ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cybercrime-journal

The Commonwealth

UK Cybercrime, Victims and Reporting: A Systematic Review

Juraj Sikra,[1,2,3] Karen V. Renaud[1,4,5,6] and Daniel R. Thomas[1,7]

Abstract

Individuals and organisations based in the UK often fall foul of cybercriminals. Unfortunately, however, these kinds of crimes are underreported [68][123] [133]. This underreporting hampers the ability of crime-fighting units to gauge the full extent of the problem, as well as their ability to pursue and apprehend cybercriminals [14][81].

To comprehend cybercrime underreporting, we need to explore the nature of UK cybercrime and its impact on UK-based victims. We investigated the entire landscape by carrying out a systematic literature review, covering both academic and grey literature. This review sought to answer three research questions.

1. What characterises cybercrime in the UK?
2. What is known about UK cybercrime victims?
3. What influences and deters cybercrime reporting in the UK?

Our investigation revealed three types of reportable cybercrime, depending on the target: individuals, private organisations and public organisations.

Victimhood varies depending on a number of identified dimensions, including vulnerability aspects, psychological perspectives, age-related differences and researcher attempts to model the victims of cybercrime. We also explored UK victims' reported experiences in dealing with the consequences of falling victim to a cybercrime.

In terms of cybercrime reporting, we identified three kinds of reporting: human-to-human, human-to-machine and machine-to-machine. In examining factors deterring reporting, we incorporated discussions of policing, and the challenges UK police forces face in coping with this relatively novel crime. Unlike in traditional

1 Computer and Information Sciences, University of Strathclyde (Glasgow, UK).
2 Faculty of Psychology, Taras Shevchenko National University of Kyiv (Kyiv, Ukraine).
3 E-mail: juraj.sikra@strath.ac.uk
4 Department of Information Systems, Rhodes University (Grahamstown, South Africa).
5 School of Computing, University of South Africa (Pretoria, South Africa).
6 Division of Cybersecurity, Abertay University (Dundee, UK).
7 Computer Laboratory, University of Cambridge (Cambridge, UK).

crimes, perpetrators possess sophisticated technological skills and may reside outside of the UK's police jurisdiction. We discovered a strong social dimension to reporting incidence, with the UK government's cyber-responsibilisation agenda likely playing a major role in deterring reporting. This strategy involves the government providing a great deal of advice and then expecting citizens to take care of their own cybersecurity. Within this, if citizens do not act on the advice, they have to accept the consequences.

Improvements in cybercrime reporting have to date been technologically focused. This neglects the social dimensions of cybercrime victimhood and does not acknowledge the reporting-deterring side-effects of the UK's cyber-responsibilisation agenda. We thus conclude with suggestions for improving cybercrime reporting in the UK.

1. Introduction

Cybercrime is a reality of everyone's networked lives, and UK citizens are no exception, and are increasingly falling victim [52][60][105][113]. Indeed, Caneppele, and Aebi [24] report that between a third and half of the crimes committed in a country are likely to be cybercrimes. Cybercrime costs citizens and the UK dearly, as shown in Figure A1 in the Appendix. The consequences of falling victim to a cybercrime can be significant and are not limited to financial loss. Some victims suffer from poor mental health and other health consequences [102]. The UK's cybercrime landscape is poorly understood, given that cybercrimes are significantly underreported [68][105][123][133]. Such underreporting makes it difficult for law enforcement to gauge the true extent of cybercrime [116] or to invest resources appropriately to address it [14][81].

One aspect that could be deterring reporting is the cyber-responsibilisation agenda pursued by the UK government, in common with other neoliberal governments [118] [119]. Responsibilised citizens are given advice and then are expected to embrace the responsibility and accept the consequences if they do not follow it. Consequently, victims may be too embarrassed to report what has occurred if they did not, or could not, follow the government-issued advice [1]. Reporting a cybercrime may well be considered an embarrassing admission of negligence and signal irresponsibility. As such, reporting could trigger an additional trauma that victims may dread.

This paper focuses only on the UK because carrying out this kind of study globally would introduce noise emanating from a large variety of legal, economic and policing differences, and this might confound our analysis and obscure insights. Fortunately, UK findings related to underreporting can still offer lessons for other countries, especially those with neoliberal governments, given that a side-effect of responsibilisation may be to deter reporting.

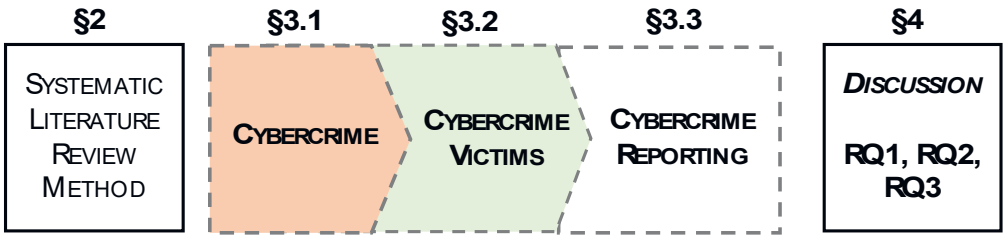
A systematic review was carried out to answer the following research questions with respect to the UK's cybercrime landscape:

RQ1: What characterises cybercrime in the UK?

RQ2: What is known about UK cybercrime victims?

RQ3: What influences and deters cybercrime reporting in the UK?

Figure 1. Structure of the paper: Cybercrime, Victims and Reporting in the UK



As Figure 1 shows, Section 2 outlines the systematic literature review methodology. Section 3 then reports our findings on UK cybercrime (Section 3.1), UK cybercrime victims (Section 3.2) and cybercrime reporting (Section 3.3). Section 4 returns to the research questions and discusses the findings. Section 5 concludes.

2. Systematic literature review methodology

Using the principles of systematic research as outlined by Pickering et al. [112], a search was conducted across the following databases: Scopus, Web of Science and ProQuest. Keywords were chosen to meet the needs of each of the research questions. The search period commenced in 1999, based on publicly available information concerning the growth of online retail in the world, which saw its inception in the mid-1990s onward [93]. The earliest included article concerning the subject is by Fisher in 2008 [51]. The searches are depicted using the PRISMA diagrams supplied in the Appendix. Table 1 maps the research questions to the PRISMA diagrams.

Table 1. Systematic review process

	PRISMA in Appendix
RQ1: What characterises cybercrime in the UK?	Figure A2
RQ2: What is known about UK cybercrime victims?	Figure A3
RQ3: What influences and deters cybercrime reporting in the UK	Figure A4

We focused primarily on UK sources but included publications from outside of the UK where we considered that the applicability of their findings to the UK could be argued. Where we found research from other countries that offered lessons to the UK, we retained these. Table A1 in the Appendix provides a list of these references.

Filtering

The documents were filtered based on their titles and abstracts, which were the core determinants for including them in the review. Documents that were included in the review were grouped according to common themes.

Analysis

The approach applied within was adapted from Robinson's guidance on thematic analysis [120]. Specifically, an inductive approach was operationalised, which commences with data immersion (i.e., re-reading the identified articles) and results in several emergent themes. These themes are then contrasted against all the data to ensure a good fit.

3. Results

Previous research has shown that cybercriminals seek to understand victims in a predatory way so that they can insert themselves into their lives by exploiting their needs [17][43][66][89][106][140]. Johnson [74] reports that 20 per cent of UK survey respondents had found malicious software on their devices over the past three years. This demonstrates a measure of success in compromising UK citizens' devices. We now consider what is reported about UK-related cybercrime.

3.1 Cybercrime in the UK

The National Crime Agency (NCA) estimated that 1 million cybercrimes were committed in 1999 across the UK's households [105]. Similarly to in other countries, there is evidence that the number of cyber-offences is increasing: by 2021 it had doubled, to 1.8 million, relative to 2019 [50]. In December 2021 [130], it was reported that 48 per cent of UK citizens had experienced cybercrime, as compared with 76 per cent of Indians and only 32 per cent of Japanese. According to Daniel Markuson [99], cybercriminals, like other criminals, look for opportunities. Countries where citizens spend more time online, and shop more online, are more at risk. The top 10 'at risk' countries include the UK.

Fraud was the most common type of cybercrime targeting UK citizens in the NCA survey in 2019 [105], with Internet-enabled fraud making up 54 per cent of all fraud cases. Romance fraud was another major type of crime, causing economic damage of £60 million, primarily targeting women with disposable funds.

A major source of cybercrime incidents in the UK (by number) is illegal booter services, which allow criminals to target specific organisations with denial-of-service attacks. In 2016, a 20-year-old British male was sentenced to 18 months in a youth detention centre and required to pay £800 damages for running four booter services [31].

In the UK, criminal networks are often responsible for attacks [83]. The NCA survey found that that Russian-language cybercrime groups posed the greatest threat to the UK [105]. Yet, Lavorgna [83] has warned against overestimating the extent of organised cybercrime within the UK lest public funds be unnecessarily depleted, because cybercriminals are not all affiliated with organised groups. Another common kind of crime that targets UK citizens is romance scams, which involve interaction with a fake profile [140]. People are tricked into sending money to these scammers in exchange for explicit media [66][107].

Research tracing individual cybercrime reports to offenders has revealed interesting results [17]. It emerges that a relatively small number of offenders are responsible for many offences. A deeper analysis of these reported results reveals that the offenders who attract the most reports are not always those who make the most money from their crimes.

In May 2022, the Director of the UK's Government Communications Headquarters (GCHQ), Sir Jeremy Fleming, advised the public about the organisation's proactive approach to cyber-fraud, which had spiked in conjunction with Russia's illegal invasion of Ukraine. Specifically, GCHQ took down 2.7 million online scams during 2021 alone [52]. He argued that this approach mirrored the overall restructuring of the western security architecture, as summarised by the old Latin proverb: *si vis pacem, para bellum* – that is, 'If you want peace, prepare for war.'

Typology of cybercrime

A three-dimensional typology of cybercrime emerged from the literature, reflecting attacks against (1) individuals, (2) private institutions and (3) public institutions. According to Levi [88], companies rather than individuals incur the largest financial losses. Yet the impact on individuals should not be downplayed, as they are likely to be seen as easy targets for cybercriminals [128]. The typology is critical for improving cybercrime reporting because it supports categorisation and coding of offences.

Even so, it should be noted that an attack on an individual can spread to their employer's devices. A case in point occurred in Scotland in March 2022 [75], when the Scottish Association for Mental Health experienced a ransomware attack that sprang from an individual employee's personal device. This resulted in passports and personal data being made public.

