doi:10.1093/bjc/azv011 BRIT. J. CRIMINOL. (2016) **56**, 21–48
Advance Access publication 27 April 2015

# GUARDIANS UPON HIGH: AN APPLICATION OF ROUTINE ACTIVITIES THEORY TO ONLINE IDENTITY THEFT IN EUROPE AT THE COUNTRY AND INDIVIDUAL LEVEL

Matthew L. Williams*

*Online fraud is the most prevalent acquisitive crime in Europe. This study applies routine activities theory to a subset of online fraud, online identity theft, by exploring country-level mechanisms, in addition to individual determinants via a multi-level analysis of Eurobarometer survey data. This paper adds to the theory of cybercrime and policy debates by: (1) showing that country physical guardianship (e.g. cyber security strategy) moderates the effects of individual physical guardianship; (2) introducing a typology of online capable guardianship: passive physical, active personal and avoidance personal guardianship; (3) showing that online identity theft is associated with personal and physical guardianship; and (4) identifying public Internet access and online auction selling as highly risky routine activities. The paper concludes by emphasizing the importance of studying country-level effects on online identity theft victimization.*

Keywords: online identity theft, online fraud, cybercrime, cyber security, routine activities theory, Eurobarometer

## *Introduction*

In January of 2014, the German cybercrime watchdog the Federal Office for Information Security discovered the theft of 16 million email addresses and passwords (ENISA 2014). In the same year, three major global cyberhacks, including the largest ever recorded, resulted in the theft of over two billion credit card and customer records from large US retailers[1] (Banjo 2014; Finkle and Hosenball 2014; Perlroth and Gelles 2014). These recent mass criminal events and the burgeoning 'darknet'[2] evidence that networks of hijacked computers and malware represent the most significant threats in relation to contemporary identity theft (Ablon *et al.* 2014). Indeed, most statistical sources indicate cybercrime is on the rise, while terrestrial forms of crime are generally in decline (Williams and Levi 2012; Levi and Williams 2013). A recent Office for National Statistics discussion paper suggests the 55 per cent crime drop between 1995 and 2013 may be accounted for by the displacement of crime offline to online. Examining the financial losses from online identity fraud alone, the paper states '…it is clear that this [online identity fraud] would represent a huge increase in the crime statistics if they were included' (ONS 2014: 5). Indeed, the Eurostat 2010 ICT survey shows that online fraud has become the most prevalent acquisitive crime in Europe, above car theft and burglary (Anderson *et al.* 2012).

*Matthew L. Williams, School of Social Sciences, Cardiff University, King Edward VII Ave., Cardiff CF10 3WT, UK; WilliamsM7@cf.ac.uk.

[1] The Home Depot and Target superstores were the main targets.

[2] The darknet is a restricted computer network used chiefly for the illegal sharing of stolen data: a cyber black market.

In an attempt to explain this seemingly unrelenting rise in cybercrimes, authors have compared cyberspace to a frontier town, characterized by an abundance of opportunity (both criminal and legitimate) and self-regulation, where citizens take the main responsibility for their safety in the absence of *effective* state intervention (Williams 2000; 2004; 2006; Wall and Williams 2007; Williams 2007; Wall and Williams 2013; Wall and Williams 2014). The effectiveness of online self-regulation has been explored via routine activities theory (RAT; Cohen and Felson 1979). Several empirical applications point to the significant effects that frequent and varied routine online activity and the lack of capable guardians have on cyber victimization (Choi 2008; Holt and Bossler 2008; van Wilsem 2011; Bossler *et al.* 2012; van Wilsem 2013a). However, none of this online work to date has examined the effectiveness of state intervention, or 'contextual' guardianship that has been shown to be important in having causal effects that are irreducible to individual phenomena in offline applications of RAT (see Miethe and McDowall 1993; Wilcox *et al.* 2007). This omission is problematic not only theoretically, but also because of the wide-spread *non-evidenced based* policy assumption that national cyber-security strategies, that have seen recent growth, result in the reduction of cybercrime at the individual level (OECD 2011; BIS 2012; ENISA 2012*a*; 2012*b*; Home Office 2013; United Nations 2013; Cabinet Office 2014; World Bank 2014).

For the first time, this paper empirically tests these theoretical and policy suppositions at both the national and individual level across 27 European countries using the example of online identity theft. Results of a series of multi-level regression models using Eurobarometer survey data predict online identity theft based on routine online activities and personal and physical guardianship while investigating the effects of country-level characteristics (e.g. national cyber security strategies) on individual outcomes. This paper adds to the growing body of work on the theory of cybercrime and policy debates by (1) showing for the first time that the presence of country-level physical guardianship (national cyber security strategies and Internet infrastructure) significantly moderates the effects of individual level physical guardianship (e.g. installing anti-virus) on online identity theft; (2) introducing a novel typology of online capable guardianship: passive physical guardianship, active personal guardianship and avoidance personal guardianship; (3) showing that individual-level differences in online identity theft are significantly associated with personal and physical guardianship; and (4) identifying public Internet access and online auction selling as highly risky routine activities. The paper concludes by emphasizing the importance of studying country-level effects on online identity theft victimization.

### *The Manifestation and Impacts of Online Identity Theft*

Online identity theft is a subset of more general online fraud and describes crimes that involve the duplication of digital information or the high-jacking of online accounts for the purposes of committing identity fraud against individuals or businesses (for a comprehensive overview, see Wall 2013). Phishing is the most common technique used in the commission of online identity theft. Social engineering techniques are most often used where perpetrators pose as legitimate companies requesting personal details. More sophisticated attacks, such as Spear Phishing, Pharming and Smishing, target profiled groups based on desires for goods and services, improving their success;

bypass social engineering, instead targeting software resulting in the automatic redirection to illegitimate imitation websites; and use SMS text messages to target mobile Internet users. Online banking credentials can also be obtained by malware that is installed on computers without users' knowledge, typically by clicking on a link connected to infected software in an unsolicited email. Malware has been designed to log users' keystrokes, insert fake web pages (browser in the middle attack) and perform unauthorized actions on computers, in an attempt to capture passwords and financial information. The financial malware Zeus, SkyEye and Citadel67 continue to be responsible for the theft of personal banking information (ENISA 2013). More recently social media has seen a rise in phishing attacks. These networks expose a pool of 2.5 billion non-unique suitable targets to motivated identity theft perpetrators (Burnap *et al.* 2013; Sloan *et al.* 2013; Williams *et al.* 2013; Burnap *et al.* 2014).

Research suggests consumers in the United Kingdom are more at risk of falling victim to online identity theft than consumers in any other country in Europe (Fellowes 2012). The National Fraud Authority (NFA) estimates that identity theft costs the UK taxpayer up to £1.2 billion per year (NFA 2012). The UK annual number of phishing incidents in 2012 was just over 250,000, a 130 per cent increase compared to 2011 (Financial Fraud Action UK 2013). Globally, phishing attacks rose by 87 per cent (37 million attacks) between 2012 and 2013. In relation to routine online activities, phishing attempts have been targeted at email and search (e.g. Google) (30 per cent), social media (e.g. Facebook) (20 per cent), banks (12 per cent) and payment services (6 per cent) (ENISA 2013). The extent and impact of online identity theft indicates that it constitutes a significant proportion of all online fraud (Wall 2013), hence the focus of this paper.

### *RAT and Online Identity Theft*

Cohen and Felson (1979) suggested there is an increased likelihood of victimization when individuals are placed in high risk situations, are attractive targets, lack a capable guardian and are in the reach of a motivated offender. RAT takes as its focus the criminal event rather than the criminal. This is particularly salient to the study of cybercrime as we rarely have access to cyber criminals to study their motivations (due to low levels of apprehension) and cybercriminal events are in abundance and leave behind digital signatures for analysis. Newman and Clarke (2003) were amongst the first to advance the applicability of RAT to cybercrime and argued that Internet target accessibility (increased by the absence of capable guardianship) and visibility (increased by the variety and frequency of online routine activities, e.g. shopping and banking) are discriminating characteristics between victims and non-victims of cybercrime. Yar (2005) found that with respect to the central core concepts of RAT, 'motivated offenders' and 'capable guardianship' could be treated as largely similar between cyber and terrestrial settings. However, the application of 'suitable targets' was problematic given the theory holds that the 'organization of time and space is central for criminological explanation' (Felson 1998: 148); yet cyberspace is spatio-temporally *disorganized* (i.e. the victim and offender are rarely co-present). Eck and Clarke (2003) address this issue suggesting RAT can be expanded to explain crimes where the perpetrator and victim do not occupy the same physical space. By modifying the theory's shared physical space requirement to include a ‘shared network’, such as the Internet, then it remains that the perpetrator can reach a target through this network.

RAT has been empirically applied to various cybercrimes with mixed results. Proximity to motivated offenders and more varied and intense online routine activity were found to be associated with cyber-harassment, while physical guardianship (such as installing anti-virus software, akin to installing household security devices) was not (Holt and Bossler 2008; van Wilsem 2011; Bossler *et al.* 2012; van Wilsem 2013a). The application of RAT to computer virus infection also generated mixed results. Choi (2008) showed that online lifestyle and physical guardianship were both related to victimization, while Bossler and Holt (2009) showed that both personal (changing passwords on a regular basis) and physical guardianship were unrelated. The authors highlight significant limitations with their samples derived from college student populations that may account for these contradictory findings.[3]

The application of RAT to online identity theft has generated more favourable results. From a small sample of US adults, Pratt *et al.* (2010) found that two online routines, spending time online and purchasing from online retailers, were significantly related to the crime and more important than the consumer attributes of age and education in predicting victimization. A study of Internet consumer fraud, where items bought were not received, showed that Internet purchasing and visiting online forums increased the likelihood of victimization (van Wilsem 2013b). Reyns’ (2013) study of identity theft drawing on the British Crime Survey (08 & 09) showed that several routine activities were related to an increased chance of victimization. Four measures of online routine activity, using the Internet for banking, shopping, emailing and downloading, were significantly associated with identity theft. Males, older respondents and high earners were also more at risk from victimization, although these relationships were mediated by the introduction of the theoretical measures, showing the importance of routine activities in explaining identity theft victimization. However, Reyns’ study was limited by its lack of focus on the *online* manifestation of identity theft given the non-specific BCS survey question wording. Therefore, the present study represents the first to focus exclusively upon *online* identity theft and to test the effect of guardianship on victimization at the individual and country level.

