups. They are also used by major industry players such as Microsoft and FACT, and by transnational police agencies such as Europol's European Cybercrime Centre. As early as 2011, the NFIB suspended a number of websites, telephone numbers and email accounts and redirected those who accessed the suspended websites to an alert page. Disruption also allows law enforcement to take a more proactive approach in engaging with potential offenders and their networks. It can provide relevant intelligence and the basis for reciprocity of information sharing that, as we have already noted, is a significant part of the development of Protect and Prepare. Nevertheless, although these indicate to victims and politicians that something is being done, the effectiveness of disruptive tactics such as incapacitation beyond the immediate case is often difficult to assess, whether they are small operations or massive take-downs such as DarkMarket and Silk Road.

There is arguably a case for realism combined with transparency – telling individuals and businesses that their cyber-enabled frauds cannot be investigated effectively to conviction unless the offenders are within the jurisdiction of our legal system, and even then these investigations are difficult enough. The high numbers of people being given extra training to roll out core cyber-investigative competence to the police, should help to address this challenge.

However, it may be necessary, given businesses' concerns about the absence of an effective law enforcement deterrent, that business funds a specific task force whose objective is to address cybercrime directed against UK business – and possibly some material cybercrimes against individuals such as dating scams – from overseas jurisdictions. This model, as we have noted, has worked in three specific areas and has been utilised to some effect, using a spectrum of quasi-law enforcement approaches and a range of criminal and civil sanctions, in the private sector (such as intellectual property, where its use has been contentious). It may encourage the privatisation of policing but it is a pragmatic route to efficiency.

There is a risk that the police and media have overstated the technical difficulties of cyber investigation but understated the jurisdictional problems in recovering both offenders and money. To date, there have been a few cases of cyber money laundering in Europe (e.g. via Bitcoin) and offenders will usually cash out the proceeds at some stage. Recovering them may require better implementation of existing mutual recognition mechanisms within the EU and Council of Europe, and globally. Though the European Central Bank currently takes a different view, the UK has more positively expressed an intention to regulate cryptocurrency exchanges for anti-money laundering and other purposes, as well as to examine the prospects for making them work at scale (HM Treasury, 2015), and the use of proceeds of crime approaches, through using:

- Laws on cybercrime or fraud against hackers targeting users (Bitcoin-stealing malware, mining malware, network disruption malware);
- Laws on financial regulations against intermediaries and third party platforms making transactions without any agreement (unlawful banking/deposit-taking); and
- Laws on money laundering for marketplaces that assist criminals to launder proceeds of crime.

This approach, which has to address economic cybercrime against individuals as well as business, with the purpose of seeking prosecution and/or confiscation, would act as a necessary policing signal that, across the Four Ps, law enforcement is responding to security and confidence issues with a range of measures. It would also be of value if any recovered assets were, as with the general 'payback' approach, seen to be used to fund community or other Protect initiatives.

5.10. Challenges of the current approach to victims generally: choosing between the 'Ps'

As the Pursue component remains under severe pressure and has not yet received significant allocations from police resources, the other components of the Four Ps Model also need revisiting and refining in terms of a targeted (and widely advertised) response. Indeed, to draw on previous reassurance policing and signal crime policing, we would recommend comprehensive messages that emphasise police choices and solutions through identifying 'signal' concerns; visible control – reassuring the public by offering visible proof that their problems are important to the police and are being addressed in specific ways; a targeted, intelligence-led approach focusing resources on a hierarchy of threats drawn from Action Fraud/NFIB data; joint action from the police and other partner agencies across at least three of the Four Ps; and evidence of dedicated resources where practicable (see Millie, 2014).

Here, we may need a significant educational focus across all generations of the general public, using insights from behavioural economics to 'nudge' them into greater and better informed care of their ICT; in addition, we need a network of people at grassroots level and via various communication mechanisms, including social media, to provide support when needed. It is essential to keep emphasising the importance of checking whether something sounds 'too good to be true'.

This raises problems for banks, which are under pressure on the one hand not to act as oppressive paternalists when government is encouraging freedom, and which, on the other hand, are liable to be blamed for not protecting the vulnerable, even when they have no legal mandate to stop account-holders from spending their own

money how they choose. Banks and Cifas are improving efforts for those identified as vulnerable, though the criteria used when classifying people as 'vulnerable' require considerable care. It is not just the 'elderly' or the 'mentally ill' – both of which are on a spectrum of vulnerability; social attitudes to victim culpability also play their part. For some individuals, no Protect and Prepare efforts will work. It is also arguable that they should not receive scarce Pursue policing resources because they have not exercised due diligence on their own behalf. But who will convey these messages and who will listen to them and respond with better self-protection? Or will/should they be left to make their own decisions and suffer the consequences? We need a more serious debate about the actual and proper limits of policing by the police and financial institutions than this has so far received.

In principle, the model of external funding for particular industry-focused action for business increases the general funding pool for economic cybercrimes and releases more police for those fraud victims who cannot afford to pay for their own policing. In practice, this framework merely sets out a high-level set of parameters. The question then is what criteria should be used to guide the allocation of funds to the Pursue function generally, and to what particular sorts of frauds within those allocated funds? With finite resources and excessive demands upon them, criteria will exist – the question is whether they are explicit and thought through, or are implicit and a less well considered reflection of priorities. Whether they should be made public is another decision, and one that should be informed by a willingness to engage with the public to enhance legitimacy. This is always an uncomfortable area because media and political demands are often stampeded by populist reactions to individual cases (or by critical HMIC reports that the police should do better), when (as in other areas of policing such as 'historic abuse cases' and in other public services such as medicine) the question is what aggregate levels of support can be managed and supported collectively. This requires hard decisions on the differentiation and consistency of response.

Another area of challenge relates to how the negative impacts of cybercrime are managed in policing. Research does not currently tell us the relative impact of economic cybercrime compared with otherwise similar face-to-face scams. It could be inferred that frauds undertaken face-to-face have greater negative impact than those carried out online. Yet the sense of powerlessness and violation that often accompanies identity fraud and, a variant of that, dating frauds might suggest that cybercrime has at least as much impact, if not more so in some cases.[66] As regards personal and financial information lost in data breaches from business or government, this can have both financial and emotional repercussions that are hard to predict or measure in the current state of our knowledge. Remediation via reassurance mechanisms – including protective registration against identity theft – is possible. It is an open question whether there should be a greater degree of compulsion on private and public sector bodies which lose personal and financial data through security breaches to provide free monitoring and protection to those individuals affected. This might encourage organisations to protect their data better; though the vast data breaches in recent US corporate and government cases would suggest that this is a bigger cultural problem than a rational or economic one. Nevertheless, even if it does not lead to greater care by organisations, one might

[66] A caveat here about comparing like with like: dating frauds are not just about money but about the twisting of affection, so their comparators would be offline dating scams, for example.

argue that it is a right of victims that contributes to restorative justice as well as to reduced re-victimisation risks.