Cybercrime against individuals: In 2016, Levi [87] references a cybercrime survey of 3.8 million cases. He found that individuals were most likely to experience bank card fraud. The total number of incidents of fraud in 2016 exceeded 2.5 million (66 per cent of all

incidents). Online shopping fraud totalled more than 1 million incidents (28 per cent of all incidents). Other authors highlight denial-of-service attacks on end users (i.e., game players) [31]. Shared computers constitute a particular problem given the ease with which users' personal details can be collected and sold [3] and with which compromises can jump from one individual's device to another's and from individual to organisational devices.

Kemp et al. [79] analysed the changes in cybercrime during the pandemic in the UK. They found a significant increase from over 2,000 reported offences before lockdown to nearly 4,000 offences during lockdown. Kemp et al. found that the closing of physical shops led to an increase in online shopping, which sometimes resulted in fraud. On the other hand, a reduction in ticket-related leisure activities and aviation reduced ticket-related fraud. Cybercriminals exhibit adaptiveness and innovativeness.

Cybercrime against private institutions: The 2022 Cyber Security Breaches Survey [47] reported that 39 per cent of UK businesses were attacked in 2022, mostly by phishing attempts (83 per cent). In the past, these have included attacks on banks via forged cheques [51]. Cybercriminals can also impersonate a CEO's email, to achieve a speedy transfer of funds to a named 'supplier' (known as 'CEO fraud' or 'business email compromise' [91]. Small and medium-sized enterprises (SMEs) are particularly vulnerable to these kinds of attacks [90]. However, Kemp et al. [79] found that, during the pandemic, organisations experienced decreased levels of cybercrime. The suggested explanations relate to the closing of businesses and restructuring, which may have reduced attack surface and victimhood.

Cybercrime against public institutions: Wirth [143] outlined the devastating effect of the WannaCry ransomware on the National Health Service (NHS) in 2017. WannaCry impacted 81 of 236 hospital trusts and 597 of 7,545 GP surgeries and resulted in the cancellation of 20,000 appointments. This sets these kinds of targeted cybercrime apart from other kinds of crime [39]. Criminals who burglarise or mug would not be able to attack this many targets simultaneously. A single cyber-attack can target multiple organisations and be hard to recover from, given the required technological expertise [5]. WannaCry 2017 is a case in point [106].

Summary

The UK is clearly experiencing high levels of cybercrime. The profile is not identical to that in other EU countries [116]. For example, online shopping fraud affects 0.6–4 per cent of people annually based on a comparison of survey data vs police data, and the UK's higher online shopping levels will mean that it is more affected than other countries where there is less shopping online. Online banking fraud, too, is less common in the EU than in the UK, at around 1–2 per cent. Less than 1 per cent of the EU population have been victimised

via advance fee fraud or identity fraud. Cybercriminal creativity and adaptivity target victims where the attack surface presents itself. With so many UK residents being online, the attack surface is large enough to facilitate attacks.

The next section considers UK cybercrime victims.

3.2 UK cybercrime victims

Action Fraud has highlighted a dramatic spike in cybercrime against individuals during the recent COVID-19 pandemic [17], so it is reasonable to argue that cyber-victimhood is increasing. How does the UK government respond? In 2008, Shadow Home Secretary David Davis MP, after his own victimisation, criticised the UK government for being ineffective in tackling cybercrime [63]. Hunter [63] critiqued the lack of a dedicated centre for tackling cybercrime and the police's tendency to investigate only high-value crimes. At that point, Action Fraud, a designated centre for cybercrime reporting, was established. However, the problem with investigating only high-value offences persists. The difference is that Hunter complained that the police investigated only losses of more than £500. In 2019, that figure increased to losses over £100,000 [35]. The literature also highlights the cost of an effective defence system to assist victims [11].

Böhme [11] argues that cyber-attacks must be quantified in terms of both financial and psychological damage but also acknowledges that it is difficult to quantify such attacks in terms of the latter. However, it is important to recognise both kinds of impact in terms of delineating the cybercrime landscape.

Victims can experience adverse health consequences. Button et al. [22] found that some cyber-victims experienced headaches, flare-ups of existing conditions such as fibromyalgia and Crohn's disease, withdrawal from relationships, isolation, depression, anxiety and suicide. Other research from UK psychiatry argues that, while it is difficult to develop an objective compensation for psychological distress, the affected party should be provided with psychological therapy to help them deal with the victimhood trauma [13].

Böhme and Moore [23] analysed the experiences of victims within the EU (which included the UK at the time of the study). They found that victims reduced their online shopping and online banking activities by 4–5 per cent. Moreover, people who had been exposed to information about cybercrime threats were twice as likely to diminish their online activity, as compared with actual victims, suggesting that dread and fear were preventing them from benefiting from the online world. Indeed, Cross et al. [44] revealed unrealistic risk perceptions, with respondents considering their risk of victimisation to be low despite most having reported falling victim to a cybercrime in the past. Considering these two studies, it seems that those who have fallen victim to cybercrime underestimate the risk, whereas those who merely hear about the possibility of falling victim deliberately reduce their risk by changing their behaviours.

Individual victim profiles

There are several dimensions to consider here.

Vulnerability: Victims' experiences are connected to their needs [86]. Feelings of loneliness and isolation lead to increased cybercrime victimisation [17]. Pet scams targeting pet owners have increased, with fraudsters requesting money, falsely claiming to have found a lost pet [89].

Crimes against the elderly increased during the COVID-19 pandemic [43], especially economic scams [113][36]. Correia [36] discovered that the average repeat victim was older than an average single case victim. Age also played a significant role with respect to romance fraud during the pandemic [17]. Seniors who fall victim are treated much less fairly in the UK and require special assistance to participate fully in criminal proceedings [14].

Psychological perspective: In terms of personality type, people high on neuroticism, low on conscientiousness and high on openness (to experience) are likelier to be victimised by cybercrimes [133]. Jones et al. [76] found that people who were able to proceed with cognitive reflection (i.e., suppressing incorrect information vs correct information) were moderately less prone to opening fraudulent emails. Moreover, people who scored high on sensation seeking (i.e., the personality trait of pursuing varied, novel, intense and complex experiences) were more inclined to give into automatic processes and to open fraudulent emails. Monteith et al. [102] found that even previously mentally unaffected individuals could slide into mental illness because of falling victim to cybercrime. People with pre-existing mental health conditions are particularly vulnerable to economic cybercrime. It is likely that people with a mental health conditions will experience additional obstacles to reporting if, for instance, they suffer from paranoid delusions, which can make them question their authentic experiences.

Modelling cybercrime victims: To compile an accurate victim profile, the Routine Activity Theory (RAT) is helpful [104]. The theory can be summarised as follows: people who behave insecurely online are more likely to be victimised. Nasi et al. [104] surveyed 999 respondents from the UK and matched their data with the assumptions from RAT. They found that being male, young, migrant, urban, not living with parents and unemployed with more social life online vs offline were all predictors of victimisation. Even so, caution should be exercised when discussing victim profiles so that the rhetoric does not slide into victim-blaming.

Private institution victim profiles

Bana and Hertzberg [6] found that, between 2012 and 2014, the UK's top law firms' prioritisation of cybersecurity doubled from 23 to 46 per cent. This means that nearly half of UK law firms had come to view cybersecurity as a priority, up from just under one-quarter two years earlier. This increase may have been influenced by an attack on ACS:Law, a prominent UK law firm, in 2010 [6]. Subsequent research has discussed the

unexpected dip in the number of victims from private institutions despite the increased number of attacks, because of improved cybersecurity [26]. Connolly et al. [34] have found that private institutions suffer much greater harm than public institutions when attacked (p=0.044). This is because the former facing greater redundancies but also because public institutions can invest more in securing their systems. Donegan [49] argues that cybercriminals profile SMEs because these have more vulnerabilities. First, they often communicate payment correspondence via email. Second, their use of systems such as Office365 is another source of vulnerability. Third, SMEs often have publicly available information on the web that includes information about staff, which allows hackers to target those with access to funds using social engineering techniques. Connolly and Borrion [33] examine the trade-offs in victims' decision-making processes when deciding whether to pay off a ransomware attacker. Private institutions pay when they have ineffective backup, when the data are critical to the business, when there is a real risk of bankruptcy or when they follow the advice of an IT consultant.

Public institution victim profile

The WannaCry attack of 2017 cost the NHS over £93 million. In addition, Johnson [71] reports on extensive attacks aimed at the public sector in the UK, claiming that the number of ransomware attacks between 2020 and 2021 more than doubled. In 2022, the pattern of attacks mentioned by Johnson impacted UK citizens' ability to access health and social care, council tax and the like. In the case of Hackney Council, the effects of an attack cost £10 million and endangered human lives. However, the cybercrime landscape with respect to public institutions in the UK is nuanced. Take, for example, an attack on Advance in August 2022 by Ransomware [134][100]. Advance is a provider of digital services to the NHS (e.g., patient check-in) but is also a company, so is difficult to classify into one category. The attack had negative impacts on the NHS and the health of its patients.

3.3 What deters cybercrime reporting in the UK?

The first question to consider is the extent to which cybercrime victims report cybercrimes if they do fall victim. There is a great deal of evidence to show that cybercrimes are underreported [93][81]. A survey carried out in 2006 in the UK revealed that only 13 per cent of victims of cybercrime incidents had reported them [141]. To address this, some countries have created specific cybercrime reporting portals – for example Nigeria [67], Taiwan [81], the UK [2] and India [78]. These efforts attempt to address the fact that people do not always know *where* to report cybercrimes [20][10].

Despite these efforts, cybercrime continues to be underreported. It is likely that the barriers to reporting are more complex and nuanced than a technical solution could address merely by coming into being. Consider that victims may well report these kinds of crimes to their banks [81] or to their Internet service provider [141]. They may feel that these entities are better placed to help them than some country-wide reporting service.

In contemplating cybercrime reporting, we can learn from more general crime reporting, which depends on the nature of the victimisation, trust in the police, expectation that reporting will be responded to and the convenience of reporting [77][144]. It may be that a minor virus infection, which is easily ameliorated, is considered too small to merit reporting.

Some studies have specifically looked at cybercrime reporting. For example, van de Weijer et al. [136] found that Netherlands citizens would often not report cybercrime because they did not believe the police could do anything about what had happened (echoing [77][144]). McMurdie [98] suggests that people do not see any benefit in reporting cybercrimes, with Correia [37] confirming that people's perceptions of the effectiveness of police responses either deter or encourage reporting. Chawki [27] says that cybercrime victims can lose more from reporting crimes than they have already lost from the crimes themselves. Even such a perception would deter reporting. Wall [138] suggests that cybercrime may seem less significant than a violent crime such as mugging, because it is informational. People may not consider it worth reporting, perhaps because they do not realise the future implications of the information loss.