Crime prevention initiatives in Europe have focused on raising the awareness of citizens to the risks of cybercrime (ENISA 2012*a*; 2012*b*). These national policy directives encourage a form of personal guardianship that increases individual cognizance of the risks and consequences of cybercrime (Reyns 2013). In addition to diverting from risky routine online activities, this form of personal guardianship also encourages physical guardianship via the adoption of security behaviours that lessen or mitigate the risks via target hardening techniques. Most recently, the UK Government’s National Cyber Security Tracker showed that only 44 per cent of the public installed security software, only 37 per cent updated software patches, less than 30 per cent habitually used passwords and 57 per cent did not check website security before purchasing goods online (Home Office 2013). Preventative campaigns for both businesses and individuals aimed at increasing physical guardianship have been launched throughout Europe

[3] Many studies that apply RAT to cybercrime rely on college student populations that are limited by their non-random sampling strategies that result in inevitable biases.

(ENISA 2012*a*; 2012*b*). The most recent UK campaign ‘Cyber Street Wise’ funded by the National Cyber Security Programme aims to increase the number of individuals and organizations: (1) installing anti-virus and secure browsing; and (2) changing passwords regularly, while (3) discouraging digital disengagement due to anxiety about cybercrime (e.g. doing less online, such as banking and shopping). These security behaviours can be considered forms of individual capable guardianship: (1) *passive physical guardianship*; (2) *active personal guardianship* and (3) *avoidance personal guardianship*. These forms of guardianship are considered amongst professionals and researchers to be the weakest points in the cyber security chain and it is argued if adopted they could reduce cyber victimization to a significant extent (Gupta and Sharman 2011). However, there currently exists no empirical evidence to show that presence of capable guardians actually reduces online identity theft victimization. This paper empirically tests the assumptions of RAT and crime prevention policy, that guardianship at the country and individual level reduces cyber-victimization, providing evidence for the first time on a multi-national European wide scale.

### *Country-Level Factors in Cybercrime*

For the first time, the present study incorporates both country- and individual-level factors to predict online identity theft victimization. Routine activities factors explaining criminal victimization measured at the aggregate area level are well established (Miethe and McDowall 1993; Wilcox *et al.* 2007). In these studies, the focus is on the distinct effects of both aggregate and individual-level factors as well as on the conditionality of individual relationships—i.e. the extent to which the latter vary from one aggregate context to another. In their study of burglary, Wilcox *et al.* (2007) found that contextual guardianship mediated the effect of individual guardianship (such as target hardening), with individual guardianship reducing victimization in high guardianship neighbourhoods to a greater extent as compared to low guardianship neighbourhoods. Miethe and McDowall (1993) found that interactions between criminal opportunities at the individual and city-block level were important in explaining violent victimization. Both of these patterns, contextual guardianship and interactions between context and individual are examined in this study of online identity theft.

Country geography has been taken as the aggregate level in this present study as cyber victimization is likely to have a limited lower level dependency above the individual, particularly because perpetrators are often geographically distant from the victim (Williams 2006). Indeed, in the majority of cases of cyber victimization, the parties are in different countries (Kim *et al.* 2012). The International Crime Victimisation Survey (ICVS) has consistently found that offline criminal victimization varies significantly between countries and is related to urbanicity, economic inequality and age composition measured at the country level (van Kesteren *et al.* 2014). In particular, Eastern European countries repeatedly show higher rates of violent and acquisitive crimes (van Wilsem *et al.* 2003). As an indicator of variation in cyber *victimization* between higher level geographies, and in line with the point made above with regards to the distance between victim and perpetrator in cybercrimes, the work of Kim *et al.* (2012) shows how systems hacking *perpetration* patterns vary by country. When controlling for the country level factor of economic performance, they find significant differences in prevalence of hacking attempts by country and show the highest number of acts of perpetration emanate from Latvia, Slovenia and Estonia within the EU. The same study also found the countries that had not adopted the Council of Europe (CoE) Convention on Cybercrime and that had less developed Internet infrastructure (measured in terms of Internet penetration) harboured a disproportionate number of hacking perpetrators. The country-level factors found to be significant in Kim *et al.*'s study (economic, Internet penetration, cyber security strategy) and in the ICVS (urbanicity) are incorporated into the hypotheses in this study.

### *Hypotheses*

*Hypothesis 1 [H1]*: Individual level differences in online identity theft are positively associated with online routine activities.

*Hypothesis 2 [H2]*: Individual level differences in online identity theft are negatively associated with Active Personal, Avoidance Personal and Passive Physical Guardianship.

These first two hypotheses test the application of RAT to online identity theft at the individual level. The second expands upon the work of van Wilsem (2013b) and Reyns (2013) by incorporating physical guardianship measures. Both also test the policy assumption that the adoption of active personal and passive physical guardianship reduces cyber victimization (ENISA 2012*a*; 2012*b*; Home Office 2013).

*Hypothesis 3 [H3]*: Individual level differences in online identity theft are negatively associated with the country level capable guardianship measure of national cyber security strategy, and are associated (either positively or negatively) with Internet penetration, economic performance, and level of urbanicity.

The third hypothesis tests the effect of capable guardianship at the country level, identifying if patterns found in *offline* multi-level studies of contextual guardianship are replicated *online* (Wilcox *et al.* 2007), and tests if the patterns found in online hacking *perpetration* are replicated in relation to online identity theft *victimization* (Kim *et al.* 2012). In doing so, it also tests the policy assumption that national cyber security strategies are effective at reducing individual victimization (ENISA 2012*a*; 2012*b*; United Nations 2013). As no research has shown Internet penetration has an impact upon cyber victimization, no assumption is made as to the direction of the potential effect, and it is recognized that number of users (quantity) may or may not translate to better country security (quality) (I return to this in the Discussion). The hypothesis also extends the work on country-level offline victimization rates that are shown to vary by urbanicity (van Kesteren *et al.* 2014) and economic performance (Wilsem *et al.* 2003), by testing if these also associated with cyber-victimization.

*Hypothesis 4 [H4]*: The effect of individual level predictors on online identity theft varies as a function of country adoption of cyber security strategy, Internet penetration, economic performance, and level of urbanicity.

This final hypothesis tests the *interaction* between country and individual-level guardianship to identify if moderating effects found in offline studies of RAT are also present for online identity theft (Miethe and McDowall 1993).

## *Data and Methods*

### *Data*

This paper analyses data from the Special Eurobarometer 390 survey on cyber security, collected in 2012 as part of the Standard Eurobarometer run bi-annually by the European Commission. This Special Eurobarometer represents the largest and most comprehensive cyber security survey globally, that is statistically representative of the domestic population in Europe (see Levi and Williams 2012 for a review of the quality of existing cybercrime datasets). The survey ($N = 26{,}593$) is representative of 1,270 regions in 27 countries. Country-level multistage random probability sampling was adopted, with sampling points drawn with probability proportional to population size (for a total coverage of the country) and to population density. Several questions from the survey, all of which were subject to robust cognitive testing to ensure measurement validity,[4] were used in this study.

### *Dependent measure of online identity theft and method of estimation*

The survey question selected as the dependent variable was specially tailored to capture only *online forms* of identity theft and was worded as follows: "*Cybercrimes can include many different types of criminal activity. How often have you experienced or been a victim of the following situations?*" Response item 1: "*Identity Theft (somebody stealing your personal data and impersonating you, e.g. shopping under your name)*". This question is consistent with Article 8 of the Council of Europe Convention on Cybercrime 2001 and hence compatible with the laws of all signatories to the convention and international law enforcement (Interpol and Europol). The author is confident that this question is one of the first robust measures of *online* identity theft to be included in a cross-national survey based on a representative random probability sample design. Reyns' (2013) analysis of identity theft using the British Crime Survey is the only other example of a study using a representative sample, and this was limited by its lack of focus on the *online* manifestation of the crime given the non-specific survey question wording. A scale response was used to elicit experiences of online identity theft: 0 = never; 1 = occasionally; 2 = often. Exploration of this variable evidenced an extreme positive skew with the majority not experiencing victimization, and a minority experiencing one or more instances of victimization. As this distribution violates an assumption of linear regression, a multi-level Poisson model was used to fit to the data using Stata 12 (see Analytic Strategy and Appendix). There exists a growing methodological and empirical criminological literature on Poisson regression models (see Osgood 2000). These models account for events that are largely not experienced by the majority of the sample.[5]

[4] European Commission-sponsored reviews of the validity of cyber crime and security survey measures were undertaken in 2006 (business surveys) and 2007 (domestic surveys) (i2010 High Level Group 2006; Empirica 2007).

[5] Linear regression models are not appropriate for such distributions, given the non-linear distribution of the dependent. A multi-nominal model was ruled out as it would fail to account for the order of the categories of the outcome variable which are important here for accounting for repeat victimization. The desire to take into account repeat victimization at the upper end also ruled out collapsing the dependent into a binary outcome required for logistic regression. Ordinal regression was ruled out as the distances between response items were not 'equal'. Furthermore, there were concerns over the violation of the assumption of independence of irrelevant alternatives (IIA). Poisson-related models are suited to these data as they are built on assumptions about error distributions that are consistent with the nature of event occurrences.

### *Independent variables*

#### *Individual-level covariates*

Table 1 provides item coding details and descriptive statistics for the covariates entered into the models.

*Online routine activities.* Reyns (2013) shows how multiple measures of online routine activities, capturing a variety of potentially risky situations, are an improvement upon single measures of Internet activity, such as time spent online. Twelve routine activities were included as potential correlates of online identity theft: *Internet activities* (banking, purchasing, auction selling, social networking and emailing) each entered as binary covariates, measure variety of online activity; *location of Internet access* (home, university, public, café, mobile and work) each entered as binary covariates, measure location of access, where some locations are riskier than others (e.g. computers in cafés and public settings have multiple users increasing the possibility of virus infection) and *frequency of Internet use*, entered as a scale covariate. These are direct measures of routine online activities that, if left unguarded, have the potential to expose suitable online targets to motivated online identity theft offenders.