Much hinges on the interpretation of the term 'vulnerability' as applied to fraud victimisation, and on intentional or merely implicit case selection. Here we would propose a review of the 2004 Home Office guidance on fraud acceptance criteria (see Table 5.3) for fraud generally, and economic cybercrime in particular, now that Action Fraud and industry data paints a much clearer picture of risk and threats.

Table 5.3: Home Office Fraud Acceptance Criteria 2004, as subsequently updated by one force outside London

Higher priority cases	Lower priority cases
• The victim(s) are believed to be vulnerable: for example, older people, people with disabilities and other protected groups under the Equality Act 2010,[67] businesses providing key services in difficult circumstances, or in distinct communities. • Frauds having a significant impact on the victim(s). For example, a negligible loss to a large company could be catastrophic for a private individual or small business. • The offence is believed to be part of a linked series within the force area. • Strong positive lines of inquiry are immediately apparent. • The offenders are part of an organised crime group and the activity reported would score 'high' on the harm matrix. • There are clear opportunities to identify and restrain assets from the criminals with the aim of pursuing confiscation or forfeiture proceedings. • The circumstances under investigation fall within the category of a critical incident, or the decision not to investigate could have a significantly detrimental effect on public confidence or satisfaction. • Frauds giving rise to significant public concern, possibly highlighted by a high degree of press interest. • Frauds involving substantial sums of money. (NB: Cases meeting the acceptance criteria of the Serious Fraud Office may be referred	• The investigation would require a disproportionate level of resource to bring the case to a conclusion and would adversely impact upon law enforcement's ability to investigate other crime. • Frauds where the likely eventual outcome, in terms of length of sentence and/or financial penalty, is not sufficient to justify the likely cost and effort of the investigation. • The victim has pursued civil recourse and has subsequently turned to the police for a criminal investigation as a result of dissatisfaction with the civil remedy. • Delays to the investigation would be caused by the location of key evidence elsewhere. • Available resources would not permit an immediate and expeditious investigation. • Victims have ignored guidelines designed to prevent them from becoming victims of fraud, for example online banking and auction sites. • Frauds where the victim's conduct has contributed to the loss, in particular where the police have previously given guidance or warnings to victims about fraud risks that have not been acted upon. • Cases where the victim's motive for making the complaint appears to be malicious and is primarily focused on recovering monies owed, or designed to distract attention from the complainant's own involvement in the fraud. (Such cases might nevertheless merit investigation, particularly where there are other victims involved.) • Cases where victims are not prepared to cooperate fully with the investigation and prosecution, although we will always

[67] The relevant protected characteristics under the Equality Act 2010 are: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

Higher priority cases	Lower priority cases
directly to them, either by the victim or the police.) • Frauds committed by, or knowingly facilitated by, professional advisers, e.g. lawyers, accountants, merchant bankers. • Frauds likely to undermine confidence in leading UK institutions or otherwise undermine the economy. • Frauds committed by members of boards or other senior managers. • Frauds where law enforcement action could have a material deterrent effect. • Frauds which indicate a risk of more substantial/extensive fraud occurring. • Cases where the victim has devoted significant resources to fraud prevention or has been willing to participate in appropriate crime prevention partnerships or otherwise assist the police. • Frauds which it has been agreed should be a current law enforcement priority.	consider carefully how to assist victims and witnesses who have concerns about safety. • Frauds more suitable for investigation by another enforcement or regulatory agency. • Cases where another police force has decided not to investigate other than for geographical reasons. • Frauds that have already been investigated by the police or another enforcement agency, or that have been the subject of regulatory proceedings, unless significant new evidence has come to light or the previous investigation had a narrow remit that did not address all the relevant issues. • Cases where the existence of other proceedings might have a detrimental effect on a criminal investigation and subsequent prosecution. • Frauds which took place a long time ago (probably more than two years), unless there are exceptional circumstances.

Evidently this leaves a great deal of room for discretion, since there are more cases that fall within the higher priority category than there are resources available to deal with them; and if the police were to disregard the lower priority cases, this might be 'rational' but not politically acceptable. Repeat victimisation in this model is also missing, except within the category of 'frauds which indicate a risk of more substantial/extensive fraud occurring', which suggests more concern with offender escalation than with repeat victimisation. Perhaps in a Pursue framework that is a correct approach, but in a Prepare and Protect framework we might expect a stronger focus on reducing repeat victimisation, as well as on victim care. It shows that the lessons from our growing understanding of domestic and sexual violence and of burglary have not yet fully transferred to the fraud arena, perhaps because public awareness and lobbying groups are less developed for fraud.

The marginal status of economic crime – especially cyber-enabled – within policing may also be inferred from the limited information we have about its policing outside London. Efforts have been made to address this, such as the establishment of an Economic Crime Command and a National Cyber Crime Unit within the NCA, both of which can if necessary draw upon constabulary policing resources as well as their own. But it remains to be seen what impact this will have upon levels of economic cybercrime.

Despite such changes, what we are prepared to resource for the policing of frauds that do not fall within that category remains a challenge, especially as these types of fraud increase as a proportion. For example, in Greater Manchester, 60% of volume fraud cases were cyber-enabled. With the complexity and escalating number of complex, high-value frauds, this led to a management decision to

subsume dedicated volume fraud teams into the serious fraud teams in order to address the higher order demands (King & Doig, unpublished). This points to a serious problem: either we tell victims (as presently) that their complaints will be used for intelligence only, or we struggle trying to investigate cases, many of which will not reach the prosecution stage. In the abstract, we might prefer to raise the capabilities and the resources to conduct cyber-enabled fraud investigations.

This can only come from taxation (which has been ruled out for the present), from reallocating resources from other areas, from unpaid private volunteers, or via privately or publicly paid forensic investigators from the private sector, some of whose work currently has to be reinvestigated by police units to ensure investigative continuity to satisfy the courts. Evidential rules and judicial attitudes may need to change before the private sector can play a bigger role. We accept that policing has to battle for resources with other crime and social problems. These are balancing issues of enormous difficulty for the police, the NCA, the security services, and for all those in whose name this balancing occurs – the general public and businesses of all sizes. Even if we were to raise investigation levels for economic cybercrimes to the resources found in US agencies, many such frauds would still remain uninvestigated or, if investigated, would not result in prosecution.