Other researchers surmise that people will not report because of a fear of being ridiculed [69]. Chawki [27] highlights reporting barriers including embarrassment, legal fees and increased insurance premiums, citing Parker [110][109]. This would align with the country's cyber-responsibilisation strategy, with citizens feeling they cannot complain since they did not follow the advice the government provided [118][119].

Reporting, or the lack thereof, is dependent on individual factors too. Gutierrez and Kirk [56] find that immigrants are less likely to report all kinds of crimes, and this is likely to apply to cybercrimes too. Holt et al. [60] find that those with less technological expertise underreport virus infections. Sometimes, cultural aspects prevent reporting, such as the need to save face [28].

Cross [40] argues that there is limited research documenting all the reasons for victims reporting, or not reporting, cybercrimes. With a relatively poorly understood range of deterrents or incentives, law enforcement does not get the reports, and cannot gain insights into the full extent of the country's cybercrime. This means it is less able to compile robust statistics [72].

In examining cybercrime reporting rigorously, several dimensions are pertinent: what kinds of cybercrimes people would report and what kinds they would simply accept; to whom they would report the crimes; and what they want from the entity they would report to. We consider the research for each of these dimensions here.

1. **Kinds of cybercrimes:** Crime type and seriousness are the largest predictors of reporting behaviour for other kinds of crimes [8][132][136]. Because cybercrime is underreported, it is difficult to answer this question definitively. What we do know is

that females are significantly more likely to report advance-fee fraud, with this effect being more pronounced in seniors [35][36]. This fraud requires victims to transfer a small amount of money with the promise of a significant return on their investment.

2. **Whom to report to:** Using a hypothetical and simulated setup, scientists presented 595 participants with vignettes about cybercrime to explore whom they would report such crimes to. People were more likely to report the offence to an organisation as opposed to the police. The exception is identity theft, which people were equally likely to report to the police and to organisations [136]. A study in Saudi Arabia [4] found that, of 267 victims, 31 per cent would not know whom to report to but would ask their friends, 15 per cent would use the Saudi government e-portal and only 7 per cent would report directly to the police.

3. **What victims want:** Victims of cyber-fraud have pronounced emotional needs, which revolve around receiving recognition from society and the police for their ordeal, which is linked to being able to tell their story [86]. Leukfeldt et al. [86] found that cybercrime victims needed to receive regular updates regarding the investigative process. Prislan et al. [115] asked people what they wanted to see post-reporting. The vast majority experienced cybercrime as a form of psychological aggression (e.g., stalking). Most people expected to see positive results if they reported to a friend in hope of getting advice (77.9 per cent) followed by the police (76 per cent).

Taxonomy of cybercrime reporting mechanisms

Baror et al. [7] suggest low levels of cybercrime reporting could be caused by a lack of clear criteria that victims can follow when reporting a crime. In fact, cybercrimes can be reported in one of three ways. We present a taxonomy of crime reporting mechanisms developed via inductive thematic analysis derived from the work of Robinson [120]. This taxonomy considers three different mechanisms for reporting: human-to-human (H2H), human-to-machine (H2M) and machine-to-machine (M2M). It should be noted that these individual categories are not independent because we cannot exclude the human element from any reporting mechanism. As such, human discretion is present in all categories, albeit to varying degrees.

H2H cybercrime reporting: H2H poses novel demands on the reporting infrastructure, which is accustomed to accepting complaints about traditional crime. Bidgoli et al. [9] present excerpts from 10 interviews of how some of their participants reported economic cybercrime using the H2H approach. One victim reported online shopping fraud to their bank to cancel their card but also to the clothing retailer Abercrombie & Fitch because the fraudulent website was mimicking the designer brand. A victim from another case study reported the computer virus to Dell customer service.

In another article, the author proposes a framework for businesses to share cybercrime knowledge [67]. The incentive for joining the voluntary initiative is the protection of the brand and service reputation. This is an example of businesses choosing to cooperate to tackle cybercrime because they realise that, while today it may be the competition that is attacked, tomorrow it could happen to them.

H2M cybercrime reporting: Heinonen et al. [58] describe reporting to the US Internet Crime Complaint Center (IC3), which receives complaints from members of the public via its online interface, but also from other organisations such as PayPal. The main strength of IC3 is that it provides helpful advice and tips on how people should protect themselves online. The main weakness is that IC3's work is insufficiently publicised to citizens.

Bidgoli et al. [10] streamlined a procedure for reporting cybercrime in PayPal. They produced a user-friendly reporting interface achieving two important goals: (1) it effectively connected reports within PayPal and outside PayPal with the relevant entities and (2) it raised awareness of cybercrime. The authors suggest that their pilot project be used by the industry and law enforcement authorities alike, even though it had not been adopted at the time of publication.

Mapimele and Mangoale [97] devised an H2M reporting platform called the Cybercrime Combating Platform (CP3). The CP3 algorithms allow users to search for compromises of their data. The system makes use of databases to trawl through online cybercrime activities. The databases it engages with are HavelBeenPwnd, Phishtank, Dshield and Breach Level Index.

An independent analysis of the ACORN system discovered that victims who reported to the ACORN online system experienced high levels of dissatisfaction [41]. Specifically, 77 per cent of complainants were unhappy with the outcome of their complaint. This is perhaps because the data captured by ACORN were of poor quality. Moreover, reports were stored in an unorganised text format, which made investigation problematic. This highlights the fact that cybercrime reporting should not be reduced to a mere transfer of information about an offence. Rather, everything related to the reporting interface should be designed with great care and in consultation with members of the public. In particular, the way the information is stored and subsequently analysed should be transparent to reporters [46] and helpful to law enforcement in terms of apprehending the perpetrator.

M2M cybercrime reporting: Carpineto and Romano [25] designed an automated pipeline with two machine learning stages to identify sellers of counterfeit luxurious clothes. This prototype was found to be more effective than established trustworthiness systems and non-expert humans.

Sheikhalishahi et al. [126] designed an automated analysis and classification of spam email pilot. The authors proposed an automatic method and resulting framework founded on pioneering categorical divisive clustering, which was successfully tested on a dataset retrieved from honeypots.

A technological development by Singh et al. [127] delved into identifying the difference between a phishing website and a classical web page. This task was challenging because of its semantic structure. Singh et al. managed to apply a phishing detection system by utilising deep learning mechanisms. The framework engages URLs via an application of the Convolutional Neural Network (CNN) with an accuracy of 98 per cent. The CNN is a type of deep learning algorithm capable of inputting, analysing, and differentiating between images. This system produces an outcome of its activity as a classification report where it classifies URLs as either 'phishing' or 'legitimate'. Currently, this system is just a prototype awaiting deployment in the wider cybersecurity stratosphere.

Policing cybercrime

The way cybercrime is policed, and perceptions related to such policing, is inextricably linked to cybercrime reporting. Hence it is worth discussing these aspects when we are considering cybercrime reporting. Policing of cybercrime has several dimensions, which we discuss now.

Connection between traditional and cybercrime: Cybercrime researchers debate the policing of cybercrime. Some attempt to adapt the principles from traditional crime policing onto cybercrime [64][65]. Others highlight the insufficiency of the cybercrime-related training of police forces [52][92][122]. This can be the result of a vicious circle whereby the police do not feel the same enthusiasm for pursuing cybercrime vs traditional crime, with which they are more familiar. This feeds into poor training standards and uptake. As a result, police are sometimes not equipped with the skills required to solve cybercrimes, which compromises their ability to pursue cybercriminals. Constables who engage in cybercrime training do indeed feel they are more prepared to deal with reported cybercrimes [12]. It has been found that face-to-face training is more effective than online training [30]. In addition, police forces would benefit from clear guidelines for cybercrime policing [12]. This is challenging because the English system is highly decentralised, which would create disagreement [72]. A human resources piece explored the new role of Digital Media Investigators (DMIs) in the UK [141]. The DMIs were created by up-skilling police officers to use technology to relieve the specialised teams from mundane tasks.

Challenges: Yadav et al. [147] reported on a case study of actual reporting related to an offender who had created abusive websites to target various actors in the art business and who had managed to extort over $3 million from his victims. The offender used multiple fake accounts, each of which had to be individually reported and linked to identify the single attacker.

Cross [42] talks about the problems of jurisdiction that police face, such as cases when the offender commits the crime from abroad against a home national. This makes it difficult to determine in which jurisdiction the crime took place.

Meanwhile, victims who report cybercrimes often have misconceptions about the various policing bodies in Australia. Cross [42] argues for greater transparency as well as more awareness-raising about the competencies and limitations of investigations.

Hadlington et al. [57] reported on interviews with 16 frontline police officers to examine the crucial aspects of cybercrime. The police staff said they continued to struggle with how to define cybercrime, with its constantly evolving nature and with the lack of appropriate training that would help them remain on the cutting edge. This is simply a new type of situation to which humanity needs time to adapt.

Models: Hunton [64] has developed a model for cybercrime policing. In Stage 1, the investigation of the offence starts. During Stage 2, the cybercrime is modelled. During Stage 3, a specialist assessment of what is known takes place. The purpose of Stage 4 is risk assessment. Investigation planning takes place as a part of Stage 5. The activities in Stage 6 are focused on handling data to keep evidence intact. Stage 7 is the carrying-out of the intervention and Stage 8 presents the results.

Roles: Hunton [65] identifies five policing roles within the investigation framework, organised based on a hierarchical power principle. The main strengths of this model are its functional specialisation and division of labour. The main weakness may be its rigidity, which can get in the way of accepting ideas from staff seen as lower on the pecking order.

Organisation: The police are navigating their activity in a sector that originally fell under the private sector [138]. As an example of the increasing controversy surrounding this merger, a trend has been observed whereby the police rely on the private sector to assist with cybercrime policing [72]. The UK police have evaluated the effectiveness of local policing [48]. In 2018, it was found that the force did not have an established line of communication with the National Crime Agency to pass on information about cybercrime. This may have changed some four years later. It is also worth noting examples that highlight the analytical capabilities of the police [124]. Lastly, it is worth mentioning 'influence policing', which is based around the digital footprint of at-risk Internet users. This is used to tailor deterrence ads [32].

Human resources: Obstacles to cybercrime policing can range from inter-agency competition to lack of resources to hire specialised staff [129]. An integral part of human resources is development. The London Met have rolled out the Ncalt training package, which is an online cybercrime training that has drawn some criticism as most police officers from the study felt under-trained [45]. Problems with training are a theme that re-emerges in research [53][122]. As a solution to this issue, a local police force boosted its expertise by hiring a former hacker [92]. Since 2003, the problem of cyber-fraud is also policed by vigilantes [21].