*Capable guardianship.* Guardianship was assessed via a range of direct and indirect measures, in keeping with traditional RAT research (see Miethe and McDowall 1993; Wilcox *et al.* 2007). Eight direct measures of individual-level Internet security behaviours were identified in the survey. These items were combined using the principal components analysis data reduction technique to produce three underlying components: (1) *passive physical guardianship* (using only one computer, email spam filtering, installing anti-virus and secure browsing); (2) *active personal guardianship* (changing security settings and passwords) and (3) *avoidance personal guardianship* (doing less online, such as banking and purchasing goods) (see Table 2 for component loadings). A non-linear relationship between avoidance personal guardianship and the dependent was identified by incorporating a polynomial into the regression model. A worry of online identity theft victimization item from the survey was included as proxy of personal guardianship, based on evidence that suggests fear of crime influences perceptions of risk that constrain behaviour and redirect from risky routine activities online (Reisig *et al.* 2009).

*Individual characteristics.* Based on research that shows time spent engaged in online routine activities is a function of age and gender (Pratt *et al.* 2010) several individual characteristics items from in the Standard Eurobarometer survey were entered as covariates. Six covariates were included: age, sex, education, social status, deprivation and urban, rural and suburban.

#### *Country-level covariates*

*Country capable guardianship.* The maturity of national cyber security strategies was taken as a direct measure of country level capable guardianship and was derived by summing the months since their institution in each of the respective EU countries in the sample based on ENISA data.[6] ENISA (2012*a*) identified that 18 out of 27 EU states (67 per cent) had implemented a strategy[7] compared to around 30 per cent of countries globally. These

[6] See http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

[7] Austria, Belgium, Czech Republic, Estonia, Finland, France, Italy, Germany, Hungary, Latvia, Lithuania, Luxembourg, The Netherlands, Poland, Romania, Slovak Republic, Spain and The United Kingdom.

Table 1 *Descriptive statistics (N = 18,214)*

| | Coding | Sample | |
|---|---|---|---|
| | | *M* | SD |
| Dependent variable | | | |
| Experience of online identity theft | 0 = never, 1 = occasionally, 2 = often | 0.08 | 0.31 |
| Independent variables | | | |
| Individual level | | | |
| Online routine activities | | | |
| Internet location: home | 1 = yes | 0.79 | 0.41 |
| Internet location: university | 1 = yes | 0.01 | 0.11 |
| Internet location: public | 1 = yes | 0.01 | 0.09 |
| Internet location: cafe | 1 = yes | 0.01 | 0.07 |
| Internet location: mobile | 1 = yes | 0.01 | 0.08 |
| Internet location: work | 1 = yes | 0.16 | 0.37 |
| Internet use: banking | 1 = yes | 0.54 | 0.50 |
| Internet use: purchasing | 1 = yes | 0.50 | 0.50 |
| Internet use: selling | 1 = yes | 0.18 | 0.38 |
| Internet use: social networking | 1 = yes | 0.53 | 0.50 |
| Internet use: email | 1 = yes | 0.85 | 0.36 |
| Frequency of Internet use | Scale (range: 1–15) | 7.32 | 3.37 |
| Capable guardianship | | | |
| Active PG | Scale (range: −1.91 to 3.25) | −0.00 | 1.00 |
| Avoidance PG | Scale (range: −0.86 to 3.17) | −0.00 | 1.00 |
| Passive PG | Scale (range: −1.25 to 2.48) | −0.00 | 1.00 |
| Worry about online identity theft | Scale (range: −3.47 to 3.27) | −0.00 | 1.00 |
| Individual: characteristics | | | |
| Male | 1 = yes | 0.47 | 0.50 |
| Age | Scale (range: 15–97) | 42.50 | 15.97 |
| Education | Scale (range: 1 = no education, 2 = left at 15, 3 = left 16–19, 4 = left 20+) | 3.34 | 0.63 |
| Social status | Scale (range: 1–10) | 5.75 | 1.55 |
| Deprivation (difficulties paying bills) | Scale (range: 1 = almost never, 2 = from time to time, 3 = most of the time | 1.47 | 0.67 |
| Suburban | 1 = yes | 0.38 | 0.48 |
| Urban | 1 = yes | 0.30 | 0.46 |
| Rural | 1 = yes | 0.32 | 0.47 |
| Country level | | | |
| Capable guardianship | | | |
| National cyber security strategy | Scale (range: 0–68 months) | 17.66 | 18.92 |
| Internet penetration | Scale (range: 0–100%) | 74.80 | 12.81 |
| Economy and urbanicity | | | |
| GDP (PPP) | Scale (range: €12,100–€67,100) | 25760.21 | 9180.60 |
| % population living in urban areas | Scale (range: 49.9–97.5) | 73.93 | 12.44 |

Active PG = Active Personal Guardianship; Avoidance PG = Avoidance Personal Guardianship; Passive PG = Passive Physical Guardianship.

strategies primarily cover cybercrime prevention via awareness raising, law enforcement and criminal justice capacity, partnership working, legislation and international cooperation and have been found to reduce country-level *perpetration* in terms of systems hacking (Kim *et al.* 2012). In addition, a measure of country-level Internet penetration was derived from the International Telecommunications Union (ITU) of the United Nations.[8]

[8] See: http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

Table 2 *Principal components analysis for online individual guardianship*

| Survey item | Component matrix | | |
|---|---|---|---|
| QE7: Has concern about security issues made you change the way you use the Internet in any of the following ways? | Avoidance Personal Guardianship | Active Personal Guardianship | Passive Physical Guardianship |
| Less likely to bank online | 0.814 | | |
| Less likely to buy goods online | 0.808 | | |
| Change security settings | | 0.683 | |
| Use different passwords for different sites | | 0.656 | |
| Only use your own computer | | | 0.521 |
| Do not open emails from people you don't know | | | 0.737 |
| Only visit trusted websites | | | 0.569 |
| Have installed anti-virus software | | | 0.714 |

Bartlett's test sphericity = $\chi^2$ (28) = 15561.11, $p < 0.01$; Kaiser–Meyer–Olkin measure of sampling adequacy (overall) = 0.707.

Previous research has demonstrated that countries with low Internet penetration and hence under-developed infrastructure are more likely to harbour cybercriminals (Kim *et al.* 2012). While no direction of the effect on *victimization* is assumed, we recognize that a negative association may indicate this measure acts as a proxy for country-level capable guardianship, with higher rates of use possibly indicating a more developed and secure Internet infrastructure (Manyika and Roxburgh 2011). We also recognize a positive association may indicate higher penetration increases the pool of potential victims.[9] These measures enable the testing of the effect of capable guardianship at the country level on individual online identity theft victimization, identifying if the patterns of contextual guardianship and cross-level interactions found in offline multi-level studies of RAT are replicated online (Miethe and McDowall 1993; Wilcox *et al.* 2007).

*Country economy and urbanicity.* A measure of country Gross Domestic Product (GDP) Purchasing Power Parity (PPP) was derived from International Monetary Fund statistics.[10] This measure, along with Internet penetration, replicates the work of Kim *et al.* (2012). A measure of country urbanization was derived from the United Nations Department for Economic and Social Affairs 'World Urbanization Prospects, 2011 Revision'.[11] This measure replicates the work on country-level offline victimization rates that are shown to vary by urbanicity (van Kesteren *et al.* 2014) by testing if this factor is also associated with cyber-victimization.

## *Analytic strategy*

Multi-level models allow for a fuller understanding of social processes as they consider place-level characteristics, as well as individual-level determinants. The former are important in that they can have causal effects that are irreducible to individual phenomena (Sampson 2012). This method of analysis was adopted in the present study

[9] I thank the anonymous reviewer for their comments on the possible effect of Internet penetration on victimization.

[10] See: http://www.imf.org/external/pubs/ft/weo/2013/02/

[11] See: http://esa.un.org/unpd/wup/index.htm

as country- and individual-level factors (e.g. guardianship) are hypothesized to effect online identity theft. Four models were built to test each of the hypotheses. Model 1 is a random intercept model including individual-level fixed effects and no country-level effects, providing a test of H1 to H2. This model also shows the extent to which unobserved EU country characteristics contribute to variations in online identity theft victimization. Model 2 adds country-level effects providing a test of H3. In Model 3, random effects are included by allowing individual level associations to vary across countries.[12] In conceptual terms, this means that the individual-level associations were allowed to take on different values in different EU countries. To identify the country characteristics that mediate individual associations with online identity theft, Model 4 includes cross-level interactions providing a test of H4 (see Appendix for formula and model diagnostics).

## *Results*

This section reports on the results from the series of multi-level Poisson regression models, where experiencing online identity theft was the outcome (Table 3). The random intercept model with individual-level covariates only (Model 1) provides an indication of the extent to which unobserved EU country characteristics contribute to variations in the incidence of online identity theft, acting as a reference point for the subsequent models. Several of the online routine activities emerged as significantly predictive of online identity theft, supporting hypothesis H1. Counter-intuitively, the routine activity of emailing emerged as negatively associated with online identity theft. This contradicts Reyns' (2013) finding that shows a positive association with identity theft (on and offline). This disparity may be explained by the difference in dependent measures between studies (the present study is purely focused on the online manifestation of the crime) and/or by the conflation of instant messaging with emailing in Reyns' study. In an attempt to explain why those who do not use email were expected to have a victimization rate 1.56 times greater than those who do,[13] logistic regression analysis was conducted (not shown here) to identify the unique characteristics of this sub-group in the sample.[14] The analysis revealed this group were significantly less likely to adopt passive physical guardianship (e.g. anti-virus) and active personal guardianship (e.g. changing passwords), were more likely to use the Internet in public places, and to use the Internet infrequently with low confidence, all factors that expose them to greater risk (see below). The analysis also revealed that non-users were more likely to be aware of cybercrime and to adopt passive avoidance guardianship (e.g. avoiding online banking, shopping etc.), which is also reflected in their lack of routine activities in these areas. This contradictory combination of high risk factors, avoidance behaviour and high awareness indicates that lack of email use is not causal of victimization, and that the reverse is likely possible: that victimization causes avoidance of email use, especially if this vector was used in the commissioning of the crime. Given the cross-sectional

[12] All individual-level associations were allowed to vary across countries, with each random coefficient estimated separately, before estimating all significant coefficients simultaneously.