5.11. Summary

This chapter has addressed the question of where and how policing may become more engaged in economic cybercrime. The preceding chapters have emphasised the remarkably complex nature of the landscape in terms of types of cybercrime, against whom, and to what purpose. The figures of losses, while significant to offenders and to victims, are variable as a ratio of other crimes and their costs. The mass attacks, their geographical location and so on make a significant investigative response problematic. Certainly, business and the public sector in principle have the resources to respond and in those areas where a law enforcement response is required, dedicated units predicated on joint working have been established. This is currently being reinforced by high-level police cybercrime units. These, however, are more likely to operate at the high, organised and severity ends of the Pursue spectrum, leaving the bulk of volume cases at the individual level where police resources, staffing losses, etc., mean that prevention and protection, or even disruption, may be a more realistic response than pursuit through criminal courts. Who should do this, and how, is a significant social issue that requires informed debate.

6. Concluding remarks and suggestions for next steps

This report presents a modest exploration of what we know about the evolution of cyber-enabled and cyber-dependent economic crime and how it is being and could be policed. This has turned out to be a much more complex and still evolving inquiry into how to manage a varied set of local, national and transnational problems of consumer and business awareness, transformation of awareness into action, and private–private and public–private collaborations in risk management, in which police and criminal justice interventions have played a modest part. In a sense, this is as it should be. The regulation of harm in society is primarily about how we understand and manage risks socially, and there are limits to what specifically police intelligence and criminal justice can achieve in this regard. Some might argue that if GCHQ is going to continue to collect metadata about all our daily communications, it might be put to more use in combating fraud and cyber-enabled crimes; but that would require not just a change in its mandate but also people willing and able to act on the information, from Libor and corporate price-fixing cartels to organised mass-marketing frauds.

6.1. The scale of the challenge

This research has shown that incidences of cyber-enabled and cyber-dependent economic crimes have been rising, though the lack of comparable data for previous years makes this a matter of interpretation rather than demonstrable fact. Nevertheless, fraud is a distinct and definable crime category and the Action Fraud data indicates that the cyber component is significant and growing. However, given the rise in the number of internet-enabled devices and the proportion of the population who are connected, it would be extraordinary if this were not so. Given a large number of people around the world with the motivation to defraud and so many situational opportunities that the internet now provides, it is somewhat surprising that the crime rate is not higher. The data indicates that there are significant variations in the impact of cyber-enabled and cyber-dependent economic crimes by crime category, and even within the latter there are non-trivial variations in the level of cyber-involvement in the crime, in the types of victims (whether businesses or individuals), the interplay between cyber-involvement and other communication modes for the commission of the crime, and the losses associated with the crime. Such variations have implications for responses which, for the purposes of this report, we have addressed under the Four Ps Model.

6.2. Developing responses

This report has noted the various initiatives and strategies undertaken by law enforcement and non-law enforcement organisations, and sought to provide some guidance and evidence about what a broad policing approach can do – or could do – to protect individuals and businesses from economic cybercrimes. However, guidance is not self-implementing. People have to know what to do and to actually carry out these measures and review them over time: cyber-fraud prevention is not a one-time effort, and both online and offline social engineering seek to move potential victims away from the protections they might know about in the abstract.

Nevertheless, we are persuaded from the Action Fraud data that much of the reported economic cybercrime does not lend itself to a traditional reactive law enforcement response, given either the criteria noted in Table 5.3 or the normal acceptance criteria applied by individual forces, unless there is evidence of numbers of linked series of allegations or large numbers of lower-value cases against

groups of individuals. The police, either by themselves or with partner organisations, have long pursued awareness and alert campaigns and ICT vulnerability would lend itself to a similar approach, particularly for individuals and SMEs.

Even once messages have been disseminated – on radio, television, the press, and via friends and family – there are always some who do not follow the advice, and we suggest automated security with opt-out rather than opt-in, especially if insecurity can cause problems for others, such as botnets. We suggest also that more behavioural research would help to identify what needs to be done to 'nudge' such people to take action to protect themselves and make better informed judgements, while allowing them to continue to enjoy the benefits of the internet. Certainly, the imperfect information on the nature, motivation and geographical location of the perpetrator, as well as the limited possibilities of prosecution and even more limited likelihood of recovery of any losses, emphasise proactive prevention rather than the reactivity of an investigative response. Time spent on information security, however, also has an opportunity cost, and many of those who are not security professionals are generally reluctant to 'waste' time on what they see as an unproductive function (until or unless their inaction has serious consequences). Here we would also like to see a 'nudge' to encourage financial and other services to be more proactive in requiring the use of mandated software, if only to encourage more security awareness and less self-determination among businesses and the public who do not have a common understanding of what to do to protect themselves, and why.

There is scope for a more dynamic, structured and response-focused approach to guidance, warnings and awareness-raising, to complement the valuable alerts that the NFIB and the NCA currently put out via media contacts and by their open and protected circulars. The latter go directly to professionals rather than to those who are not 'fraud experts'. The police have made increasingly successful efforts to mainstream fraud issues into radio 'soaps' and television documentaries, as well as consumer programmes on radio and television. It would be possible for the police or other approved bodies to set up educational 'sting operations' to warn users who respond to fraudulent offers of different kinds (created by the authorities) that they could have become victims of fraud, via on-screen 'pop-ups'. (Such tactics could also be used on criminal marketplaces as warnings to those seeking illicit products or co-offenders on the web.) This might lead to greater reflection by potential victims on their vulnerability, though there might be attempted push-backs by the public and media about police intrusion.

When people become victims and recognise that they are – two stages that do not always happen at the same time – they may be more receptive to prevention advice as well as meriting care. Button et al. (2015: 208) conducted interviews with some online fraud victims and assert:

> "there was a view amongst the victims and the stakeholders that providing an opportunity for the victims to meet the fraudsters and articulate the damage it had done would be beneficial to both the victims and the offender. The global nature of online fraud would pose more practical challenges compared with other volume property crimes. However, there are offenders based in the UK and with modern technological developments the challenges are not insurmountable."

This might be helpful for those few offenders who are convicted in the UK and overseas, but its impact both on offending rates and victim satisfaction remains to

be seen. We do not currently regard restorative justice as having a major role to play in economic cybercrime in the near future.

Nevertheless, it may be asked if those who do not take any protective measures should be entitled to the same level of policing effort than those who do, and should this assistance also reflect the affordability of those protective measures? (This applies equally to how we treat victims of other property and violent crimes who do not take 'sufficient' precautions.)

There is another policy question concerning the appropriate level of policing and in which parts of the country, and about how we can ensure both adequate levels and an appropriate balance between prevention and criminal investigation/prosecution of economic cybercrimes. We have noted in the previous chapter that law enforcement can draw upon experiences in other, non-economic, areas of online crime such as child sexual exploitation and hacking, and may have to develop a hierarchy of responses according to their own priorities and assessment of the data. Nevertheless, we consider that the police need to develop and communicate more clearly their strategic response to 'signal economic cybercrimes', preferably accompanied by independent evaluation of the impact of those responses.