Jurisprudence: Current laws can challenge the policing of cybercrime [95]. Examples of challenges include using a fake social media profile to access information on social media, which is an offence under the Computer Misuse Act 1990. Moreover, specific national differences in legal definitions affect investigations and prosecutions. For example, not every group of organised criminals constitutes organised crime [85].

It has been argued that current legal approaches focus on conceptualising the systems of crime but fall behind offenders. What might be required is a bespoke force of dedicated online constables [121]. Lastly, Brexit has affected cybercrime jurisprudence. According to Stevens and O'Brein [131], Brexit affects the UK's capabilities in terms of policing and sentencing cybercrime by loosening ties with Europol and the European courts.

Community policing: It has been suggested that the links between the local police and communities could provide a network that can work to improve cybercrime reporting in a democratic way. Horgan et al. [62] suggest harnessing the power of community links with the police. It can only be added that the insider's view of the community police may be useful in filling many of the holes that are contained within cybercrime reports. This argument is in line with the favourable view that Wooff et al. [145][146] have towards community policing.

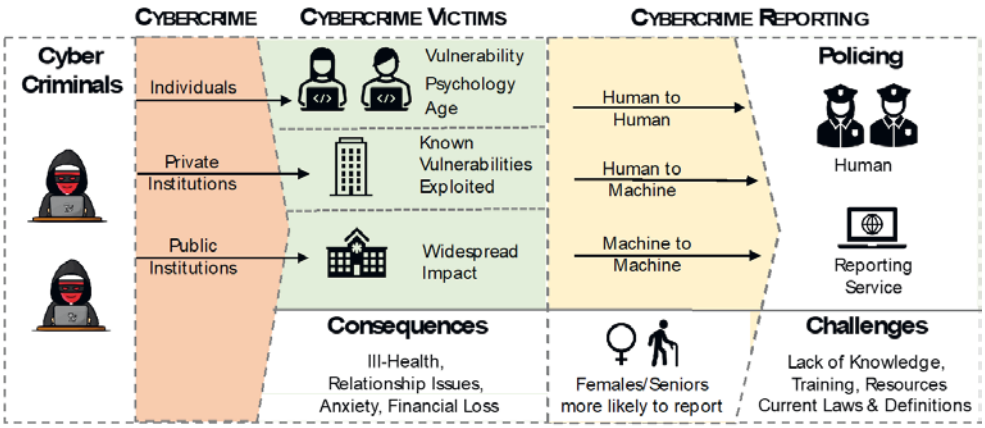
Choi and Lee [29] find that, in the UK, citizens are willing to participate in voluntary policing in their communities because it gives them a sense of authority, respect and recognition as well as a potential trajectory into a policing career. Hence, broader engagement with community resources could mobilise citizens to help their vulnerable neighbours stay safe from and report economic cybercrime.

Cybercrime reporting: final comments

In Australia, Cross [38] found that people's reporting experiences were often influenced by overestimation of the police force's capabilities. She coined this the 'CSI effect', based on the popular TV crime show. This means that people's expectations of the police are unrealistically high based on what they see on TV. On CSI, all investigations run smoothly and successfully. Consequently, victims are disappointed if their cases do not meet their expectations.

Figure 2 summarises this section. The next section addresses each of the research questions in turn.

Figure 2: Summary of the discussion in this section



4. Discussion

We now return to the original research questions.

RQ1: What characterises cybercrime in the UK?

The UK is clearly a target for cybercriminals, because of the high percentage of retail sales that occurs online in the UK (24.8 per cent [109]). This constitutes a massive opportunity for criminals, with the UK being in the top 10 countries targeted by cybercriminals. In 2021, the UK lost £1.3 billion to cybercrime and fraud [124], so there is a considerable need to maximise cybercrime reporting to ensure cybercriminals are apprehended and prosecuted.

RQ2: What is known about UK cybercrime victims?

It has been reported that one in five UK citizens has been a victim of cybercrime [54]. The same report found that Wales was the worst region for cybercrime, with Scotland least affected. However, these figures are based on data from Action Fraud and, since cybercrimes are underreported, the true figures could be much higher.

RQ3: What influences and deters cybercrime reporting in the UK?

Responsibilisation is a strategy applied by the UK government, which provides a great deal of advice on how to prevent cybercrime and expects citizens to follow this. In the UK, this strategy may well be contributing to underreporting of cybercrimes in three ways.

1. The responsibilisation agenda assigns responsibility to citizens to take care of their own cybersecurity. If people fall victim to an attack, they are like to blame themselves for it. Reporting the crime may be perceived as an admission of their own failure. This may discourage reporting.

2. Raising awareness of the need for cybercrime reporting, and disseminating ways of doing this, is not receiving the investment it should, leaving citizens confused.

3. The 'Cybercrime Reporting' section of the UK's Victim Support website [137] says: 'Please note that it's no longer possible to report fraud to your local police station – Action Fraud is the national fraud reporting service and is the starting point for any police investigation into your loss.' This is bound to be confusing, given that all other crimes are reported to the police.

Technological solutions are insufficient. If reporting were dependent merely on a technical system being available to collect reports, underreporting should not persist, since such systems exist in the UK. It has become clear, then, that merely making such systems available does not, in and of itself, encourage reporting. Bossler [12] argues that cybercrime reporting could be improved with a set of 'best practice' procedures and guidelines rolled out across the board. This idea has been questioned by Johnson et al. [72] because the decentralisation of the English force makes this infeasible. In contrast, the centralised Scottish force may be able to test this idea [103]. Even so, merely having such a set of processes and procedures does not guarantee that citizens will engage in them.

Responses to reports must be seen as effective. If people report an attack and do not believe the police have taken their cybercrime report seriously or attempted to apprehend the criminal, they may well not report further cybercrimes.

An oft-neglected dimension to reporting is related to societal norms and context. Such societal aspects are likely to play an important role in the compilation of accurate reports. Previous research has also supplied inferential evidence to suggest that cybercrime reporting should be treated as a social interaction [80], which could improve reporting by vulnerable populations [98].

People may well believe they deserve to lose money because they have not followed the provided advice. They may also keep quiet if they think their peers would think less of them if they have fallen for a con.

We must consider all these influences if we want to encourage cybercrime reporting – and not only the availability, accessibility and usability of the technical systems that people can use to report cybercrimes.

Research implications

There is a clear need to develop reporting systems that people will be more likely to use. It would be helpful to model cybercrime reporting, and its deterrents, to better understand the factors that encourage and/or discourage cybercrime reporting. Once the influential factors have been identified, the next step would be to identify interventions to mitigate the deterring factors and to enhance those factors that motivate victims to report cybercrimes.

5. Conclusion

A systematic literature review was conducted to explore questions around UK cybercrime, to answer the questions: What characterises cybercrime in the UK? What is known about UK cybercrime victims? and What influences and deters cybercrime reporting in the UK?

We discovered that UK is experiencing increasing levels of cybercrime, which has been exacerbated by the pandemic lockdowns. UK citizens tend to shop more online than do citizens of other countries, meaning that the potential to fall victim to cybercrimes is high. However, the full extent of UK citizen victimisation is not well understood, owing to cybercrime underreporting. The UK's responsibilisation agenda may be contributing to low levels of cybercrime reporting: reporting is likely to remain low if victims blame themselves for their victimisation. To improve reporting prevalence, we must focus on all dimensions of underreporting systems, all the way from technical to societal deterrents.

References

[1] Abdulai, M.A. (2020) 'Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud'. *International Journal of Cyber Criminology* 14(1): 157–174. https://doi.org/10.5281/zenodo.3749468

[2] Action Fraud (nd) '24 Hour Live Cyber Reporting for Businesses'. www.actionfraud.police.uk/

[3] Akdemir, N. and Lawless, C.J. (2020) 'Exploring the Human Factor in Cyber-enabled and Cyberdependent Crime Victimisation: A Lifestyle Routine Activities Approach'. *Human Factor in Cybercrime Victimisation* 30(6): 1665–1687. https://doi.org/10.1108/INTR-10-2019-0400

[4] Alzubaidi, A. (2021) 'Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia'. *Heliyon* 7(1): e06016.

[5] Arora, B. (2016) 'Exploring and Analyzing Internet Crimes and Their Behaviours'. *Perspectives in Science* 8: 540–542. https://doi.org/10.1016/j.pisc.2016.06.014

[6] Bana, A. and Hertzberg, D. (2015) 'Data Security and the Legal Profession: Risks, Unique Challenges and Practical Considerations'. *Business International Law* 16(3): 247–264.

[7] Baror, S.O., Ikuesan, R.A. and Venter, H.S. (2020) 'A Defined Digital Forensic Criteria for Cybercrime Reporting'. Proceedings of the 15th International Conference on Cyber Warfare and Security: 617–626.

[8] Bennett, R.R. and Wiegand, R.B. (1994) 'Observations on Crime Reporting in a Developing-Nation'. *Criminology* 32(1): 135–148. https://doi.org/10.1111/j.1745-9125.1994.tb01149.x

[9] Bidgoli, M., Knijnenburg, B.P. and Grossklags, J. (2016) 'When Cybercrimes Strike Undergraduates'. *eCrime Researchers Summit, eCrime*: 42–51. https://doi.org/10.1109/ECRIME.2016.7487948

[10] Bidgoli, M., Knijnenburg, B.P., Grossklags, J. and Wardman, B. (2019) 'Report Now. Report Effectively. Conceptualizing the Industry Practice for Cybercrime Reporting'. *eCrime Researchers Summit, eCrime*: 1–10. https://doi.org/10.1109/eCrime47957.2019.9037577

[11] Böhme, R. (2013) *The Economics of Information Security and Privacy*. Heidelberg, New York, Dordrecht, London: Springer.