[13] An incidence-rate ratio (IRR) is a univariate transformation of the estimated betas for the multi-level Poisson models. It is a relative difference measure used to compare the incidence rates of events (online identity theft) occurring at any given point in time. A score above 1 indicates an increased incidence rate ratio and below 1 a reduced incidence rate ratio for victimization.

[14] Results available upon request.

Table 3 *Individual and EU country correlates of individual counts of online identity theft victimization (multilevel Poisson models)*

| Predictor variables | Model 1 | | | Model 2 | | | Model 3 | | | Model 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Coefficient | SE | IRR | Coefficient | SE | IRR | Coefficient | SE | IRR | Coefficient | SE | IRR |
| Individual level | | | | | | | | | | | | |
| Constant | −1.69** | 0.08 | 0.13 | −1.17* | 0.70 | 0.31 | −0.96 | 0.67 | 0.38 | −2.04** | 0.95 | 0.07 |
| Online routine activities | | | | | | | | | | | | |
| Internet use: banking | −0.01 | 0.08 | 0.99 | 0.00 | 0.08 | 1.00 | −0.01 | 0.08 | 0.99 | −0.01 | 0.08 | 0.99 |
| Internet use: purchasing | −0.11 | 0.08 | 0.89 | −0.11 | 0.08 | 0.90 | −0.11 | 0.08 | 0.89 | −0.10 | 0.08 | 0.89 |
| Internet use: selling | 0.46** | 0.08 | 1.59 | 0.47** | 0.08 | 1.59 | 0.46** | 0.08 | 1.59 | 0.45** | 0.08 | 1.59 |
| Internet use: social ntwrkng | −0.03 | 0.07 | 0.97 | −0.03 | 0.07 | 0.97 | −0.02 | 0.07 | 0.98 | −0.02 | 0.07 | 0.98 |
| Internet use: email | −0.45** | 0.09 | 0.64 | −0.45** | 0.09 | 0.64 | −0.44** | 0.09 | 0.64 | −0.45** | 0.09 | 0.64 |
| Internet location: home | 0.18* | 0.08 | 1.20 | 0.18* | 0.08 | 1.19 | 0.18* | 0.08 | 1.20 | 0.18* | 0.08 | 1.20 |
| Internet location: university | 1.01** | 0.23 | 2.75 | 1.01** | 0.23 | 2.75 | 0.96** | 0.24 | 2.60 | 0.99** | 0.24 | 2.60 |
| Internet location: public | 1.14** | 0.22 | 3.14 | 1.15** | 0.22 | 3.16 | 1.12** | 0.22 | 3.07 | 1.09** | 0.22 | 3.07 |
| Internet location: cafe | 0.58 | 0.39 | 1.79 | 0.58 | 0.39 | 1.79 | 0.60 | 0.39 | 1.81 | 0.59 | 0.39 | 1.81 |
| Internet location: mobile | 0.12 | 0.33 | 1.13 | 0.12 | 0.33 | 1.13 | 0.09 | 0.33 | 1.10 | 0.08 | 0.33 | 1.10 |
| *(Reference: work)* | | | | | | | | | | | | |
| Frequency of Internet use | 0.09** | 0.01 | 1.09 | 0.09** | 0.01 | 1.09 | 0.09** | 0.01 | 1.09 | 0.09** | 0.01 | 1.09 |
| Capable guardianship | | | | | | | | | | | | |
| Active PG | 0.26** | 0.03 | 1.30 | 0.27** | 0.03 | 1.30 | 0.26** | 0.03 | 1.30 | 0.48 | 0.36 | 1.53 |
| Avoidance PG | 0.34** | 0.06 | 1.41 | 0.34** | 0.06 | 1.41 | 0.29** | 0.07 | 1.34 | 0.43 | 0.24 | 1.50 |
| Avoidance PG$^2$ | −0.14** | 0.03 | 0.87 | −0.14** | 0.03 | 0.87 | −0.14** | 0.03 | 0.87 | −0.34 | 0.29 | 0.38 |
| Passive PG | −0.25** | 0.03 | 0.76 | −0.25** | 0.03 | 0.76 | −0.25** | 0.05 | 0.76 | −0.98** | 0.05 | 0.76 |
| Worry about online ID theft | −0.32** | 0.03 | 0.72 | −0.31** | 0.03 | 0.73 | −0.31** | 0.03 | 0.73 | −0.31** | 0.03 | 0.73 |
| Individual characteristics | | | | | | | | | | | | |
| Male | 0.07 | 0.06 | 1.07 | 0.06 | 0.06 | 1.07 | 0.07 | 0.06 | 1.07 | 0.07 | 0.06 | 1.07 |
| Age | −0.01* | 0.00 | 0.99 | −0.01* | 0.00 | 0.99 | −0.01* | 0.00 | 0.99 | −0.01* | 0.00 | 0.99 |
| Education | 0.01 | 0.06 | 1.01 | 0.00 | 0.06 | 1.00 | 0.00 | 0.06 | 1.00 | 0.00 | 0.06 | 1.00 |
| Social status | −0.24** | 0.09 | 0.79 | −0.24** | 0.09 | 0.79 | −0.24** | 0.09 | 0.79 | −0.05 | 0.09 | 0.95 |
| Social status$^2$ | 0.02** | 0.01 | 1.02 | 0.02** | 0.01 | 1.02 | 0.02** | 0.01 | 1.02 | 0.02** | 0.01 | 1.02 |
| Deprivation | 0.14** | 0.05 | 1.15 | 0.13** | 0.05 | 1.14 | 0.14** | 0.05 | 1.15 | 0.09** | 0.05 | 1.15 |
| Suburban | −0.11 | 0.08 | 0.89 | −0.11 | 0.08 | 0.89 | −0.11 | 0.08 | 0.89 | −0.11 | 0.08 | 0.89 |
| Urban | 0.02 | 0.08 | 1.02 | 0.02 | 0.08 | 1.02 | 0.03 | 0.08 | 1.03 | 0.03 | 0.08 | 1.03 |
| *(Reference: rural)* | | | | | | | | | | | | |
| Country level | | | | | | | | | | | | |
| Capable guardianship | | | | | | | | | | | | |
| National cyber scrty strgy | | | | 0.00 | 0.01 | 1.00 | 0.00 | 0.00 | 1.00 | −0.00* | 0.00 | 0.99 |
| × Active PG | | | | | | | | | | 0.00 | 0.00 | 1.00 |
| × Avoidance PG | | | | | | | | | | 0.00 | 0.00 | 1.00 |

Table 3 *Continued*

| Predictor variables | Model 1 | | | Model 2 | | | Model 3 | | | Model 4 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Coefficient | SE | IRR | Coefficient | SE | IRR | Coefficient | SE | IRR | Coefficient | SE | IRR |
| × Passive PG | | | | | | | | | | −0.01** | 0.00 | 0.99 |
| Internet penetration | | | | −003* | 0.01 | 0.97 | −0.02* | 0.01 | 0.98 | −0.01 | 0.01 | 0.98 |
| × Active PG | | | | | | | | | | 0.00 | 0.00 | 1.00 |
| × Avoidance PG | | | | | | | | | | 0.01* | 0.00 | 1.00 |
| × Passive PG | | | | | | | | | | 0.01** | 0.00 | 1.01 |
| Economy and urbanicity | | | | | | | | | | | | |
| GDP (PPP) | | | | 0.01* | 0.01 | 1.01 | 0.01* | 0.00 | 1.01 | 0.01 | 0.00 | 1.01 |
| × Social status | | | | | | | | | | 0.00** | 0.00 | 1.00 |
| Urbanicity | | | | 0.01 | 0.01 | 1.01 | 0.01 | 0.01 | 1.01 | 0.01 | 0.01 | 1.01 |
| Random effects | | | | | | | | | | | | |
| Variance Avoidance PG | | | | | | 0.03 | 0.02 | | | 0.01 | 0.01 | |
| Variance Passive PG | | | | | | 0.04 | 0.02 | | | 0.02 | 0.02 | |
| Variance (intercept) | | | | | | 0.19 | 0.07 | | | 0.18 | 0.07 | |
| Covariance (avoid, passive) | | | | | | 0.00 | 0.01 | | | −0.01 | 0.01 | |
| Covariance (Avoid, intercept) | | | | | | 0.03 | 0.03 | | | 0.02 | 0.02 | |
| Covariance (Passive, intercept) | | | | | | 0.01 | 0.03 | | | −0.00 | 0.01 | |
| Variance component | | | | | | | | | | | | |
| MIRR | 1.60 | | | 1.52 | | | 1.60 | | | 1.55 | | |
| Log likelihood | −3591.4243 | | | −3588.8648 | | | −3571.2886 | | | −3555.7864 | | |
| *N* individual/*N* country | 14,193/29 | | | 14,193/29 | | | 14,193/29 | | | 14,193/29 | | |

Active PG = Active Personal Guardianship; Avoidance PG = Avoidance Personal Guardianship; Avoidance PG$^2$ = Avoidance Personal Guardianship$^2$; Passive PG = Passive Physical Guardianship. *$p < 0.05$; **$p < 0.01$.

nature of the survey, it is not possible to confirm this, but this analysis does suggest that email remains a likely risky routine activity that is targeted by offenders in the commissioning of online identity theft.

Holding all other factors constant, those using the Internet to sell goods were expected to have a victimization rate 1.59 times higher than those that did not. This is the first study to identify online auction selling as a highly risky routine activity for the targeting of potential victims in the commission of online identity theft. While other studies have identified website purchasing and banking as significant predictors of online identity theft (Pratt *et al.* 2010; Reyns 2013; van Wilsem 2013b) neither emerged as significant in this study. Place of Internet access and frequency of Internet use also emerged as significant. Compared to access in work, accessing the Internet anywhere else (except café and mobile) increased the incidence rate ratio. Frequent users of university and public computers (e.g. libraries) were expected to have victimization rates 2.75 and 3.14 higher, respectively. This is the first study to compare place of Internet access precluding comparisons with previous research. Nonetheless, it is clear this measure is important in the application of RAT to cybercrime.