This is a difficult decision because honest assessments of how much and what kinds of economic crime the police are able to handle are bound to arouse controversy. This might be accompanied by a decision about which economic crimes might be required to be reported and which, as under the present approach, are voluntary. Even if reporting were to be compulsory, it is not clear what the sanctions would be and how they would be enforced, and both businesses and individuals might still need to have explained to them the potential benefits of such aggregation of intelligence for the country, for their business sector, and for themselves personally.

Larger businesses may require more sophisticated versions of the same approach, particularly in terms of expert alerts and guidance, so that they can revise and refresh their own security arrangements, including ensuring the appropriate conduct by staff as well as the more technical and system-based controls.

Within the totality of the response framework, however, there will still be a need for a suitably resourced investigative response. Whether this will be focused on volume, value, harm or perpetrators will require an assessment of the purpose – deterrence, disruption, denial of the proceeds of cybercrime, and so on – as well as whether this will be located at national, regional or local levels, whether it will be technology led, and whether it will focus on cybercrime in general or economic cybercrime in particular.

These are not issues to which there is a clear answer, but we hope that we have provided a basis for continuing dialogue on these important social and economic issues, which touch an ever-increasing proportion of the population, in proposing themes, issues, questions and potential police responses.

6.3. Themes from the research

- The routinisation and pervasiveness of internet use has made certain types of internet-based crimes for economic gain possible (cyber-dependent economic crimes), and has facilitated immensely the scale of others (cyber-enabled economic crimes) by reducing the cost and effort of reaching out to potential victims.

- Cyberspace is constantly evolving, with an extensive range of functions, services and products, while also providing platforms for aggregation and innovation in the perpetration of economic cybercrime.
- Cyberspace has multiple criminal actors living in many jurisdictions whose typologies and methods of organisation and operation do not lend themselves easily to existing categories and understanding.
- Cyberspace is developing its own criminal marketplaces and financial arrangements that require specialist awareness and access to address.
- The perpetration of economic cybercrime outstrips preventative and other measures for control protection and has increased the difficulties of identifying, investigating and prosecuting offenders as much as it has increased the vulnerability of businesses, governments and individuals (including the general public).
- There is widespread agreement that policing, both in the UK and around the world, is being challenged by evolving patterns of crime, especially economic cybercrimes and the cyber-forensic aspects of police investigations.
- UK policing resources are reducing, driven as they are by competing priorities and agendas in a time of economic stringency. Those initiatives that are in place in relation to cybercrime are emerging rather than comprehensive and established.

6.4. Themes from the UK data

Despite its limitations, the available data, particularly that from Action Fraud, can provide a foundation for more evidence-based policy with which to refresh and refine existing strategies and approaches.

- There is a high level of cyber-involvement in reported cases of fraud but there is no established pattern in terms of what categories of crimes have cyber-involvement, or by whom they are committed.
- Cybercrime for gain is significant, much more significant than perceptions of non-economic cybercrimes.
- Losses are substantial by case and by crime, but there are significant variations – not all economic cybercrime results in large or emotionally significant losses and not all such crimes require ICT.
- Even in those industries with established Protect and Prepare approaches, such as financial services, the level of cybercrime remains high.
- The level of financial asset recovery from offenders, whether primary offenders (the fraudsters and counterfeiters) or money launderers (financial intermediaries or professional launderers), is low.

6.5. Questions for responses to economic cybercrime

- Who within and outside policing should be involved and in what capacity?
- What are the specific roles and responsibilities of the police and where should ownership lie in terms of tackling cybercrime and economic cybercrime?
- What resources (in money and effort) will be considered worthwhile for greater cyber security?
- How will that security be organised for and/or by the huge numbers of businesses and people that are (potentially) affected?

6.6. Potential policing responses

1. Establishing cyber-dependent and cyber-enabled economic crime on the policing agenda in ways that allow a meaningful and realistic response, where the role of the police is less about being the sole player in the law enforcement landscape. It needs to be more about identification of specific roles and responsibilities in that landscape, alongside equally realistic assessments of the roles of other agencies and the promotion of partnership and other arrangements.

   This requires a careful analysis of resources, police priorities and engagement with other agencies to complement police roles. The relatively ad hoc and uncoordinated nature of such responses currently suggests that a more coherent, joined-up approach should be taken, addressing those economic crimes that by volume, value, harm and/or severity of threat, and identification of the organisation and location of perpetrators appear to pose the biggest risk, while admitting that the rest are going to be left unpursued. Undoubtedly there will be parties – politicians, the media and sections of the public – which will find this unacceptable. However, demonstrating that the police could do more with the same, with the aim of achieving greater resource provision, might help to address this.

2. A review of the 2004 Home Office guidance on fraud acceptance criteria for fraud generally, and economic cybercrime in particular, now that Action Fraud and industry data paint a much clearer picture of current risks and threats (though the NFIB's case screening rules go some way towards this goal).

3. For individuals and SMEs, the dominant thrust of policy and action should be in the Prevent, Protect and Prepare sphere, with the police developing coherent strategies, coordinating identification of key risks and threats from data (plus 'guesstimating' the problems of 'known unknowns'), preparing communications materials, developing response packages for individual forces in relation to the most common and harmful economic cybercrimes, identifying relevant partnerships and associations with their respective constituencies, and promoting better arrangements for cybercrime victims (for both care and reducing repeat victimisation).

4. For large organisations, there is a need for promotion and participation in information sharing and police/government/industry guidance on emerging threats and trends around which the organisations can develop their responses, while establishing in policing terms across English and Welsh police forces sufficient resource and expertise to provide some assurance. The aims are to increase appropriate business and customer confidence in the security of the internet and offer some credible downside risks to cybercriminals, including freezing and confiscation of the proceeds of cybercrime in countries of operation and offender residence.

5. A hierarchy of law enforcement responses focused on indicating to businesses and the public the presence of law enforcement in this space, as well as investigating and prosecuting the perpetrators where feasible, are likely to have the greatest deterrence impact.

It could be argued that those crimes which are reported to Action Fraud are those that the public want the police to do something about. Whether, in the absence of an insurance claim motivation for businesses to report crimes, this relative lack of Pursuit will lead to a fall in Action Fraud reports over time, we cannot tell, though this

seems plausible. Enhancing our intelligence about fraud levels and patterns may be less attractive to victims than it is to security professionals. If it does lead to a fall in reports, there will be a greater disparity between police-recorded data and both individual and commercial crime surveys in the future, at least in those areas of economic crime that are measured by the surveys. There are arguments in favour of making the reporting of identified fraud to Action Fraud compulsory – it may drive up Prepare, Protect, Pursue and even Prevent activity, and some businesses which currently do not report because of fear of reputational damage relative to their peers would then feel less uncomfortable. Provided that the police ensured the confidentiality of those reporting, this would help limit media publicity to where there were arrests and charges. However, there needs to be acknowledgement that this involves firms and individuals in opportunity costs, and even if it is made a legal compulsion, effort should be put into using the data or it becomes a socially valueless burden on the private sector. If it is compulsory for the private sector to report cyber-enabled crimes, it seems logical to apply this to the public sector also.