[12] Bossler, A.M., Holt, T.J., Cross, C. and Burruss, G.W. (2020) 'Policing Fraud in England and

Wales: Examining Constables' and Sergeants' Online Fraud Preparedness'. *Security Journal* 33: 311–328. https://doi.org/10.1057/s41284-019-00187-5

[13] Boyce, C.J. and Wood, A.M. (2010) 'Money or Mental Health: The Cost of Alleviating Psychological Distress with Monetary Compensation Versus Psychological Therapy'. *Health Economics, Policy and Law* 5(4): 509–516. https://doi.org/10.1017/S1744133109990326

[14] Bowles, R., Garcia Reyes, M. and Garoupa, N. (2009) 'Crime Reporting Decisions and the Costs of Crime'. *European Journal on Criminal Policy and Research* 15(4): 365–377. https://doi.org/10.1007/s10610-009-9109-8

[15] Brenner, S.W. (2007) 'At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare'. *Journal of Criminal Law and Criminology* 97(2): 379–476. https://www.jstor.org/stable/40042831

[16] Brown, K.J. and Gordon, F. (2022) 'Improving Access to Justice for Older Victims of Crime by Reimagining Conceptions of Vulnerability'. *Ageing and Society* 42(3): 614–631. https://doi.org/10.1017/S0144686X20001051

[17] Buil-Gil, D. and Saldana-Taboada, P. (2021) 'Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime'. *Deviant Behavior* 43(12): 1–18. https://doi.org/10.1080/01639625.2021.1988760

[18] Buil-Gil, D. & Zeng, Y. (2021) 'Meeting You Was a Fake: Investigating the Increase in Romance Fraud during COVID-19'. *Journal of Financial Crime* 29(2): 460–475. https://doi.org/10.1108/JFC-02-2021-0042

[19] Buil-Gil, D., Miro-Llinares, F., Moneva, A. et al. (2021) 'Cybercrime and Shifts in Opportunities during COVID-19: A Preliminary Analysis in the UK'. *European Societies* 23(S1): S47–S49. https://doi.org/10.1080/14616696.2020.1804973

[20] Burgard, A. and Schlembach, C. (2013) 'Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet'. *International Journal of Cyber Criminology* 7(2): 112.

[21] Button, M. and Whittaker, J. (2021) 'Exploring the Voluntary Response to Cyber-Fraud: From vigilantism to responsibilisation'. *International Journal of Law, Crime and Justice* 66: 100482. https://doi.org/10.1016/j.ijlcj.2021.100482

[22] Button, M., McNaughton Nicholls, C., Kerr, J. and Owen, R. (2014) 'Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology* 47(3): 391–408. https://doi.org/10.1177/0004865814521224

[23] Böhme, R. and Moore, T. (2012) 'How Do Consumers React to Cybercrime?' eCrime Researchers Summit, Las Croabas, Puerto Rico, 22–25 October. https://doi.org/10.1109/eCrime.2012.6489519

[24] Caneppele, S. and Aebi, M.F. (2019) 'Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes'. *Policing: A Journal of Policy and Practice* 13(1): 66–79. https://doi.org/10.1093/police/pax055

[25] Carpineto, C. and Romano, G. (2020) 'An Experimental Study of Automatic Detection and Measurement of Counterfeit in Brand Search Results'. *ACM Transactions on the Web* 14(2): 1–35. https://doi.org/10.1145/3378443

[26] CFS (2018) 'Number of Cybercrime Victims Falls'. *Computer Fraud & Security* 5: 20. https://doi.org/10.1016/S1361-3723(18)30045-9

[27] Chawki, M. (2005) 'A Critical Look at the Regulation of Cybercrime'. *The ICFAI Journal of Cyberlaw* IV(4).

[28] Cheng, C., Chau, M.C.L. and Chan, M.L. (2018) 'A Social Psychological Analysis of the Phenomenon of Underreporting Cybercrimes and the Concomitant Underlying Factors: Three Real Local Case Studies'. *Communications Association of Hong Kong*.

[29] Choi, K. and Lee, J. (2016) 'Citizen Participation in Community Safety: A Comparative Study of Community Policing in South Korea and the UK'. *Policing & Society* 26(2): 165–184. https://doi.org/10.1080/10439463.2014.922087

[30] Cockroft, T., Shan-A-Khuda, M., Schreuders, Z.C. and Trevorrow, P. (2021) 'Police Cybercrime Training: Perceptions, Pedagogy, and Policy'. *Policing: A Journal of Policy and Practice* 15(1): 15–33. https://doi.org/10.1093/police/pay078

[31] Collier, D., Thomas, D.R., Clayton, R. and Hutchings, A. (2019) 'Booting the Booters: Evaluating the Effects of Police Interventions in the Market for Denial-of-Service Attacks'. Proceedings of the Internet Measurement Conference, October. https://doi.org/10.1145/3355369.3355592

[32] Collier, D., Thomas, D.R., Clayton, R. et al. (2021) 'Influence, Infrastructure, and Recentering Cybercrime Policing: Evaluating Emerging Approaches to Online Law Enforcement through a Market of Cybercrime Services'. *Policing & Society. An International Journal of Research and Policy* 32(1): 103–124. https://doi.org/10.1080/10439463.2021.1883608

[33] Connolly, A.Y. and Borrison, H. (2020) 'Your Money or Your Business'. Proceedings of the 41st International Conference on Information Systems. Association for Information Systems. https://aisel.aisnet.org/icis2020/cyber_security_privacy/cyber_security_privacy/6

[34] Connolly, A.Y., Wall, D.S., Lang, M. and Oddson, B. (2020) 'An Empirical Study of Ransomware Attacks on Organizations: An Assessment of Severity and Salient Factors Affecting Vulnerability'. *Journal of Cybersecurity* 6(1): tyaa023. https://doi.org/10.1093/cybsec/tyaa023

[35] Correia, S.G. (2019) 'Responding to Victimisation in a Digital World: A Case Study of Fraud and Computer Misuse Reported in Wales'. *Crime Science* 8(4): 1–12. https://doi.org/10.1186/s40163-019-0099-7

[36] Correia, S.G. (2020) 'Patterns of Online Repeat Victimisation and Implications for Crime Prevention'. 2020 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA. https://doi.org/10.1109/eCrime51433.2020.9493258

[37] Correia, S.G. (2022) 'Making the Most of Cybercrime and Fraud Crime Report Data: A Case Study of UK Action Fraud'. *International Journal of Population Data Science* 7(1): 9. https://doi.org/10.23889/ijpds.v7i1.1721

[38] Cross, C. (2018) 'Expectations vs. Reality: Responding to Online Fraud across the Fraud Justice Network'. *International Journal of Law, Crime and Justice* 55: 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

[39] Cross, C. (2019) 'Is Online Fraud Just Fraud? Examining the Efficacy of the Digital Divide'. *Journal of Criminological Research, Policy and Practice* 5(2): 120–131. https://doi.org/10.1108/JCRPP-01-2019-0008

[40] Cross, C. (2019) 'Responding to Individual Fraud'. In E.R. Leukfeldt and T.J. Holt (eds) *The Human Factor of Cybercrime* (pp. 359–388). Abingdon: Routledge.

[41] Cross, C. (2020) 'Reflections on the Reporting of Fraud in Australia'. *Policing* 43(1): 49–61. https://doi.org/10.1108/PIJPSM-08-2019-0134

[42] Cross, C. (2020) '"Oh We Can't Actually Do Anything about That": The Problematic Nature of Jurisdiction for Online Fraud Victims'. *Criminology and Criminal Justice* 20(3): 358–375.

[43] Cross, C. (2021) 'Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons'. *The Journal of Adult Protection* 23(2): 98–109. https://doi.org/10.1108/JAP-08-2020-0035

[44] Cross, C. and Kelly, M. (2016) 'The Problem of "White Noise": Examining Current Prevention Approaches to Online Fraud'. *Journal of Financial Crime* 23(4): 806–818. https://doi.org/10.1108/JFC-12-2015-0069

[45] Cross, C., Holt, T., Powell, A. and Wilson, M. (2018) 'Responding to Cybercrime: Results of a Comparison between Community Members and Police Personnel'. *Trends and Issues in Crime and Criminal Justice* 635: 1–20.

[46] Das, A., Nayak, J. Naik, B. and Ghosh, U. (2021) 'Generation of Overlapping Clusters Constructing Suitable Graph for Crime Report Analysis'. *Future Generation Computer Systems: The International Journal Of EScience* 118: 339–357. https://doi.org/10.1016/j.future.2021.01.027

[47] Department for Digital, Culture, Media & Sport (2022) 'Cyber Security Breaches Survey'. www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

[48] Doig, A. (2018) 'Implementing National Policing Agendas and Strategies for Fraud at Local Level'. *Journal of Financial Crime* 25(4): 984–996. https://doi.org/10.1108/JFC-04-2017-0027

[49] Donegan, M. (2019) 'Crime Script for Mandate Fraud'. *Journal of Money Laundering* 22(4): 770–781. https://doi.org/10.1108/JMLC-03-2019-0025

[50] Elkin, M. (2022) 'Crime in England and Wales: Year Ending December 2021'. www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2021#computer-misuse

[51] Fisher, J. (2008) 'The UK's Faster Payment Project: Avoiding a Bonanza for Cybercrime Fraudsters'. *Journal of Financial Crime* 15(2): 155–164. https://doi.org/10.1108/13590790810866872

[52] Fleming, J. (2022) 'Director GCHQ Speaks at CyberUK 2022'. GCHQ speech, 10 May www.gchq.gov.uk/speech/cyberuk2022

[53] Forouzan, H. Jahankhani, H. and McCarthy, J. (2018) 'An Examination into the Level of Training, Education and Awareness among Frontline Police Officers in Tackling Cybercrime within the Metropolitan Police Service'. In H. Jahankhani (ed.) *Cyber Criminology. Advanced Sciences and Technologies for Security Applications* (pp. 307–323). Amsterdam: Springer.

[54] Fox, H. (2022) 'The Worst UK Regions for Cybercrime'. *Ocean Finance News*, 22 April. www.oceanfinance.co.uk/blog/the-worst-uk-regions-for-cybercrime/

[55] Goudriaan, H., Wittebrood, K. and Nieuwbeerta, P. (2006) 'Neighbourhood Characteristics and Reporting Crime Effects of Social Cohesion, Confidence in Police Effectiveness and Socio-Economic Disadvantage'. *British Journal of Criminology* 46(4): 719-742. https://doi.org/10.1093/bjc/azi096

[56] Gutierrez C.M. and Kirk D.S. (2017) 'Silence Speaks: The Relationship between Immigration and the Underreporting of Crime'. *Crime Delinq.* 63(8): 926–950. https://doi.org/10.1177/0011128715599993

[57] Hadlington, L., Lumsden, K. Black, A. and Ferra, F. (2021) 'A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime'. *Policing: A Journal of Policy*

and Practice 15(1): 34–43. https://doi.org/10.1093/police/pay090

[58] Heinonen, J.A., Holt, T.J. and Wilson, J.M. (2012) 'Product Counterfeits in the Online Environment: An Empirical Assessment of Victimization and Reporting Characteristics'. *International Criminal Justice Review* 22(4): 353–371.

[59] HMICFRS (2020) 'A Call for Help: Police Contact Management through Call Handling and Control Rooms in 2018/19'. Technical Report.

[60] Holt, T.J., VanWilsem, J., Van deWeijer, S.G.A. and Leukfeldt, E.R. (2018) 'Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization'. *Social Science Computer Review* 38(2). https://doi.org/10.1177/0894439318805067

[61] Horgan, S. (2021) 'The Reality of "Cyber Security Awareness": Findings and Policy Implications for Scotland'. Scottish Justice Fellowship Briefing Paper.