The individual guardianship covariates all emerged as statistically significant, partially supporting hypothesis H2. Adoption of passive physical guardianship (e.g. anti-virus and secure browsing) was negatively associated with online identity theft victimization. Holing all other factors constant, individuals who increased their passive physical guardianship by one point on the scale reduced their incidence rate ratio by a factor of 0.76. Put another way, those who decreased their passive physical guardianship by one point were expected to have a victimization rate 1.32 times greater. Active personal guardianship (changing security settings and using different passwords) was positively associated with victimization, indicating a victimization causes adoption of guardianship relationship (see Discussion). A non-linear relationship was identified between avoidance personal guardianship (less banking and purchasing online) and experience of online identity theft, evidenced by the significant squared and non-squared terms. This indicates a monotonic increasing function of victimization by this type of guardianship until a turning point is reached, after which the function decreases. Differentiating the polynomial produces the slope of the relationship and Figure 1 presents a plot of predicted victimization by avoidance personal guardianship, confirming this assumption. Calculus was used to estimate the value of $x$ (avoidance personal guardianship) where $y$ (online identity theft) was greatest. This shows that the function turns at 1.22 on the avoidance personal guardianship scale. Those who worried more about online identity theft were less likely to be victimized, indicating concern may divert individuals from risky routines.

Of the individual characteristics, only social status and deprivation emerged as significant. Social status emerged as having a non-linear relationship to the dependent variable. Differentiating the polynomial and calculating the maxima shows that as self reported status increases, victimization decreases to a mid turning point of 5.24 where victimization begins to increase as social status rises (see Figure 2). Individual-level deprivation was also positively associated with victimization, with an increase by one point on the deprivation scale increasing the expected victimization rate by 1.15 times. Like Reyns (2013), this study shows socio-economic factors have an effect on online identity theft victimization, contrary to the studies by van Wilsem (2013b) and Pratt *et al.* (2010).

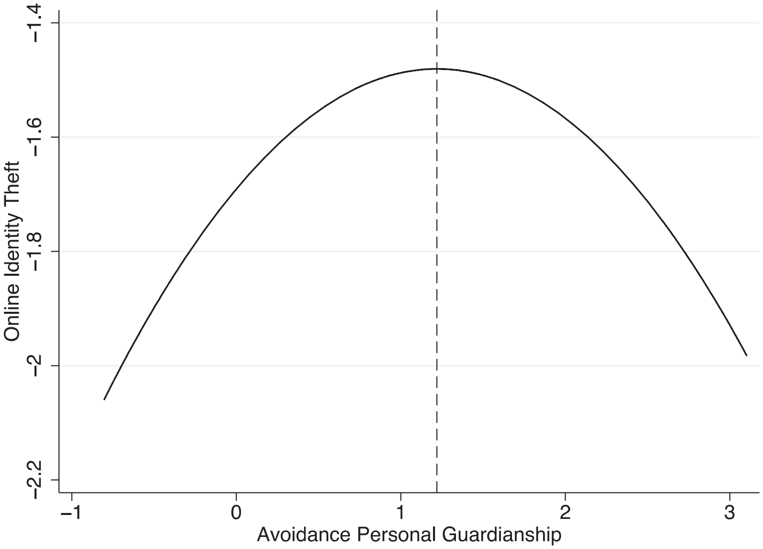

Fig. 1 Plot predicting online identity theft victimization by avoidance personal guardianship

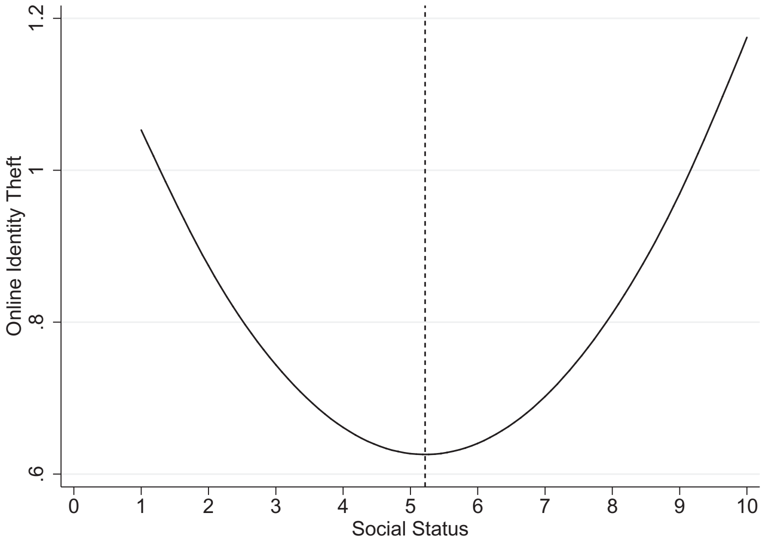

Fig. 2 Plot predicting online identity theft victimization by social status

The first model also confirms that variations in the incidence of online identity theft cannot be explained by individual level factors alone, with unobserved EU country characteristics accounting for a proportion of the variability. As a Poisson variant of a multi-level model was used, the Variance Partition Coefficient (VPC) could not be calculated.[15] Instead, to estimate the amount of residual variation in

[15] As a reference, a multi-level logistic regression was run on the same data, using a binary recoded outcome variable for online identity theft victimization, where the VPC was calculated as 7.9 per cent.

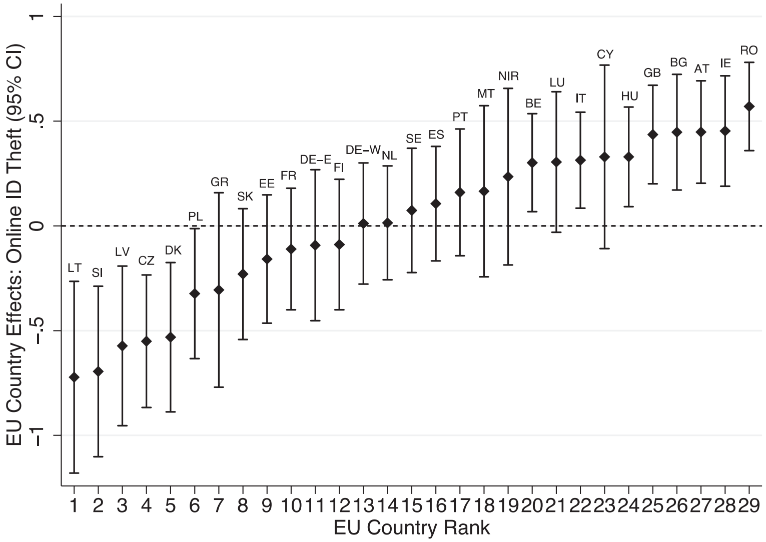

Fig. 3 Ordered EU country effects for online identity theft victimization

the likelihood of being a victim of online identity theft attributable to unobserved EU country characteristics (between-country variance), the Median Incidence Rate Ratio (MIRR) was used (Rabe-Hesketh and Skrondal 2008). The random intercept model country-level MIRR is equal to 1.60, which shows that in the median case, the residual heterogeneity between countries increases by a factor of 1.60 over the individual rate of victimization when randomly picking out two individuals in different countries—i.e. if an individual moves to another country with a higher incidence rate, their expected victimization rate will be 1.60 times greater (in median). These findings lend support to the contention that online identity theft victimization is not simply an attribute of individuals but may have a collective country-level component. Figure 3 presents a ranked caterpillar plot showing the estimates of the country effects with 95 per cent confidence intervals. The EU country[16] effects show that online identity theft victimization rates are significantly above the European average for Romania, Ireland, Austria, Bulgaria, Great Britain, Hungry, Italy and Belgium and significantly below the European average for Lithuania, Slovenia, Latvia, Czech Republic, Denmark and Poland. This variation in online crime patterns is consistent with the variation in patterns of offline crime across EU countries (Clarke 2013; van Kesteren *et al.* 2014).

The inclusion of country-level predictors (Model 2) decreased the country-level MIRR to 1.52. One feature of interest of the MIRR is that it is directly comparable with the IRRs of individual or country variables. The residual heterogeneity between countries remained of greater relevance than all individual-level guardianship covariates. However, individual-level routine activities covariates were of greater relevance,

[16] The figure shows 29 EU regions. This is because the Eurobarometer data collection strategy separates Northern Ireland from the rest of the United Kingdom and West and East Germany.

including Internet activity (auction selling IRR 1.59; email IRR 0.64) and Internet access (university IRR: 2.75; public IRR: 3.16 and café IRR: 1.79).

Hypothesis H3 was partially supported given Internet penetration was negatively associated with online identity theft, indicating that penetration may act as a proxy for more developed and secure physical Internet infrastructure that in turn mitigates victimization,[17] mirroring offline multi-level studies of RAT in relation to burglary (Wilcox *et al.* 2007). However, the direct measure of country capable guardianship (national cyber security strategy maturity) did not emerge as significantly associated with victimization. Higher levels of country level GDP (PPP) were significantly associated with increased rates of online identity theft. Therefore, Internet penetration and GDP (PPP) of the country both exert direct and independent effects on the rates of online identity theft impacting otherwise similar respondents in otherwise similar countries.

Model 3 allowed two individual-level coefficients, avoidance personal guardianship and passive physical guardianship, to have a random component at the country level. A likelihood ratio test showed an improved model fit, indicating that both individual level guardianship measures were moderated by the country in which respondents reside, with differences in the size of these level-1 fixed effects across countries. It is therefore assumed that differences in rates of online identity theft are conditional upon factors at the country level, with avoidance personal guardianship and passive physical guardianship both varying significantly across countries. In some countries, larger than average differences in victimization will exist between participants adopting such behaviours, while in others, these differences will be more moderate.

Model 4 included cross-level interactions between country-level and individual-level covariates. These interactions allowed for the determination of the country characteristics responsible for the higher level moderating effect. Three country-level covariates (Internet penetration, GDP (PPP) and cyber security strategy) were found to significantly moderate the effects of individual-level covariates of online identity theft (avoidance and active personal guardianship, passive physical guardianship and social status), supporting H4. Figure 4 shows the interaction between country Internet penetration and individual guardianship. It shows a heightened positive effect of country Internet penetration on both avoidance personal and passive physical guardianship, compared to active personal guardianship. This finding suggests that for those adopting high levels of avoidance personal guardianship, and particularly passive physical guardianship, country Internet penetration was of particular salience. Those residing in countries with low Internet penetration (and hence possibly under-developed infrastructure), who adopt these types of guardianship, were likely to experience more incidents of online identity theft, compared to those adopting these types of guardianship in countries with higher Internet penetration (and hence possibly better developed infrastructure). The same interaction effect was not evident for those adopting active security behaviour. Figure 5 shows the interactions between the direct measure of country capable guardianship (national cyber security strategy maturity) and individual guardianship. It demonstrates that maturity of cyber security strategy moderated differences in incidents of online identity theft between adopters of different types of individual guardianship. Adopters of passive physical guardianship residing

[17] We return to this in the Discussion given the alternative positive association also seems logical.