However, care must be taken about information gateways – would these also have to be reported/be allowed to be passed on to the Information Commissioner's Office and (for regulated institutions) to the Financial Conduct A*ut*hority and even to the Prudential Regulation Authority, the Solicitors Regulation Authority, etc.? Would compulsory reporting cut across the voluntary or sometimes contractual sharing agreements in CiSP, CERT-UK, Cifas and industry associations that also aim at Protect and Prepare? For transnational firms, there are already complexities arising from the EU Directive 2013/40/EU on attacks against information systems which, inter alia, require member states separately to introduce reporting and CERT-type mechanisms for data breaches and cyber-attacks.

We have no doubt that, for routine purposes, forensic digital awareness is important for the police: data and its retrieval are a core part of tracking, verifying and falsifying suspicions of all kinds, and there is no escape from this need. 'Cyber', like financial investigation – often badged as 'money laundering' and 'proceeds of crime'– needs to be mainstreamed into criminal investigation and crime prevention. All these terms carry cultural baggage which should be demystified so that we can match the need for varying degrees of technical skills against different levels of investigative difficulty. The procurement of these will need the continuing commitment of the College of Policing, police chiefs and those to whom they are accountable. In principle, one might hope for a standardised service throughout the UK, but this should not be at the expense of the best service in some areas. Cybercrimes present challenges to policing, not least because one of their core activities (Pursue) is hardest when suspects are unknown or are believed to be abroad, particularly in areas where mutual legal assistance in gaining evidence and in extradition are difficult or impossible. This is an area for government and police/NCA liaison to work on, but the current system (at least outside the EU) cannot be expected to function well for other than the most serious crimes.

6.7. Summary

We have presented, at times, a somewhat bleak view of cyber-dependent and cyber-enabled crimes and police responses to them. While economic cybercrime is not an insurmountable challenge to policing, it is necessary to think critically about what can be achieved with existing resources, as a vital prelude to producing

'satisfying' approaches to the varied problems. This sentiment was recently expressed by the head of the National Police Chiefs' Council.[68] Even if a 'reasonable' amount of extra resources was available, this would not solve a large proportion of the investigations into economic cybercrime, nor would greater investigative success alone reduce substantially the levels of such crime.

We, the public, need to accept some responsibility for our susceptibility to internet and telephone-enabled offers from strangers, acquaintances and even from people we think to be our friends. But we deserve and need to be helped to make better decisions with our money, and the police can play a collaborative role in arrangements to provide that advice before and after we become victims. A start might be made by asking, for every economic crime, what it would have taken to have stopped it from happening or to have reduced its scale, and then to see who – victim awareness, software or internet service providers, third parties or police/other enforcement agencies – might have intervened to stop those harms, and why they did not either attempt or succeed. For public reassurance and for deterrence/incapacitation, some police action is needed and more up-skilling from existing officers is necessary. If we accept that paternalism is appropriate, this could include disruption of suspected frauds-in-action via banks, families, money service bureaux, etc., though the potential victims themselves might resist because they do realise that they are in the process of being defrauded. For the rest, we need to prepare ourselves for a long struggle against local and transnational criminals using the internet and the telephone to extort us, to deceive us into thinking we are dealing with genuine organisations, or who persuade us that their offers are not 'too good to be true'. Indeed, for us to ask ourselves that question rather than be gulled into trust would itself represent progress.

It is important to realise that all countries, not just the UK, are grappling with these difficulties. The substantial problems of cyber-enabled and cyber-dependent economic crime, which have been far from eliminated by policing and prevention efforts, arise across the world. We are in the early stages of a long struggle to reduce cyber risks and economic crimes generally, and we would do better to think of this, practically and feasibly, in terms of better risk management than risk elimination.

Our suggested next step for this includes the need for better, early education of risk management (relevant for not just economic crime but also child exploitation and bullying online). We also need to focus on helping vulnerable citizens to appreciate and manage the risks of both online and offline fraud, and this may be better done via peers and the third sector than by the police and websites alone, however user-friendly. For both individuals and businesses, we need a focus on security that is built in to products and online interfaces, that is not obstructive and that is explained clearly to people.

This report has dispensed with the usual set of advisories. Of course people and businesses should group together and share their experiences and engage in problem-solving (though in the real world, competitive advantage in security can sometimes get in the way). The police can play an important role in facilitating discussions about security, especially when they feed in examples of how risks can be dealt with beneficially. Traditional investigations and prosecutions also have an

[68] See: www.telegraph.co.uk/news/uknews/crime/11767419/Police-chief-warns-that-officers-may-no-longer-respond-to-burglaries.html.

important role to play, not just for reassurance but to do justice and reduce people's willingness and ability to act harmfully. A sharper focus on identifying and helping people who are likely to become repeat victims is also important, both as a good practice in itself and to reduce crime levels. Beyond this, we have to appreciate that, in a world where many offenders are out of reach, we need to maintain our vigilance and educate ourselves about careful behaviour to help prevent victimisation. Some of us will decide that it is not worth the cost and trouble of protecting ourselves more fully, and sometimes those decisions will look poor in retrospect. But unless we adopt a hyper-paternalistic approach and mandate care (as we have done, not very successfully, with the prevention of data breaches), criminal activity will happen. The key is to prepare for it, rather than imagine that it will not happen.

We end by noting that although we have expressed some scepticism about the likelihood of reducing substantially some types of cyber-related economic crime, this report does not take a negative view of current progress and approaches. We welcome the improved relationships between the different police units, business and stakeholders such as the Intellectual Property Office and Trading Standards in the broader 'family of policing', as well as international relationships. However, the strength of these relationships varies and they require constant respectful attention to avoid the impression of condescension. We acknowledge that continuing efforts are being taken to provide a culture of awareness and pre-emptive responses, ranging from practical publications from GCHQ and CPNI at one end of the spectrum, to the emergence of local force Protect officers with a remit for cyber security.

In terms of strategy, however, much more work needs to be done on both the differentiation between the Four Ps and their relative weight. These should be focused on the patterns and impacts of different economic cybercrimes and on the preventative efforts of victims, whether individuals or organisations. This would help shape both the responses – in the case of Pursue, whether disruption is a better approach than full criminal investigation, and whether it makes sense to make more effort to go after the proceeds of cybercrime civilly and criminally – and the wider message on the balance of roles and responsibilities of those involved. We also require more clarity on resourcing, resource ownership and performance assessment.

We need to continue to focus on a full range of efforts to change the security behaviour of individuals and businesses, building in more security with minimum effort to the extent technically and politically possible, and to think clearly about the limits of policing as well as the range of co-ownership of cyber-related crime reduction. This is a permanent struggle that we hope we have made a helpful contribution to thinking through.