[62] Horgan, S., Collier, B. Jones, R. and Shepherd, L. (2021) 'Re-territorialising the Policing of Cybercrime in the Post-COVID-19 Era: Towards a New Vision of Local Democratic Cyber Policing'. *Journal of Criminal Psychology* 11(3): 222–239. https://doi.org/10.1108/JCP-08-2020-0034

[63] Hunter, P. (2008) 'UK Shadow Home Secretary Victim of Online Card Fraud'. *Computer Fraud & Security* 6: 4. https://doi.org/10.1016/S1361-3723(08)70094-0

[64] Hunton, P. (2011) 'A Rigorous Approach to Formalising the Technical Investigation Stages of Cybercrime and Criminality within a UK Law Enforcement Environment'. *Digital Investigation* 7(3): 105–113. https://doi.org/10.1016/j.diin.2011.01.002

[65] Hunton, P. (2012) 'Managing the Technical Resource Capability of Cybercrime Investigation: A UK Law Enforcement Perspective'. *Public Money and Management* 32(3): 225–232. https://doi.org/10.1080/09540962.2012.676281

[66] Hutchings, A. and Pastrana, S. (2019) 'Understanding eWhoring'. 4th IEEE European Symposium on Security and Privacy, Stockholm, 17–19 June. https://doi.org/10.1109/EuroSP.2019.00024

[67] Ismail, U. (2020) 'The Nigeria Police Force and Cybercrime Policing: An Appraisal'. *Dutse Journal of Criminology and Security Studies* 1: 78–88.

[68] ISACA (2019) 'State of Cybersecurity 2019 Part 2: Current Trends in Attacks, Awareness and Governance'. Press Release, November.

[69] Jaishankar, K. (2020) 'Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology'. In J. Joseph (ed.) *An International Perspective on Contemporary Developments in Victimology* (pp. 3-19). Heidelberg, New York, Dordrecht, London: Springer.

[70] Jhaveri, M.H. Cetin, O. Gañán, C. et al. (2017) 'Abuse Reporting and the Fight against Cybercrime'. *Comput. Surveys* 49(4): 1–27. https://doi.org/10.1145/3003147

[71] Johnson, B. (2022) 'Improving the State of Cyber Security in the Public Sector'. Government Business. https://governmentbusiness.co.uk/features/improving-state-cyber-security-public-sector

[72] Johnson, D., Faulkner, E., Meredith, G. and Wilson, T.J. (2020) 'Police Functional Adaptation to the Digital or Post Digital Age: Discussions with Cybercrime Experts'. *Journal of Criminal Law* 84(5): 427–450.

[73] Johnson, J. (2021) 'Cyber Crime and UK Consumers: Statistics & Facts'. www.statista.com/topics/8416/cyber-crime-and-ukconsumers/

[74] Johnson, J. (2021) 'Cyber Crime and UK Consumers – Statistics & Facts'. Statista. https://www.statista.com/topics/8416/cyber-crime-and-uk-consumers/

[75] Jones, C. (2022) 'Ransomware Strikes Scottish Mental Health Charity. *ITPro*, 21 March. www.itpro.co.uk/security/ransomware/367137/scottish-association-mental-health-ransomware

[76] Jones, H.S., Towse, J.N., Race, N. and Harrison, T. (2019) 'Email Fraud: The Search for Psychological Predictors of Susceptibility'. *Plos One* 14(1): e0209684. https://doi.org/10.1371/journal.pone.0209684

[77] Junger-Tas, J. and Marshall, I.H. (1999) 'The Self-Report Methodology in Crime Research'. *Crime and Justice* 25: 291-367. https://doi.org/10.1086/449291

[78] Kaur, M. and Saini, M. (2022) 'Indian Government Initiatives on Cyberbullying: A Case Study on Cyberbullying in Indian Higher Education Institutions'. *Education and Information Technologies* 46(3): 1–35. https://doi.org/10.1007/s10639-022-11168-4

[79] Kemp, S. Buil-Gil, D., Moneva, A. et al. (2021) 'Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends during COVID-19'. *Journal Of Contemporary Criminal Justice* 37(4): 480–501. https://doi.org/10.1177/10439862211027986

[80] Kieckhaefer, J.M., Vallano, J.P. and Compo, N.S. (2014) 'Examining the Positive Effects of Rapport Building: When and Why Does Rapport Building Benefit Adult Eyewitness Memory?' *Memory* 22(8): 1010–1023. https://doi.org/10.1080/09658211.2013.864313

[81] Kuo, T.L. (2022) 'Criminal Victimisation in Taiwan: An Opportunity Perspective'. Doctoral dissertation, University College London.

[82] Langton, L., Berzofsky, M., Krebs, C. and Smiley-McDonald, H. (2012) 'Victimizations Not Reported to the Police, 2006-2010'. Washington, DC: US Department of Justice, Office of Justice Programs, Bureau of Justice Statistics.

[83] Lavorgna, A. (2019) 'Cyber-Organised Crime. A Case of Moral Panic?' *Trends in Organized Crime* 22: 357–374. https://doi.org/10.1007/s12117-018-9342-y

[84] Leukfeldt, E.R. Kleemans, E.R. and Stol, W.P. (2017) 'Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis'. *Crime, Law and Social Change* 67: 39–53. https://doi.org/10.1007/s10611-016-9663-1

[85] Leukfeldt, E.R., Lavorgna, A. and Kleemans, E.R. (2017) 'Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime'. *European Journal on Criminal Policy and Research* 23(33): 287–300. https://doi.org/10.1007/s10610-016-9332-z

[86] Leukfeldt, E.R., Notte, R.J. and Malsch, M. (2020) 'Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes'. *Victims & Offenders* 15(1): 60–77. https://doi.org/10.1080/15564886.2019.1672229

[87] Levi, M. (2017) 'Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues'. *Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change. Crime, Law and Social Change* 67: 3–20. https://doi.org/10.1007/s10611-016-9645-3

[88] Levi, M., Doig, A. Gundur, R. Wall, D. and Williams, M. (2017) 'Cyberfraud and the Implications for Effective Risk-Based Responses: Themes from UK Research'. *Crime, Law and Social Change* 67(1): 77–96. https://doi.org/10.1007/s10611-016-9648-0

[89] Levi, M. and Smith, R.G. (2021) 'Fraud and Pandemics'. *Journal of Financial Crime* 29(2): 413–432. https://doi.org/10.1108/JFC-06-2021-0137

[90] Levi, M. and Williams, M.L. (2013) 'Multi-Agency Partnerships in Cybercrime Reduction: Mapping the UK Information Assurance Network Cooperation Space'. *Information Management & Computer Security* 21(5): 420–443. https://doi.org/10.1108/IMCS-04-2013-0027

[91] Lord, J. (2016) 'Fifty Shades of Fraud'. *Computer Fraud & Security* 6: 14–16. https://doi.org/10.1016/S1361-3723(15)30047-6

[92] Loveday, B. (2018) 'The Shape of Things to Come. Reflections on the Potential Implications of the 2016 Office of National Statistics Crime Survey for the Police Service of England and Wales'. *Policing: A Journal of Policy and Practice* 12(4): 398–409. https://doi.org/10.1093/police/pax040

[93] Lovet, G. (2009) 'Fighting Cybercrime: Technical, Juridical and Ethical Challenges'. Virus Bulletin Conference, September. www.virusbulletin.com/conference/vb2009/abstracts/fighting-cybercrime-technical-juridical-and-ethical-challenges/

[94] Lufkin, B. (2020) 'The Curious Origins of Online Shopping'. BBC, 27 July. www.bbc.com/worklife/article/20200722-the-curious-origins-of-online-shopping

[95] Lyle, A. (2016) 'Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism'. In *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications* (pp. 277–294). Amsterdam: Springer.

[96] Maltz, M.D. (1977) 'Crime Statistics: A Historical Perspective'. *Crime & Delinquency* 23(1): 32–40.

[97] Mapimele, F. and Mangoale, B. (2019) 'The Cybercrime Combating Platform'. In N. van der Waag-Cowling and L. Leenen (eds) *14th International Conference on Cyber Warfare and Security* (pp. 237–242). Stellenbosch.

[98] McMurdie, C. (2016) 'The Cybercrime Landscape and Our Policing Response'. *Journal of Cyber Policy* 1(1): 85–93. https://doi.org/10.1080/23738871.2016.1168607

[99] Middle East Post Box (nd) '10 Countries Whose Residents Are Most Enticing For Cybercriminals'. https://middleeastpostbox.com/10-countries-whose-residents-are-most-enticing-for-cybercriminals/

[100] Milmo, D. (2022) 'NHS Ransomware Attack: What Happened and How Bad Is It?' *The Guardian*, 11 August. www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

[101] Milne, R. and Bull, R. (2001) 'Interviewing Witnesses with Learning Disabilities for Legal Purposes'. *British Journal of Learning Disabilities* 29: 93–97. https://doi.org/10.1046/j.1468-3156.2001.00139.x

[102] Monteith, S., Bauer, M., Alda, M. et al. (2021) 'Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry'. *Current Psychiatry Reports* 23(4): 1–9. https://doi.org/10.1007/s11920-021-01228-w

[103] Murray, K. and Harkin, D. (2017) 'Policing in Cool and Hot Climates: Legitimacy, Power and the Rise and Fall of Mass Stop and Search in Scotland'. *British Journal of Criminology* 57(4): 885–905. https://doi.org/10.1093/bjc/azw007

[104] Nasi, M., Oksanen, A., Keipi, T. and Rasanen, P. (2015) 'Cybercrime Victimization among Young People: A Multi-Nation Study'. *Journal of Scandinavian Studies in Criminology and Crime Prevention* 16(2): 203–210. https://doi.org/10.1080/14043858.2015.1046640

[105] NCA (2020) *National Strategic Assessment of Serious and Organised Crime*. London: NCA. www.nationalcrimeagency.gov.uk/news/nsa2020

[106] NHS (nd) 'Prevention Is the Best Defence'. https://nhsfraudandsecurity.co.uk/security-information/cyber-crime

[107] ONS (2021) 'Crime in England and Wales QMI'. www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/methodologies/crimeinenglandandwalesqmi

[108] ONS (2021) 'Crime in England and Wales, Year Ending December 2020—Appendix Tables'. www.ons.gov.uk/releases/crimeinenglandandwalesyearendingdec2020

[109] ONS (2021, February 17) 'Internet Sales as a Percentage of Total Retail Sales'. www.ons.gov.uk/businessindustryandtrade/retailindustry/timeseries/j4mc/drsi

[110] Parker, D.B. (1998) *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons, Inc.