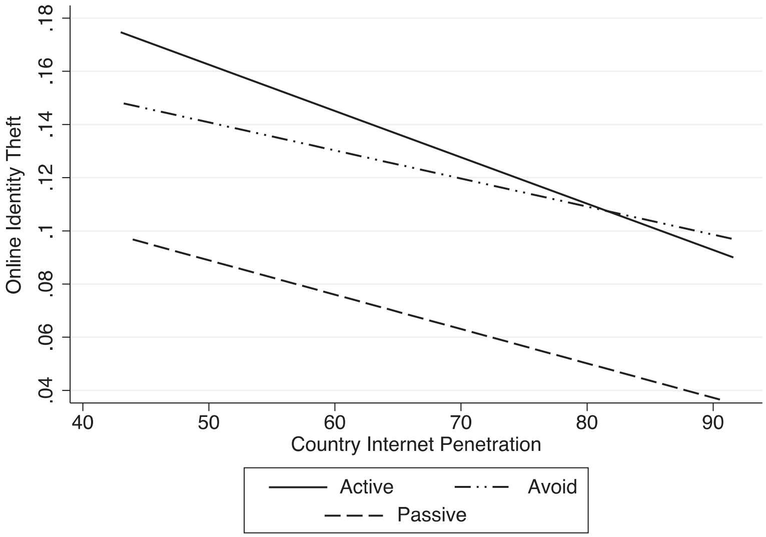

FIG. 4 Online identity theft by individual guardianship and Internet penetration

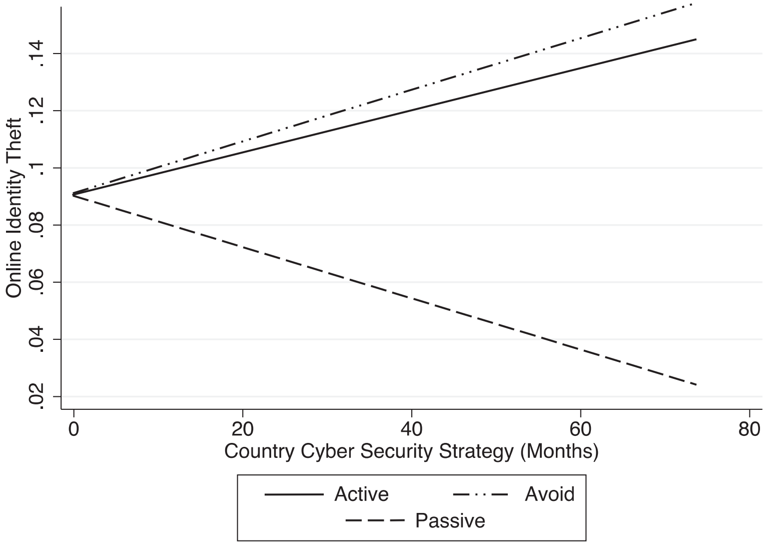

FIG. 5 Online identity theft by individual guardianship and country guardianship (National Cyber Security Strategy)

in countries with more mature cyber security strategies experienced decreased levels of online identity theft. The lack of significant interactions for active and avoidance personal guardianship indicates a lack of a cyber security strategy moderating effect on these types of individual guardianship. In other terms, personal guardianship maintains its level of effectiveness despite this type of country guardianship, while the superior effectiveness of passive physical guardianship is dependent upon this type of country guardianship. Therefore, if we are to assume Internet penetration acts a proxy

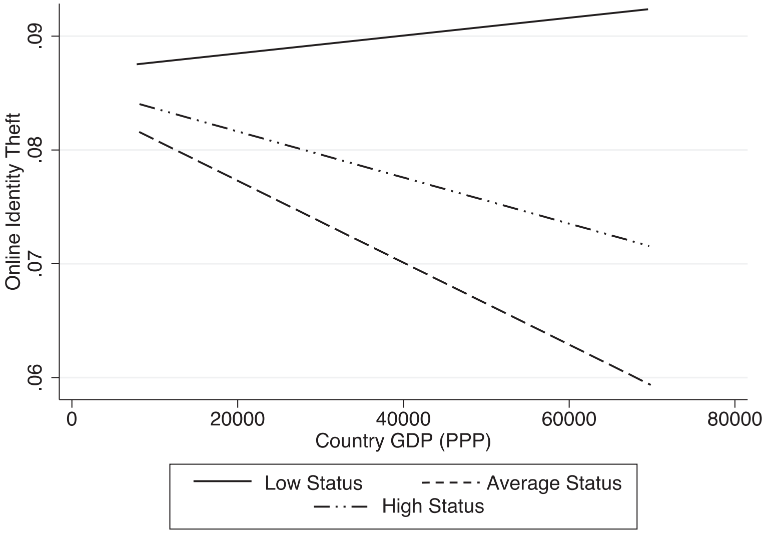

Fig. 6 Online identity theft by self selected social status and country GDP (PPP) (€)

for more secure infrastructure and hence is an indirect measure of country guardianship (see Discussion), this study finds that two types of country-level guardianship moderate the effectiveness of individual-level guardianship, mirroring findings from offline multi-level applications of RAT in the case of violent victimization (Miethe and McDowall 1993).

Figure 6 shows that the effect of self selected social status was significantly moderated by country economic performance. Mirroring the pattern in Figure 2, individuals identifying as average social status were least likely to experience online identity theft, compared to those reporting low or high status. In addition, those identifying as average and high status living in richer countries had lower victimization levels, as compared to their equivalents living in poorer countries. However, for those identifying as low status, living in richer countries was associated with significantly higher levels of victimization. In other terms, those of low status in poorer countries were less likely to be victimized compared to their equivalents in richer countries, who were most likely to be victimized.

## *Discussion*

This study contributes to the growing body of work on the theory of cybercrime and policy debates in four significant ways. First, the study showed the importance of including country-level measures in the study of online identity theft. The study found that higher levels of country Internet penetration reduced identity theft victimization. Penetration may be interpreted as a proxy for country physical guardianship, if we are to assume it is an indirect measure of more developed infrastructures. As developed infrastructures are likely to be characterized by superior security, it is possible that countries with them represent hard targets that may yield inadequate reward for the effort expended by offenders (Newman and Clarke 2003). This resonates with Wilcox *et al.*'s (2007) multi-level study of RAT and burglary where contextual guardianship mediated the effect of individual guardianship (such as target hardening), with individual guardianship reducing victimization in high guardianship neighbourhoods to a greater extent as compared to low guardianship neighbourhoods. This interpretation is supported by the rank of countries by victimization (Figure 3) that shows many of the countries clearly above the mean level of victimization (Romania, Bulgaria, Italy and Hungary) exhibit low Internet penetration (Romania, where citizens are most likely to be victimized, has the lowest penetration rate of all countries in the study).[18] Both Internet penetration and the direct measure of country capable guardianship (national cyber security strategy) were found to *moderate* individual passive physical guardianship, with higher levels of effectiveness in countries with more penetration and mature strategies. This finding mirrors offline research into RAT and violent crime that found interactions between criminal opportunities at the individual and city-block level were important in explaining victimization (Miethe and McDowall 1993).

In relation to policy, knowing that these national cyber security strategies work is key if organizations such as the United Nations (2013) and ENISA (2012*a*; 2012*b*) and national governments continue to allocate significant resources to their development. While existing work shows that countries without such policies (e.g. inter-jurisdictional arrangements and extradition protocols) host more perpetrators of cyber attacks due to a decreased risk of apprehension (Kim *et al.* 2012), similar work did not exist on victimization. This study shows that while there is no direct effect of country-level strategy, the interaction effect with passive physical guardianship provides mixed evidence as to the effectiveness of such strategies in preventing victimization in relation to online identity theft. It is clear that where they are in place, and well developed, a measurable effect on crime reduction, via bolstering passive physical guardianship, is observable. A possible explanation for the significance of the interaction effect may be the *enhanced quality* of this form of individual guardianship in countries with more mature strategies. For example, some strategies promote close working with industry and the banking sector, facilitating the exchange of information and technologies that may enhance the resilience of individual physical guardianship. The provision free of anti-virus software to customers by major banks (such as Barclays[19]) is a good example.

Second, the paper introduced a novel typology of individual online capable guardianship: passive physical, active personal and avoidance personal guardianship. The finding that passive physical guardianship was effective in reducing online identity theft is likely due to the automated form of this type of security. Like situational crime prevention techniques, anti-virus software and secure browsers are more effective than personal forms of guardianship due to their ability to automatically shape user behaviours while largely going unnoticed (Newman and Clarke 2003; Williams 2006; 2007).

[18] However, there are countries that emerge above the mean that do have higher than average Internet penetration. Previous research indicates that the United Kingdom in particular is disproportionally targeted for cyber attacks for reasons unknown (Kim *et al.* 2012). In such cases, the effect of high Internet penetration and hence better country infrastructure and security may be reduced. Furthermore, it is also logical to assume higher Internet penetration increases the potential pool of identity theft victims. Given the cross-sectional nature of the survey under study, we cannot confirm either of the possible explanations and recommend future research attempts to replicate this result and develop more robust measures of country-level infrastructure and security.