Glossary of terms

Black hat	An action with malicious or criminal intent.
Bot	An autonomous program on a network (especially the internet) which can interact with systems or users.
Botnet	A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.
Carder	A person who monetises stolen financial data such as credit card credentials.
Cryptocurrency	A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.
Cryptomarket	A type of website that employs advanced encryption to protect the anonymity of users who trade in goods.
Darknet	A computer network with restricted access that is used chiefly for illegal peer-to-peer file sharing.
Forum	An online discussion site where people can hold conversations.
Hacker	A person who uses computers to gain unauthorised access to data.
Hacktivism	The subversive use of computers and computer networks to promote a political agenda.
Malware	Software which is specifically designed to disrupt or damage a computer system.
Message board	see: Forum
Money mule	A person who transfers stolen money between different countries. Money mules are often recruited by fraudsters to receive money into their bank account, then withdraw the money and wire it overseas, minus a commission payment.
Newsgroup	A forum on the Usenet service for the discussion of a particular topic.
Pirate	To use or reproduce (another's work) for profit without permission, usually in contravention of patent or copyright.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid.
Scareware	A malicious computer program designed to trick a user into buying and downloading unnecessary and potentially dangerous software, such as fake antivirus protection.
Script kiddie	A person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own.
Usenet	An early non-centralised computer network for the discussion of particular topics and the sharing of files via newsgroups.
Warez	Software that has been illegally copied and made available.
White hat	An action in which a breach is made in a computer network to test or evaluate its security systems on the organisation's behalf.
Zombie	A computer that has been compromised with a bot.

References

Ablon, L, Libicki, MC & Golay, AA (2014). 'Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar'. Santa Monica, CA: Rand Corporation.

Accenture (2015). 'Industrial Internet of Things Will Boost Economic Growth, but Greater Government and Business Action Needed to Fulfil its Potential, Finds Accenture'. Source: http://newsroom.accenture.com/news/industrial-internet-of-things-will-boost-economic-growth-but-greater-government-and-business-action-needed-to-fulfill-its-potential-finds-accenture.htm.

Amoroso, E (2012). 'Cyber Attacks: Protecting National Infrastructure.' Amsterdam: Elsevier.

Anderson, R, Barton, C, Böhme, R, Clayton, R, Van Eeten, MJ, Levi, M, Moore, T & Savage, S (2013). 'Measuring the Cost of Cybercrime', pp. 265–300, in R. Böhme (Ed.), 'The Economics of Information Security and Privacy.' Heidelberg: Springer. See also: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

Anderson, R, Böhme, R, Clayton, R & Moore, T (2008). 'Security Economics and the Internal Market.' European Network and Information Security Agency.

Asgher, U, Dar, FM, Hamza, A & Paracha, AM (2014). 'Analysis of Increasing Malwares and Cyber Crimes using Economic Approach.' International Journal of Soft Computing and Software Engineering, 3(3): 487–491.

Ashenden, D & Sasse, A (2013). 'CISOs and Organisational Culture: Their Own Worst Enemy?' Computers & Security, 13: 396–405.

Australian Crime Commission (n.d.). 'Cybercrime', retrieved 20 May 2015. Source: www.crimecommission.gov.au/organised-crime/crime-enablers-and-pathways/cybercrime.

Blakeslee, MR (2012). 'Internet Crimes, Torts and Scams: Investigation and Remedies.' Oxford: Oxford University Press.

Bleaken, D (2010). 'Botwars: the Fight Against Criminal Cyber Networks.' Computer Fraud and Security, 2010(5), 17–19.

Böhme, R, Christin, N, Edleman, B & Moore, T (2015). 'Bitcoin: Economics, Technology, and Governance.' Journal of Economic Perspectives, 29(2): 213–238.

Bossler, AM & Holt, TJ (2009). 'On-line Activities, Guardianship, And Malware Infection: An Examination of Routine Activities Theory.' International Journal of Cyber Criminology, 3(1): 400–420.

Botezatu, B (2011). 'H1 2011 E-Threat Landscape Report.' Bitdefender.

Botezatu, B (2012). 'H2 2012 E-Threat Landscape Report.' Bitdefender.

Bradbury, D (2014). 'Testing the Defences of Bulletproof Hosting Companies.' Network Security, 2014(6): 8–12.

Brenner, SW (2010). 'Cybercrime: Criminal Threats from Cyberspace.' Santa Barbara, California: Praeger.

Brooks, G, Button, M & Frimpong, K (2009). 'Policing Fraud In The Private Sector: A Survey Of The FTSE 100 Companies In The UK.' International Journal of Police Science and Management, 11(4).

Burning Glass (2014). 'Job Market Intelligence: Report on the Growth of CyberSecurity Jobs'. Source: www.burning-glass.com/research/cybersecurity/.

Button, M, Blackbourn, D & Tunley, M (2014). 'The Not So Thin Blue Line After All?' Investigative Resources Dedicated To Fighting Fraud/Economic Crime In The United Kingdom.' Policing, pau037.

Button, M, Lewis, C & Tapley, J (2009). 'Fraud Typologies and the Victims of Fraud: Literature Review.' National Fraud Authority.

Button, M, McNaughton Nicholls, C, Kerr, J & Owen, R (2015). 'Online Fraud Victims In England And Wales: Victims' Views On Sentencing And The Opportunity For Restorative Justice?' Howard Journal of Criminal Justice, 54(2), 193–211.

Cabinet Office (2011). 'The UK Cyber Security Strategy: Protecting And Promoting The UK In A Digital World.' London: Cabinet Office.

Calderoni, F (2010). 'The European Legal Framework On Cybercrime, Crime, Law And Social Change', 54(5): 151–172.

Casper, C (2007). 'Examining the Feasibility of a Data Collection Framework.' Heraklion, Crete: European Network and Information Security Agency.

Cisco. 'Cisco Visual Networking Index Global Traffic Forecast Update, 2014-2019.' Source: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1644203. See also: 'The Internet of Things'. Source: http://www.cisco.com/web/solutions/trends/iot/portfolio.html and http://ioeassessment.cisco.com/learn

City of London Corporation (2015). 'Economic Crime Board of the Police Committee, Agenda: National Lead Force Strategic Documents'. City of London Coporation.

City of London Police (2015). 'National Policing Fraud 'Protect' Strategy: Draft prepared by the National Police Coordinator for Economic Crime' V2.1 February 2015. Source: http://democracy.cityoflondon.gov.uk/documents/s50728/Appendix%202.pdf.

City of London Police (forthcoming). 'National Capability Survey: City of London Force Support Team'.

Coventry, L, Briggs, P, Blythe, J & Tran, M (2014). 'Using Behavioural Insights To Improve The Public's Use Of Cyber Security Best Practices'. London: Office for Government Science. Source: www.gov.uk/go-science.