[111] Pastrana, S. Hutchings, A., Thomas, D.R. and Tapiador, J. (2019) 'Measuring eWhoring'. Proceedings of the Internet Measurement Conference: 463–477.

[112] Pickering, C., Grignon, J., Steven, R. et al. (2015) 'Publishing Not Perishing: How Research Students Transition from Novice to Knowledgeable Using Systematic Quantitative Literature Reviews'. *Studies in Higher Education* 40(10): 1756–1769. https://doi.org/10.1080/03075079.2014.914907

[113] Police Scotland and Scottish Police Authority (2020) *Cyber Strategy 2020: Keeping People Safe in the Digital World*. www.scotland.police.uk/spa-media/vz0d3v31/cyber-strategy.pdf

[114] Popham, J., McCluskey, M., Ouellet, M. and Gallupe, O. (2020) 'Exploring P-reported Cybercrime in Canada: Variation and Correlates'. *Policing* 43(1): 35–48. https://doi.org/10.1108/PIJPSM-08-2019-0128

[115] Prislan, K., Bernik, I., Mesko, G. et al. (2019) 'Cybercrime Victimization and Seeking Help: A Survey of Students in Slovenia'. *Third Central European Cybersecurity Conference* 1–2. https://doi.org/10.1145/3360664.3360731

[116] Protrka, N. (2021) 'Cybercrime', in M. Roycroft and L. Brine (eds) *Modern Police Leadership* (pp. 143-155). Basingstoke: Palgrave Macmillan.

[117] Reep-van den Bergh, C.M.M. and Junger, M. (2018) 'Victims of Cybercrime in Europe: A Review of Victim Surveys'. *Crime Science* 7(1): 1–15. https://doi.org/10.1186/s40163-018-0079-3

[118] Renaud, K., Flowerday, S., Warkentin, M. et al. (2018) 'Is the Responsibilisation of the Cyber Security Risk Reasonable and Judicious?' *Computers & Security* 78: 198–211. https://doi.org/10.1016/j.cose.2018.06.006

[119] Renaud, K., Orgeron, C., Warkentin, M. and French, P.E. (2020) 'Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China'. *Public Administration Review* 80(4): 577–589. https://doi.org/10.1111/puar.13210

[120] Robinson, O.C. (2022) 'Conducting Thematic Analysis on Brief Texts: The Structured Tabular Approach'. *Qualitative Psychology* 9(2): 194–208. https://doi.org/10.1037/qup0000189

[121] Sampson, F. (2014) 'Cyberspace: The New Frontier for Policing?' In B. Akhgar, A. Staniforth and F. Bosco (eds) *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 1–10). Amsterdam: Syngress.

[122] Schreuders, Z.C., Cockroft, T., Elliott, J. et al. (2020) 'Needs Assessment of Cybercrime and

Digital Evidence in a UK Police Force'. *International Journal of Cyber Criminology* 14(1): 316–340. https://doi.org/10.5281/zenodo.3757271

[123] Scroxton, A. (2021) 'Fraud and Cyber Crime Still Vastly Under-Reported'. *Computer Weekly*, 4 February. www.computerweekly.com/news/252495844/Fraud-and-cyber-crime-still-vastly-under-reported

[124] Scroxton, A. (2021) 'UK Loses £1.3bn to Fraud and Cyber Crime So Far This Year'. *Computer Weekly*, 25 August. www.computerweekly.com/news/252505825/UK-loses-13bn-to-fraud-and-cyber-crime-so-far-this-year

[125] Shan-A-Khuda, M. and Schreuders, Z.C. (2019) 'Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis'. *International Journal of Cyber Criminology* 13(2): 493–510. https://doi.org/10.5281/zenodo.3708924

[126] Sheikhalishahi, M., Saracino, A., Martinelli, F. et al. (2020) 'Digital Waste Disposal: An Automated Framework for Analysis of Spam Emails'. *International Journal of Information Security* 19(5): 499–522. https://doi.org/10.1007/s10207-019-00470-x

[127] Singh, S., Singh, M.P. and Pandey, R. (2020) 'Phishing Detection from URLs Using Deep Learning Approach'. Proceedings of the 2020 5th International Conference on Computing, Communication and Security: 1–4.

[128] Singh, S.K. and Rastogi, N. (2018) 'Role of Cyber Cell to Handle Cyber Crime within the Public and Private Sector: An Indian Case Study'. 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages. https://doi.org/10.1109/IoT-SIU.2018.8519884

[129] Sommer, P. (2017) 'The Future for the Policing of Cybercrime'. In D. Wall (ed.) *Crime and Deviance in Cyberspace* (pp. 8–12). Abingdon: Routledge.

[130] Statista (2023) 'Percentage of Internet Users in Selected Countries Who Have Ever Experienced Any Cyber Crime from November to December 2021'. www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries/

[131] Stevens, T. and O'Brein, K. (2019) 'Brexit and Cyber Security'. *The RUSI Journal* 164(3): 22–30. https://doi.org/10.1080/03071847.2019.1643256

[132] Tarling, R. and Morris, K. (2010) 'Reporting Crime to the Police'. *British Journal of Criminology* 50(3): 474–490. https://doi.org/10.1093/bjc/azq011

[133] Tcherni, M., Davies, A., Lopes, G. and Lizotte, A. (2016) 'The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?' *Justice Quarterly* 33(5): 890–911. https://doi.org/10.1080/07418825.2014.994658

[134] Tidy, J. (2022) 'NHS IT Supplier Held to Ransom by Hackers'. BBC News, 11 August. www.bbc.co.uk/news/technology-62506039

[135] Van de Weijer, S.G.A. and Leukfeldt, E.R. (2017) 'Big Five Personality Traits of Cybercrime Victims'. *Cyberpsychology, Behavior, and Social Networking* 20(7): 407–412. https://doi.org/10.1089/cyber.2017.0028

[136] Van de Weijer, S.G.A., Leukfeldt, E.R. and van der Zee, S. (2020) 'Reporting Cybercrime Victimization: Determinants, Motives, and Previous Experiences'. *Policing: An International Journal* 43(1): 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

[137] Victim Support (nd) 'Cybercrime and Online Fraud'. www.victimsupport.org.uk/crime-info/types-crime/cyber-crime/

[138] Wall, D.S. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'. *International Review of Law, Computers & Technology* 22(1-2): 45–63. https://doi.org/10.1080/13600860801924907

[139] Wall, D.S. (2013) 'Policing Identity Crimes'. *Policing and Society* 23(4): 437–460. https://doi.org/10.1080/10439463.2013.780224

[140] Whitty, M.T. (2018) 'Do You Love Me? Psychological Characteristics of Romance Scam Victims'. *Cyberpsychology, Behavior, and Social Networking* 21(2): 105–109. https://doi.org/10.1089/cyber.2016.0729

[141] Wilson, D., Patterson, A., Powell, G. and Hembury, R. (2006) 'Fraud and Technology Crimes. Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and Administrative Sources'. London: Home Office.

[142] Wilson-Kovacs, D. (2021) 'Digital Media Investigators: Challenges and Opportunities in the Use of Digital Forensics in Police Investigations in England and Wales'. *Policing: An International Journal* 44(4): 669–682. https://doi.org/10.1108/PIJPSM-02-2021-0019

[143] Wirth, A. (2018) 'The Times They Are a-Changin': Part Two'. *Biomedical Instrumentation & Technology* 52(3): 236–240. https://doi.org/10.2345/0899-8205-52.3.236

[144] Wolff, J. (2018) 'The Real Reasons Why Cybercrimes May Be Vastly Undercounted'. Slate, 12 February. https://slate.com/technology/2018/02/the-real-reasons-why-cybercrimes-are-vastly-underreported.html

[145] Wooff, A. (2015) 'Relationships and Responses: Policing Anti-Social Behaviour in Rural Scotland'. *Journal of Rural Studies* 39: 287–295. https://doi.org/10.1016/j.jrurstud.2014.11.003

[146] Wooff, A. (2016) '"Soft" Policing in Rural Scotland'. *Policing* 11(2):123–131. https://doi.org/10.1093/police/paw031

[147] Yadav, H., Gautam, S., Rana, A. et al. (2021) 'Various Types of Cybercrime and Its Affected Area'. In J. Tavares, S. Chakrabati, A. Bhattacharya and S. Ghatak (eds) *Emerging Technologies in Data Mining and Information Security* (pp. 305–315). Singapore: Springer. https://doi.org/10.1007/978-981-15-9774-9_30

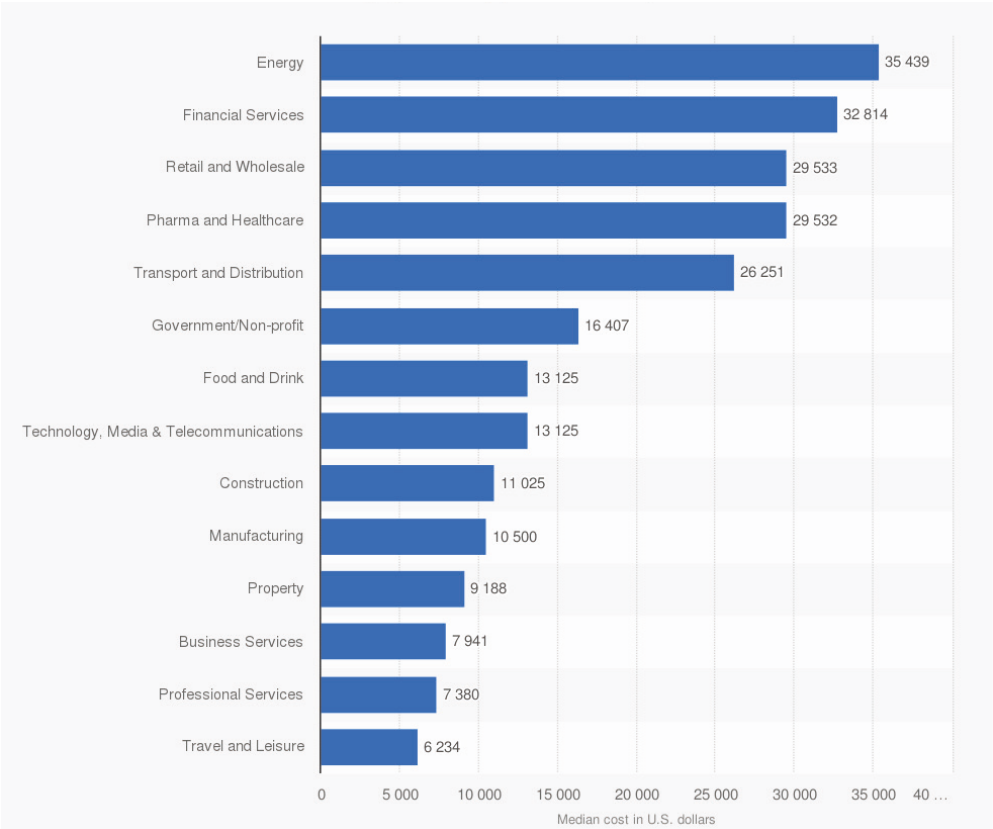
Appendix

Table A1. Annotated analysis of non-UK articles revealed via the systematic method (based on generalisability and/or universality assumptions)