[19] See: http://www.barclays.co.uk/Helpsupport/FreeInternetSecuritySoftwarefromKasperskyBarclays/P1242557966961

Further, these technologies are remotely malleable and rapidly adaptive, precluding the need for user intervention to mitigate targeting attempts. This finding provides strong support for the policy assumption that individual passive physical guardianship significantly reduces the likelihood of online identity theft (ENISA 2012*a*; 2012*b*; Home Office 2013). Individual avoidance personal guardianship exhibited a curvilinear relationship with victimization, with levels of online identity theft increasing with avoidance guardianship, until a turning point is reached where the pattern is reversed (Figure 1). Therefore, we might conclude that for this type of guardianship to be effective, it must be adhered to strictly to achieve the desired reduction in victimization. However, we must acknowledge that it is also possible, given the cross-sectional design of Eurobarometer survey, that both reactive and prospective avoidance personal guardianship behaviours were captured, resulting in this pattern. Those victimized may report adopting moderate amounts of avoidance post victimization, representing the positive association, while those adopting more significant amounts of avoidance report less victimization, representing the negative association. In policy terms, avoidance guardianship, such as disengaging with online banking and shopping services, is undesirable. The Digital Agenda for Europe lists as a key priority area digital inclusion and the uptake of digital services (European Commission 2010). However, regardless of how we interpret the curvilinear pattern, it is evident that a high amount of avoidance personal guardianship has the desired effect of crime prevention online. Whether avoidance guardianship increases social exclusion and reduces quality of life, undesirable consequences of this behaviour found in offline crime prevention, is yet to be determined, and beyond the scope of this analysis (Doran and Burges 2012). The positive association found with active personal guardianship (changing security settings and passwords) is likely explained by post-victimization security reactions. Given the cross-sectional nature of the Eurobarometer survey data, we are not able to confirm this interpretation. However, like Skogan and Maxfield (1981) articulate in relation to offline crime, it is plausible that experience of online identity theft motivates precautionary and protective measures against the crime, such as changing passwords and security settings.

Third, the study showed that the site of routine Internet access is an important factor in the targeting of online identity theft victims. The increased rate of victimization for frequent users of university and public computers (e.g. libraries), as compared to users of workplace computers, is a novel finding. As RAT suggests, online identity theft victimization is more likely to occur when a motivated offender and a suitable target intersect in a network that has low levels of guardianship (Reyns 2013). It is likely that guardianship policies in public settings are less stringent than policies in the workplace, e.g., allowing users to plug-in their own devices that may contain malware from other computers in the home or elsewhere. Furthermore, public computers tend to have multiple users, increasing the potential pool of targets on networks with low levels of guardianship. For the first time, this study also identified selling on online auction sites as a risky routine activity. This is possibly explained by the prevalence of identity theft via phishing on large selling sites such as ebay. Sellers are often approached by perpetrators posing as legitimate buyers requesting banking details for payment transactions. Sellers are also duped into logging into spoof ebay sites, allowing perpetrators to gain control of accounts and begin fake-trading under the stolen identity, drawing on their online reputation.

Fourth, the study has shown that socio-economic individual-and country-level characteristics discriminate between victims and non-victims of online identity theft. At the individual level, social status exhibited a curvilinear association with victimization. Lower and higher status citizens reported the highest levels of victimization, while those of average status reported the lowest. This pattern differs from Reyns' (2013) study that shows those with higher incomes are most likely to be victimized, and from studies of offline victimization, where the most vulnerable in society are disproportionately victimized (Trickett *et al.* 1992). A similar disjuncture is found at the country level. While international comparative studies have found poorer countries suffer offline acquisitive crimes most (van Wilsem *et al.* 2003), the present study finds it are the richer countries that suffer online identity theft most. The significant cross-level interaction allows us to unravel the relationship between these two related multi-level factors. Those identifying as average and high status living in richer countries reported having lower victimization levels, as compared to their equivalents living in poorer countries. However, for those identifying as low status, living in richer countries was associated with significantly higher levels of victimization. In other terms, those of low status in poorer countries were less likely to be victimized compared to their equivalents in richer countries, who are most likely to be victimized. Therefore, when moderated by country economic performance, online identity theft victimization patterns do in fact follow conventional criminological understanding (Trickett *et al.* 1992). Cybercrime reduction policies in richer countries should therefore focus attention on promoting guardianship amongst lower status citizens, while a less discriminate approach should be adopted in the poorest countries.

## *Conclusion*

Online fraud is now recognized as the most prevalent acquisitive crime in Europe, above auto theft and burglary (Anderson *et al.* 2012). This study has explored whether online identity theft victimization, arguably the largest subset of general online fraud, is a function of risky online routine activities conducted within a network of suitable targets and motivated offenders in the absence of capable guardianship at the country and individual level (Eck and Clarke 2003). It has also tested the global cybercrime reduction policy assumption that country- and individual-level guardianship reduce online victimization (OECD 2011; United Nations 2013; World Bank 2014). The study introduced a novel typology of online guardianship and found that individual-level active personal guardianship and passive physical guardianship significantly reduced rates of online identity theft victimization. The study also found public Internet access and selling on online auction sites were significantly risky routine activities, exposing suitable targets to motivated identity theft perpetrators. But perhaps the most novel and noteworthy findings were those reported at the country level and the interactions between lower and higher level factors. Our analysis confirmed that, in the European context, countries exert independent influences on the risk of online identity theft victimization through national guardianship (Internet penetration and cyber security strategies) and economic performance, mirroring offline multi-level applications of RAT to the study of burglary (Wilcox *et al.* 2007). Country capable guardianship was also found to *moderate* individual guardianship, resonating with the multi-level application of RAT to the study of violence (Miethe and McDowall 1993). This latter finding provides some evidence in support of the argument that the governance of the Internet is achievable via combination of micro- and macro-guardianship. Knowing the moderating effect of cyber security strategies and Internet penetration on individual guardianship is key if national governments are to continue investing significant resources in cybercrime prevention efforts. Furthermore, the finding that country economic performance moderates individual social status in relation to online identity theft tells us that such strategies should target the most socio-economically disadvantaged in the richer countries, while being less discriminate in poorer counties.

In this study, the assumption was held that these mechanisms operate independently. However, in practice, the relationships are more complex, interacting and circulating in feed-back loops that are shaped by temporal forces. The limitations imposed by the static cross-sectional multi-national dataset precluded an analysis of complex dynamic causality (e.g. in relation to the email, active personal guardianship and social status findings), and instead the focus was upon the more fundamental work of identifying the independent direct effects of each mechanism. Therefore, this work should be considered as a first step towards understanding the complex nature of online identity theft at the country and individual level using RAT. Future work in this area could improve upon this foundation in several ways: (1) the selection of countries could be expanded to include non-EU states; Europe as a continent may exhibit certain distinctive characteristics (e.g. the wide adoption of national cyber security strategies) that are only observable via comparison with a more global selection of counties and continents; (2) average sample size in participating countries should be increased; in the present study, EU country samples were relatively small ($n$ = 1,000) considering that victimization is a rare event; (3) alternative spatial scales should be considered within countries, especially for those of significantly large size and (4) adding more measures of RAT, such as low-self control and social guardianship, may in general improve the prediction of victimization.

In recent times, criminological scholarship has been preoccupied with the influence of spatial forms on individual risk of criminal victimization (Sampson 2012). This paper underlines the relevance of studying country-level mechanisms, in addition to individual determinants, in the exploration of online identity theft by evidencing spatial form, at the level of the EU state, matters in the determination of victimization. As previous cross-national studies have been based on macro-level data (Kim *et al.* 2012), inferences about the impact of differential population composition on cybercrime were hard to draw. An innovation offered by the combination of country and individual-level data in this study is the possibility of disentangling the impact of EU country context and country composition in shaping victimization rates. The symmetries identified between multi-level offline studies (Miethe and McDowall 1993; Wilcox *et al.* 2007) and this present study of online victimization represent an important advancement in the evaluation of RAT and its general applicability to both terrestrial and online forms of crime.

## *Funding*

This work was supported by the Economic and Social Research Council and the Engineering and Physical Sciences Research Council grant ‘Identifying and Modelling

Victim, Business, Regulatory and Malware Behaviours in a Changing Cyberthreat Landscape' funded under the Global Uncertainties Consortia for Exploratory Research in Security (CEReS) programme (grant number: EP/K03345X/1).

## *Appendix*

### *Model formula and diagnostics*

Osgood (2000: 24) shows that the basic Poisson regression model is:

$$\ln(\lambda_i) = \sum_{k=0}^{K} \beta_k x_{ik} \tag{1}$$

$$P(Y_i = y_i) = \frac{e^{-\lambda_i} \lambda_i^{y_i}}{y_i\,!} \tag{2}$$

Equation (1) is the regression equation relating to the natural logarithm of the expected rate of online identity theft for individual $i$, $\ln(\lambda_i)$, to the sum of the products of each predictor variable, $x_{ik}$, multiplied by a regression coefficient, $\beta_k$. Equation (2) indicates that the probability of $\gamma_i$, the observed outcome for this individual, follows the Poisson distribution for the mean rate from Equation (1), $\lambda_i$.

The full multi-level Poisson regression model for a rate $Y_{ij}$ for individual $i$ in country $j$ can be written as (3), where, $Y_{ij}$ is the experience of online identity theft for the $i$th individual in the $j$th country, $\lambda_{ij}$ is the event rate (lambda) and $m_{ij}$ is the optional variable exposure rate (not specified in this model but included with a log transformation $\ln(m)$ to put it on the same scale as the latent outcome variable $\eta$). The standard link function for the Poisson distribution is the logarithm, and (4). The level-1 and level-2 model is constructed as (5) and (6), where $\beta_0$ is the intercept and $\beta_1$ is the regression coefficient for individual $i$ in country $j$ for the individual-level covariate $x$, giving (7) where $\gamma_{01}$ is the regression coefficient for the area-level coefficient $z$ in area $j$, and $\gamma_{11}$ is a cross-level interaction between individual covariate $x$ and area covariate $z$. In the random part of the model, $u_j$ are country departures from the overall level of online identity theft.

$$Y_{ij} \big| \lambda_{ij} = \text{Poisson } (m_{ij}, \lambda_{ij}) \tag{3}$$

$$n_{ij} = \log(\lambda_{ij}) \tag{4}$$

$$n_{ij} = \beta_{0j} + \beta_{1j} x_{ij} \tag{5}$$

$$\beta_{0j} = y_{00} + y_{01} z_j + u_{0j} \tag{6}$$

$$\beta_{1j} = y_{10} + y_{11} z_j + u_{1j}$$

$$n_{cij} = y_{00} + y_{10} x_{ij} + y_{01} z_j + y_{11} x_{ij} z_j + u_{0j} + u_{1j} x_{ij} \tag{7}$$

A non-significant likelihood ratio test of alpha = 0 ($\overline{\chi^2}$(01) = 0.00 $Pr \geq \overline{\chi^2}$ = 1.0000) indicated there was not a problem with over-dispersion of counts of online identity theft (the conditional variance did not exceed the conditional mean), indicating a Poisson model was preferred to a negative binomial model (Osgood 2000). The likelihood-ratio test statistic ($p$ = 0.00) compared the multi-level model to a single-level model with no country effects (i.e. linear regression). The two-level model therefore offered a significantly better fit to the data than the single-level model, meaning the likelihood of victimization varies significantly across countries. Correlation between the three individual guardianship measures and several demographic characteristics (social status, education and deprivation) were expected. However, results from correlational analyses, and tolerance statistics and variance inflation factors showed there were no problems with multi-collinearity among the predictor variables (correlation matrix omitted due to space restrictions. Available upon request.).