Cross, C & Blackshaw, D (2014). 'Improving The Police Response To Online Fraud'. Policing, December: 1–10.

Cross, C, Smith, RG & Richards, K (2014). 'Challenges Of Responding To Online Fraud Victimisation In Australia. Trends And Issues In Crime And Criminal Justice'. Canberra: Australian Institute of Criminology.

Denning, DE & Baugh, WE (1997). 'Encryption And Evolving Technologies: Tools Of Organized Crime And Terrorism'. Trends in Organized Crime, 3(1): 84–91.

Detica & Office of Cyber Security and Information Assurance (2011). 'The Cost of Cyber Crime'. London: Cabinet Office.

Dingledine, R & Mathewson, N (2006). 'Anonymity Loves Company: Usability and the Network Effect'. Paper presented at the 5th Workshop on the Economics of Information Security, Cambridge, UK.

Dittrich, D (2012).'So You Want To Take Over A Botnet'. Paper presented at the 5th USENIX conference on Large-scale Exploits and Emergent Threats, San Jose, California.

Doig, A, Johnson, S & Levi, M (2001). 'New Public Management, Old Populism And The Policing Of Fraud'. Public Policy and Administration, 16(1), 91–113.

Doig, A & Levi, M (2013). 'A Case Of Arrested Development? Delivering The UK National Fraud Strategy Within Competing Policing Policy Priorities'. Public Money and Management, 33(2), 145–152.

Doig, A & Macaulay, M (2008). 'Decades, Directions And The Fraud Review: Addressing The Future Of Public Sector Fraud'. Public Money and Management, 28(3): 185–192.

Empirica (2007). 'Benchmarking in a Policy Perspective: Security and Confidence'. Brussels: Empirica.

Europol (2014). 'The Internet Organised Crime Threat Assessment'. The Hague: Europol.

Europol (2015). 'The Internet Organised Crime Threat Assessment (IOCTA) 2015'. The Hague: Europol.

Felson, M and Clarke, RV (1998). 'Opportunity Makes the Thief: Practical Theory for Crime Prevention. Police Research Series Paper 98'. London: Policing and Reducing Crime Unit, Home Office.

Florêncio, D & Herley, C (2010). 'Phishing and Money Mules'. Paper presented at the 2010 IEEE International Workshop on Information Forensics and Security (WIFS), Seattle.

Finklea, K (2014). 'Identity Theft: Trends and Issues'. Washington DC: Congressional Research Service. Source: www.fas.org/sgp/crs/misc/R40599.pdf.

Gannon, R & Doig, A (2010). 'Ducking The Answer? Fraud Strategies And Police Resources'. Policing & Society, 20(1), 39–60.

Garvey, PR & Patel, SH (2014). 'Analytical Frameworks to Assess the Effectiveness and Economic-Returns of Cybersecurity Investments'. Paper presented at the 2014 IEEE Military Communications Conference (MILCOM), Baltimore, MD.

GCHQ (CESG)/CERT-UK (2015). 'Common Cyber Attacks: Reducing the Impact'. Cheltenham: GCHQ.

Ghosh, S & Turrini, E (2010). 'Cybercrimes: A Multidisciplinary Analysis'. Heidelberg: Springer Science and Business Media.

Gragido, W, Molina, D, Pirc, J & Selby, N (2012). 'Blackhatonomics: An Inside Look at the Economics of Cybercrime'. Amsterdam: Syngress.

Heinonen, JA, Holt, TJ & Wilson, JM (2012). 'Product Counterfeits In The Online Environment: An Empirical Assessment Of Victimization And Reporting Characteristics'. International Criminal Justice Review, 22(4): 353–371.

HM Government (2015). '2015 Information Security Breaches Survey'. London: PwC and Infosecurity.

HMIC (2014). 'The Strategic Policing Requirement: An Inspection of How Police Forces in England and Wales Deal with Threats of a Large-scale Cyber Incident (Including Criminal Attack)'. London: HM Inspectorate of Constabulary.

HM Treasury (2015). 'Digital Currencies: Response to the Call for Information.' London: HM Treasury.

Home Affairs Select Committee (2013). 'E-Crime. Fifth Report'. HC 70. London: TSO.

Home Office (2014). 'The Serious and Organised Crime Strategy'. London: Home Office.

Home Office (2015a). 'The Serious and Organised Crime Strategy – Annual Report for 2014'. London: Home Office.

Home Office (2015b). 'Crime Against Businesses: Findings from the 2014 Commercial Victimisation Survey'. London: Home Office.

Hutchings, A (2013). 'Hacking And Fraud: A Qualitative Analysis Of Online Offending And Victimisation', pp. 93–114 in K Jaishankar & N Ronel (Eds), 'Global Criminology: Crime and Victimization in a Globalized Era'. Boca Raton: CRC Press.

Innes, M (2014). 'Strategic Police-Community Engagement: A Report to the Scottish Police Authority'. Source: http://www.spa.police.uk/assets/128635/consultationandengagemen

Innes, M and Sheptycki, JWE (2004). 'From Detection To Disruption: Intelligence And The Changing Logic Of Police Crime Control In The United Kingdom'. International Criminal Justice Review, 14(1): 1–24.

IPO (2014). 'IP Crime Annual Report 2013/14'. Newport: Intellectual Property Office.

Jaishankar, K (2011). 'Cyber Criminology: Exploring Internet Crimes and Criminal Behavior'. Boca Raton: CRC Press.

Jeffray, C (2014). 'The Threat of Cyber-Crime to the UK: RUSI Threat Assessment'. London: Royal United Services Institute.

Johnson, ME (2009). 'Managing Information Risk and the Economics of Security'. New York: Springer.

Kikuchi, H, Matsuo, S & Terada, M (2011). 'Principal Component Analysis Of Botnet Takeover'. Information and Media Technologies, 6(4): 1241–1250.

King, J & Doig, A (forthcoming). 'A Place For Volume Fraud Within The Current Economic Crime Agenda? The Greater Manchester Police Case Study'.

Kshetri, N (2010). 'The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives'. New York: Springer Science and Business Media.

Large, J (2014). 'Get Real, Don't Buy Fakes': Fashion Fakes And Flawed Policy – The Problem With Taking A Consumer-Responsibility Approach To Reducing The 'Problem' of Counterfeiting'. Criminology and Criminal Justice, 1748895814538039.

Lauritsen, JL, Sampson, RJ & Laub, JH (1991). 'The Link Between Offending And Victimization Among Adolescents'. Criminology, 29(2): 265–292.

Lavorgna, A (2013). 'Transit Crimes in the Internet Age (PhD)'. University of Trento.

Lavorgna, A (2014a). 'The Online Trade In Counterfeit Pharmaceuticals: New Criminal Opportunities, Trends And Challenges'. European Journal of Criminology 9(2): 325–354.