3.1 CYBERCRIME: Annotation of non-UK references	
Reference	References' connection to the UK
[43]	'COVID-19' and 'older persons' pertain to the UK
[66][111]	'e-whoring' is a crime occurring globally including in the UK
[128]	Study focused on 'classification' transferable onto the UK
3.2 UK CYBERCRIME VICTIMS: Annotation of non-UK references	
Reference	References' connection to the UK
[13]	Victims' psychotherapy needs extend onto the UK
[45]	Victim-blaming may impede cybercrime reporting in the UK
[86]	An analysis of victims' needs extends onto the UK
[36]	'Repeat victimisation' pertains to the UK
[135]	'Big Five Personality traits' model is accepted in the UK
[102]	Cybercrime and psychiatry have implications for UK patients
[104]	Young people as a victim group warrant attention in the UK too
3.3 CYBERCRIME REPORTING: Annotation of non-UK references	
Reference	References' connection to the UK
[8]	Important for understanding generalisable reporting issues
[136]	Comprehensive breakdown of generalisable reporting issues
[4]	Compares UK to a country with low responsibilisation
[115]	Extrapolates help-seeking behaviour to the UK context
[7]	Includes criteria for improving cybercrime reporting applied to UK
[8]	Undergraduates as a victim group warrant attention in UK too
[70]	Models voluntary response to cybercrime reporting applied to UK
[58]	Online counterfeits are a concern for Trading Standards UK
[10][9]	Models effective reporting applicable to UK
[97]	Reference to an online platform applicable for research in UK
[41]	Mentions cybercrime reporting mechanism analogous to UK
[46]	Pertains to cybercrime reports' structuring useful for UK
[25]	Online counterfeits are a concern for Trading Standards UK
[126]	Supplies an automation for spam analysis useful for UK
[127]	Supplies an automation for phishing detection useful for UK

[147]	Supplies a cybercrime typology generalisable onto UK
[42]	Cybercrime jurisdiction obstacles impede policing in UK too
[38]	Contrasts cyber expectations vs reality in a way that extends to UK

Figure A1. Average cost of cyber incidents to organisations in the UK as of 2021, by industry



Source: Statista

Figure A2. Prisma 1 & 2 (RQ1: What characterises cybercrime in the UK?)

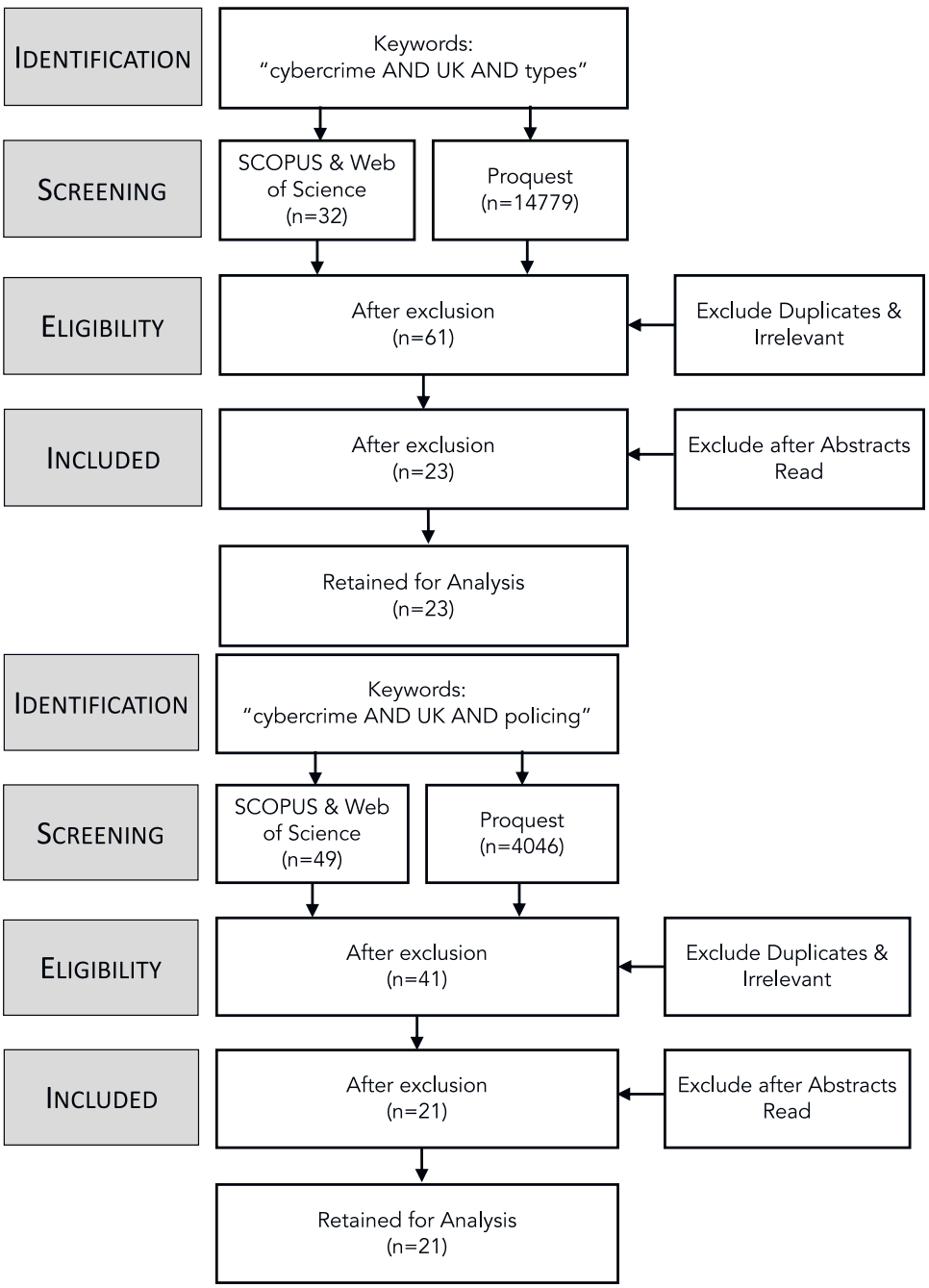


Figure A3. Prisma 3 & 4 (RQ2: What is known about UK cybercrime victims?)

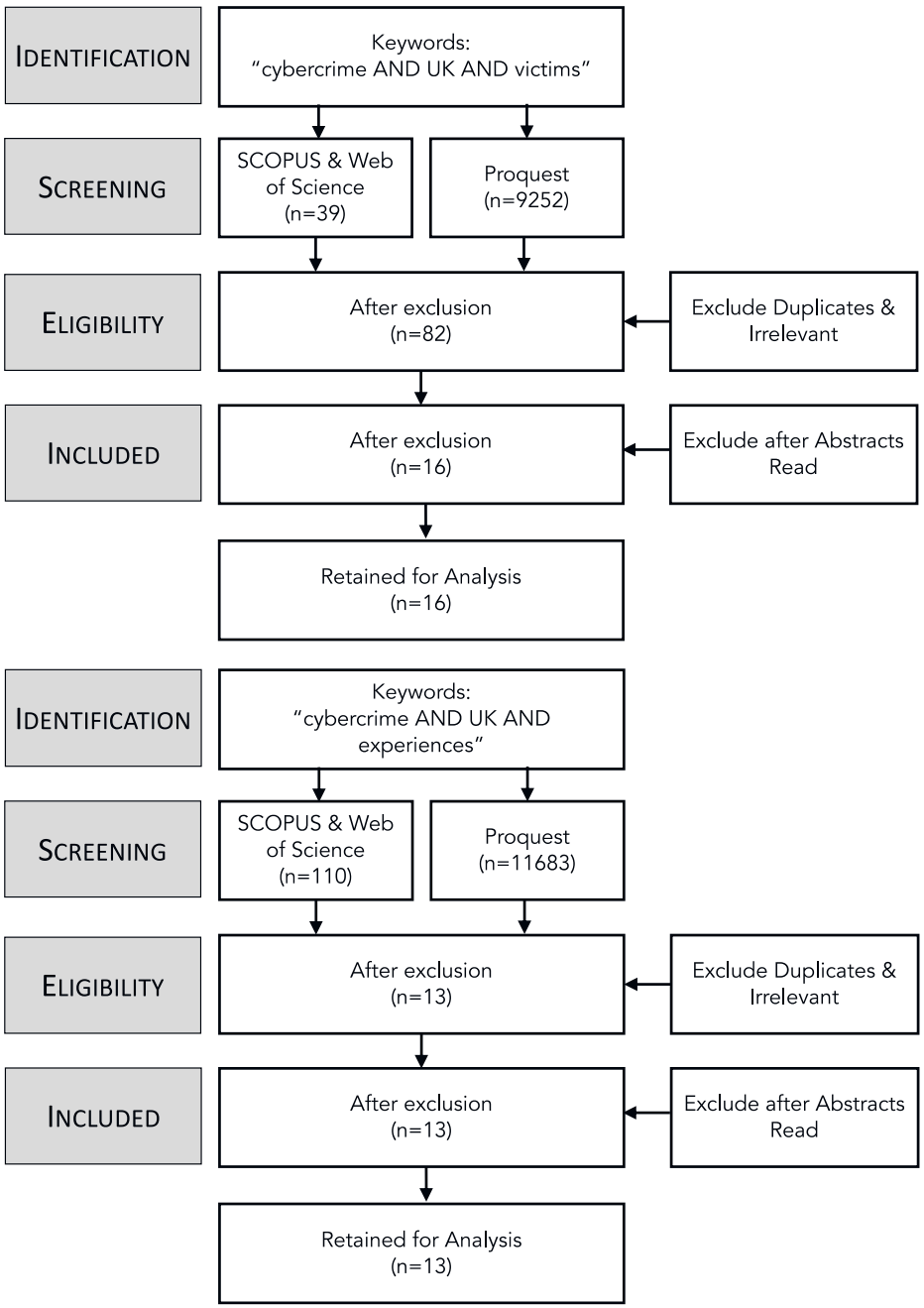


Figure A4. Prisma 5 & 6 (RQ3: What influences and deters cybercrime reporting in the UK)