## References

Ablon, L., Libicki, M. C. and Golay, A. A. (2014), *Markets for Cybercrime Tools and Stolen Data*. Rand Corporation.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T. and Savage, S. (2012), ‘Measuring the Cost of Cybercrime’. Paper presented at the WEIS Conference, Berlin.

Banjo, S. (2014), ‘Hope Depot Hackers Exposed 53 Million Email Addresses’, *The Wall Street Journal*.

BIS. (2012), *10 Steps to Cyber Security*. Department for Business, Innovation and Skills.

Bossler, A. M. and Holt, T. J. (2009), ‘Online Activities, Guardianship, and Malware Infection’, *International Journal of Cyber Criminology*, 3: 400–20.

Bossler, A. M., Holt, T. J. and May, D. C. (2012), ‘Predicting Online Harassment Victimisation Among a Juvenile Population’, *Youth & Society*, 44: 500–23.

Bradford, W. R. (2013) ‘Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses’, *Journal of Research in Crime and Delinquency*, 50: 216, doi: 10.1177/0022427811425539.

Burnap, P., Rana, O. F., Avis, N., Williams, M. L., Housley, W., Edwards, A., Morgan, J. and Sloan, L. (2013), ‘Detecting Tension in Online Communities With Computational Twitter Analysis’, *Technological Forecasting & Social Change*.

Burnap, P., Williams, M. L. and Sloan, L. (2014), ‘Tweeting the Terror: Modelling the Social Media Reaction to the Woolwich Terrorist Attack’, *Social Network Analysis and Mining*, 4: 206.

Cabinet Office. (2014), *Communiqué from the Strengthening the Cyber Security of our Essential Services Event*. Cabinet Office.

Choi, K. (2008) ‘An Empirical Assessment of an Integrated Theory of Computer Crime Victimisation’, *International Journal of Cyber Criminology*, 2: 308–33.

Clarke, S. (2013), ‘Trends in Crime and Criminal Justice, 2010’, *Eurostat: Statistics in Focus*. European Union.

Cohen, L. and Felson, M. (1979), ‘Social Change and Crime Rate Trends: A Routine Activity Approach’, *American Sociological Review*, 44: 588–608.

Doran, B. J. and Burgess, M. B. (2012), *Putting Fear of Crime on the Map*. Springer.

Eck, J. E. and Clarke, R. V. (2003), 'Classifying Common Police Problems: A Routine Activity Approach', *Crime Prevention Studies*, 16: 7–39.

Empirica. (2007), *Benchmarking in a Policy Perspective: Security and Confidence*. Empirica.

ENISA. (2012*a*), *National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace*. European Union Agency for Network and Information Security.

——. (2012*b*), *National Cyber Security Strategies: Practical Guide on Development and Execution*. European Union Agency for Network and Information Security.

——. (2013), *ENISA Threat Landscape 2013 – Overview of Current and Emerging Cyber-Threats*. European Union Agency for Network and Information Security.

——. (2014), *16 Million E-Identities and Passwords Theft*. European Union Agency for Network and Information Security.

European Commission. (2010) *A Digital Agenda for Europe*. European Commission.

Fellowes. (2012), *UK at Greatest Risk of Identity Fraud in Europe*. Dynamic Markets.

Felson, M. (1998), *Crime and Everyday Life*, 2nd edn. Pine Forge Press.

Financial Fraud Action UK. (2013), *Fraud: The Facts 2013*. Financial Fraud Action UK.

Finkle, J. and Hosenball, M. (2014), *FBI Warns Retailers to Expect More Credit Card Breaches*. Reuters.

Gupta, M. and Sharman, R. (2011), *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. Information Science Reference.

Holt, T. J. and Bossler, A. M. (2008) 'Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimisation', *Deviant Behavior*, 30: 1–25.

Home Office. (2013), *New Campaign Urges People to be 'Cyber Streetwise'*. Home Office.

i2010 High Level Group. (2006), *Benchmarking Framework*. European Commission

Kim, S. H., Wang, Q. and Ullrich, J. B. (2012), 'A Comparative Study of Cyber Attacks', *Communications of the ACM* 55: 66–73.

Levi, M. and Williams, M. L. (2012), *eCrime Reduction Partnership Mapping Study*. Nominet Trust.

——. (2013), 'Multi-Agency Partnerships in Cybercrime Reduction: Mapping the Network and Cooperation Space', *Information Management and Computer Security*, 21: 420–43.

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

Miethe, T. D. and McDowall, D. (1993) 'Contextual Effects in Model of Criminal Victimisation', *Social Forces*, 71: 741–59.

National Fraud Authority (NFA). (2012), *Annual Fraud Indicator*. National Fraud Authority.

Newman, G. R. and Clarke, R. V. (2003), *Superhighway Robbery: Preventing E-Commerce Crime*. Willan.

OECD. (2011), *Reducing Systemic Cyber Security Risk*. Organisation for Economic Cooperation and Development.

ONS. (2014) *Discussion Paper on the Coverage of Crime Statistics*. Office for National Statistics.

Osgood, W. D. (2000) 'Poisson-Based Regression Analysis of Aggregate Crime Rates', *Journal of Quantitative Criminology* 16: 21–43.

Perlroth, N. and Gelles, D. (2014), *Russian Hackers Amass Over a Billion Internet Passwords*. New York Times.

Pratt, T. C., Holtfreter, K. and Reisig, M. D. (2010), 'Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory', *Journal of Research in Crime and Delinquency*, 47: 267–96.

Rabe-Hesketh, S. and Skrondal, A. (2008), *Multi-Level and Longitudinal Modeling Using Stata*, 2nd edn. Stata Press Publication.

Reisig, M. D., Pratt, T. C. and Holtfreter, K. (2009), 'Perceived Risk of Internet Theft Victimisation: Examining the Effects of Social Vulnerability and Financial Impulsivity', *Criminal Justice and Behavior*, 36: 369–84.

Reyns, B. W. (2013), 'Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses', *Journal of Research in Crime and Delinquency*, 50: 216–38. doi:10.1177/0022427811425539.

Sampson, R. J. (2012), *Great American City: Chicago and the Enduring Neighborhood Effect*. University of Chicago Press.

Skogan, W. G. and Maxfield, M. G. (1981), *Coping With Crime – Individual and Neighborhood Reactions*. Sage.

Sloan, L., Morgan, J., Housley, W., Williams, M. L., Edwards, A., Burnap, P. and Rana, O. F. (2013), 'Knowing the Tweeters: Deriving Sociologically Relevant Demographics From Twitter', *Sociological Research Online*.

Trickett, A., Osborn, D. R., Seymour, J. and Pease, K. (1992), 'What Is Different About High Crime Areas?' *British Journal of Criminology* 32: 81–9.

United Nations. (2013), *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime.

van Kesteren, J., van Dijk, J. and Mayhew, P. (2014), 'The International Crime Victim Surveys: A Retrospective', *International Review of Victimology*, 20: 49–69.

van Wilsem, J. (2011) 'Worlds Tied Together? Online and Non-Domestic Routine Activities and Their Impact on Digital and Traditional Threat Victimisation', *European Journal of Criminology*, 8: 115–27.

——. (2013*a*) 'Hacking and Harassment – Do They Have Something in Common? Comparing Risk Factors for Online Victimisation', *Journal of Contemporary Criminal Justice*, 29: 437–453.

——. (2013*b*). '"Bought it, but never got it." Assessing Risk Factors for Online Consumer Fraud Victimisation', *European Sociological Review*, 29: 168–78.

van Wilsem J., de Graaf N. D. and Wittenbrood, K. (2003), 'Cross-National Differences in Victimisation: Disentangling the Impact of Composition and Context', *European Sociological Review*, 19: 125–42.

Wall, D. S. (2013), 'Policing Identity Crimes', *Policing and Society*, 23: 437–60.

Wall, D. S. and Williams, M. L. (2007), 'Policing Diversity in the Digital Age: Maintaining Order in Virtual Communities', *Criminology and Criminal Justice*, 7: 391–415.

——. (2013), 'Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing', *Policing & Society*, 23: 409–12.

——. (2014), *Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing*. Routledge.

Wilcox, P., Madensen, T. D., Tillyer, M. S. (2007), 'Guardianship in Context: Implications for Burglary Victimisation Risk and Prevention', *Criminology*, 44: 771–803.

Williams, M. L. (2000), 'Virtually Criminal: Discourse, Deviance and Anxiety Within Virtual Communities', *International Review of Law, Computers & Technology* 14: 95–104.

——. (2004) 'Understanding King Punisher and His Order: Vandalism in a Virtual Reality Community - Motives, Meanings and Possible Solutions', *Internet Journal of Criminology*.

——. (2006), *Virtually Criminal: Crime, Deviance and Regulation Online*. Routledge.

——. (2007), 'Policing and Cybersociety: The Maturation of Regulation Within an Online Community', *Policing and Society*, 17: 59–82.

Williams, M. L. and Levi, M. (2012), 'Perceptions of the eCrime Controllers: Modelling the Influence of Cooperation and Data Source Factors', *Security Journal*. Advance online publication 17 December 2012, doi:10.1057/sj.2012.47.

Williams, M. L., Edwards, A., Housley, W., Burnap, P., Rana, O. F., Avis, N., Morgan, J. and Sloan, L. (2013), 'Policing Cyber-Neighbourhoods: Tension Monitoring and Social Media Networks', *Policing and Society*, 23: 461–81.

World Bank. (2014), *Cyber Security: A Model for Protecting the Network*. World Bank.

Yar, M. (2005), 'The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory', *European Journal of Criminology*, 2: 407–27.