Lavorgna, A (2014b). 'Wildlife Trafficking In The Internet Age'. Crime Science, 3(1): 1–12.

Levi, M (1992). 'White-Collar Crime Victimization', pp. 169–192 in K Schlegel & D Weisburd (Eds), 'White-Collar Crime Reconsidered'. Boston: Northeastern University Press.

Levi, M (2008). 'The Phantom Capitalists: The Organization and Control of Long-firm Fraud'. Aldershot, UK: Ashgate.

Levi, M (2013). 'Regulating Fraud: White-Collar Crime and the Criminal Process'. London: Routledge.

Levi, M, Bissell, P & Richardson, T (1991). 'The Prevention of Cheque and Credit Card Fraud'. Crime Prevention Unit Paper 26. London: Home Office.

Levi, M, Burrows, J, Fleming, M & Hopkins, M with the assistance of Matthews, K (2007). 'The Nature, Extent and Economic Impact of Fraud in the UK'. London: Association of Chief Police Officers. Source: www.acpo.police.uk/asp/policies/Data/Fraud%20in%20the%20UK.pdf.

Levi, M & Maguire, M (2012). 'Something Old, Something New; Something Not Entirely Blue: Uneven And Shifting Modes Of Crime Control', pp. 195–218 in T Newburn and J Peay (Eds), 'Policing: Politics, Culture and Control', Oxford: Hart Publishing.

Levi, M, Morgan, J & Burrows, J (2003). 'Enhancing Business Crime Reduction: UK Directors' Responsibilities To Review The Impact Of Crime On Business' Security Journal, 16(4): 7–27.

Levi, M & Pithouse, A (1992). 'The Victims Of Fraud', in D Downes (Ed.), 'Unravelling Criminal Justice'. London: Macmillan.

Li, M (2009). 'The Pirate Party and the Pirate Bay: how the Pirate Bay influences Sweden and international copyright relations'. Pace International Law Revue, 21: 281.

London Chamber of Commerce & Industry (2014). 'Cyber-secure: Making London Business Safe Against Online Crime'. Source: http://www.londonchamber.co.uk/DocImages/12773.pdf

Lusthaus, J (2012). 'Trust In The World Of Cybercrime'. Global Crime, 13(2): 71–94.

Lusthaus, J (2013). 'How Organised Is Organised Cybercrime?' Global Crime, 14(1): 52–60.

Manyika, J & Roxburgh, C (2011). 'The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity'. McKinsey Global Institute.

McGuire, M & Dowling, S (2013). 'Cyber Crime: A Review of the Evidence. Summary of Key Findings and Implications'. Home Office Research Report 75. London: Home Office.

McMullan, JL & Rege, A (2010). 'Online crime And Internet Gambling'. Journal of Gambling Issues, 24: 54–85.

Mickelberg, K, Schive, L & Pollard, N (2014).' US Cybercrime: Rising Risks, Reduced Readiness'. London: PricewaterhouseCoopers LLP.

Millie, A (2014) 'Reassurance Policing and Signal Crimes', pp. 4327–4335 in G Bruinsma and D Weisburd (Eds), 'Encyclopedia of Criminology and Criminal Justice'. New York: Springer.

Modic, D & Anderson, R (2014). 'Reading This May Harm Your Computer: The Psychology Of Malware Warnings'. Computers in Human Behavior, 41: 71–79.

Montoya, AL, Junger, M & Hartel, PH (2013). 'How "Digital" is Traditional Crime?', pp. 31–37 in European Intelligence and Security Informatics Conference. New York: IEEE.

MOPAC (2014). 'Business Crime Strategy, 2014–16'. London: MOPAC.

NERA (National Economic Research Associates) (2000). 'The Economic Cost of Fraud'. London: NERA Associates.

Oakford, S (2015). 'Prosecutors in Silk Road trial present damning evidence from Ross Ulbricht's computer'. Source: https://news.vice.com/article/prosecutors-in-silk-road-trial-present-damning-evidence-from-ross-ulbrichts-computer.

ONS (2013). 'Chapter 4: Mass Marketing Fraud'. Source: www.ons.gov.uk/ons/dcp171776_309772.pdf.

ONS (2015). 'Crime in England and Wales, Year Ending December 2014'. Newport: Office for National Statistics.

Pratt, TC, Holtfreter, K & Reisig, MD (2010). 'Routine Online Activity And Internet Fraud Targeting: Extending The Generality Of Routine Activity Theory'. Journal of Research in Crime and Delinquency, 47(3): 267–296.

Pyrooz, DC, Decker, SH & Moule Jr, RK (2013). 'Criminal And Routine Activities In Online Settings: Gangs, Offenders, And The Internet'. Justice Quarterly, 32(3): 1–29.

Scottish Government (2015). 'Consultation on Proposal for a Cyber Resilience Strategy for Scotland'. Edinburgh: Scottish Government.

Singer, SI (1986). 'Victims Of Serious Violence And Their Criminal Behavior: Subcultural Theory And Beyond'. Violence and Victims, 1(1): 61–70.

Ståhlberg, M (2008). 'The Trojan Money Spinner'. Paper presented at the Virus Bulletin Conference, Vienna.

van Kranenburg, R, Anzelmo, E, Bassi, A, Caprio, D, Dodson, S & Ratto, M (2011). 'The Internet of Things'. Paper presented at the 1st Berlin Symposium on Internet and Society, Berlin.

Wall, DS (2007a). 'Cybercrime: The Transformation of Crime in the Information Age'. Cambridge: Polity.

Wall, DS (2007b). 'Policing Cybercrimes: Situating The Public Police In Networks Of Security Within Cyberspace'. Police Practice and Research, 8(2): 183–205.

Wall, DS & Large, J (2010). 'Jailhouse Frocks: Locating The Public Interest In Policing Counterfeit Luxury Fashion Goods'. British Journal of Criminology, 50(6): 1094–1116.

Weaver, N (2015). 'How I traced 20% of Ross Ulbricht's Bitcoin to the Silk Road'. Source: www.forbes.com/sites/frontline/2015/01/20/bitcoin-silk-road-ulbricht/

Whitty, M (2013). 'Mass Marketing Fraud in the UK: 2013 Report'.

Whitty, M & Buchanan, T (2012). 'The Online Romance Scam: A Serious Cybercrime'. CyberPsychology, Behavior, and Social Networking, 15(3): 181–183.

Wolfgang, ME, Ferracuti, F & Mannheim, H (1967). 'The Subculture of Violence: Towards an Integrated Theory in Criminology'. London: Tavistock Publications.

The Implications of Economic Cybercrime for Policing

RESEARCH REPORT CITY OF LONDON CORPORATION **OCTOBER 2015**

www.cityoflondon.gov.uk/**economicresearch**

CITY OF LONDON

CITY OF LONDON POLICE

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD