**Assessing the Seriousness of Cybercrime: The Case of Computer Misuse Crime in the United Kingdom and the Victims' Perspective**

Mark Button#, David Shepherd, Dean Blackbourn, Lisa Sugiura, Richard Kapend and Victoria Wang

Centre for Counter Fraud Studies, University of Portsmouth, Portsmouth PO1 2HY, UK.

#Corresponding author

E-mail mark.button@port.ac.uk Fax 02392843971

Other authors' emails: david.shepherd@port.ac.uk dean.blackbourn@port.ac.uk lisa.sugiura@prt.ac.uk richard.kapend@port.ac.uk victoria.wang@port.ac.uk

Word count: 9897 words

Abstract

The reform of the Crime Survey of England and Wales (a national victim survey) has exposed a very high number of individuals who fall victim to computer misuse cybercrimes such as hacking, computer viruses and ransomware. These crimes receive very little attention from the criminal justice system and very few are brought to justice, partly because of the nature of them (global crimes), but also because of a lack of capability among the police. This paper draws on official statistics, an empirical survey and interview research with computer misuse victims. The paper juxtaposes the low priority and lack of resources given to this crime by political and police leaders against many victims' perceptions and experiences of the crime as equivalent if not more serious than physical counterparts such as burglary, where there is greater interest. The increasing prominence of the virtual world

in human life and the impacts of these crimes call for a reappraisal of the official assessment of seriousness in order to raise the priority and increase the capacity of criminal justice towards such offences.

Keywords: Computer misuse crime, cybercrime, hacking, computer viruses, victims, crime seriousness

## Introduction

A victim interviewed for this research experienced the hacking of her laptop webcam and attempted blackmail. The hackers captured sensitive images of the victim and threatened to publicise them and share with her contacts unless she paid a ransom. She tried to report this to the police and this is what she experienced:

> …at first I spoke to 101[1] who told me to use their online forms to log a complaint, I did so and never heard back from them. I phoned again and was told someone would phone me back, again no phone call, for the third time my husband took me to the station and we spoke to someone on the desk. After what felt like a very brief discussion with an officer, I was informed that there was nothing I could do. Apart from block the emails, cover my webcam and not part with money.

[1] 101 is a telephone number to contact the police for a non-emergency situation.

She even took the printed emails with her:

> …I tried printing them out and taking them in, but they just kind of disregarded what I was trying to say. It was almost like they were thinking, oh, this is just a friend who's being funny. But I'm like, no, this is actually someone who I don't know who's causing me real problems. And even if it was a friend, that's still not right. Sam [Hacking, voyeurism, blackmail victim - Individual].

This kind of official response to cybercrime complaints is not untypical, which supports the view that this type of crime is often perceived as non-serious and therefore a low priority for law enforcement (Bossler and Holt, 2012; Bossler et al., 2019; Correia, 2019; Cross, 2015; 2018; 2020; Cross et al., 2021; Hadlington et al., 2018; Holt and Bossler, 2012a and b; Notté et al, 2021; Paek et al., 2021; Wall, 2007; 2008). However, these types of crimes have become very common. The recent reform of the Crime Survey for England and Wales (CSEW) (a national victimisation survey of individuals) exposed the level of fraud and computer misuse criminality. The inclusion of these crimes in the 2016 CSEW almost doubled the crime rates to 11.1 million per year: 3.4 million fraud and 1.8 million computer misuse offences in 2016 (ONS, 2017). There had been a small decline in these offences since the first report, but the first publication of CSEW, taking into account the emergence of the pandemic and lockdown, showed a rise from just under a million to 1.6 million incidents of computer misuse for the years ending June 2019 to 2020, illustrating the continued high prevalence of this family of offences (ONS, 2020a).

Little, however, has been written about these types of cyber-dependent offences in comparison to other traditional, volume crimes and related cyber-enabled offences (Button

et al, 2021; Wall, 2007; 2008). Fraud (cyber-enabled) has experienced much more interest than computer misuse crime (See for example, Button et al, 2014; Button and Cross, 2017; Carter, 2020; Cross et al., 2018; Drew and Farrell, 2018; Holt et al, 2018; Ibrahim, 2016; Levi, 2008) as have other cyber-enabled crimes based on harassment, stalking, bullying and sexploitation to name some (see for example, Henson et al, 2016; Wolak and Finkelhor 2016). The gap in research on computer misuse offences leads to many questions and one of the fundamental and unexplored questions is the perceived and experienced severity of computer misuse vis-à-vis traditional volume crimes. Is, for example, hacking into someone's computer the same as breaking into their house?

The authors believe it is important to understand the seriousness of crimes because this should influence the response to them. Serious crimes should have tougher penalties and a higher police priority and capability to deal with them than less serious crimes. Thus we would expect a murder to result in a well resourced investigation, with a skilled team of detectives and that the offender, if caught and found guilty, receives a prison sentence of a substantial length. An act of vandalism of a bus shelter, although we would hope the police would catch the offender, would not be expected to attract extensive police resources to investigate and the offender, if caught, result in a prison sentence of years, if at all. As new crimes emerge and grow, it is important the seriousness of them are assessed. In the UK in the 1960s the growth of motor car ownership and drink driving that accompanied it, led to drink driving becoming rated as a more serious crime, with legislative changes, tougher penalties and enforcement to counter it gradually increasing over the years.

Computer misuse crimes are relatively new crimes that have grown substantially in the last 30 years. As such it is an important question to ask just how serious are they and do the

priority, resources, sentencing etc reflect that? This paper will provide some of the first insights into the seriousness of computer misuse crimes. There are of course different constituencies in ranking seriousness: the criminal justice system, victims, the general public (non-victims), politicians to name some. These different groups will often have different perspectives on seriousness. The paper's primary base is research on victims of these crimes. It will also draw upon other data, which reflects the views of the politicians and the criminal justice system. Unfortunately, there was no scope in this project to secure similar data from those working in the criminal justice system (judges, prosecutors and police) and the general public – non-victims. As such it is only a partial picture of the views on the seriousness of computer misuse crime, but nevertheless, a very important part, if not the most important.

This paper will therefore begin with an exploration of computer misuse offences by considering the legal basis, types of behaviours and the extent of the problem in the UK. The paper will then consider some of the literature on the seriousness of crimes, before outlining the methodology for this research. The findings present an analysis of the official measures of seriousness before exploring the perceptions and experiences of victims who participated in the research by way of a survey and interviews.

## Computer Misuse Crime

In the UK the distinction between *cyber-enabled* and *cyber-dependant* crime has become the most common means to distinguish a range of crimes (Furnell, 2002). *Cyber-enabled* crimes do not require information communications technology (ICT) to commit them, but can be

facilitated by the use of ICT. For example, a lottery fraud could be perpetrated by traditional postal mail, but also by email. Conversely c*yber-dependant* crimes, such as hacking, computer viruses, distributed denial of service attacks; can only be perpetrated by using ICT (ONS, 2018b). The Computer Misuse Act 1990 (CMA) encompasses cyber-dependant offences and applies to the whole UK (CPS, 2019) and covers hacking related and computer virus related offences, such as ransomware.

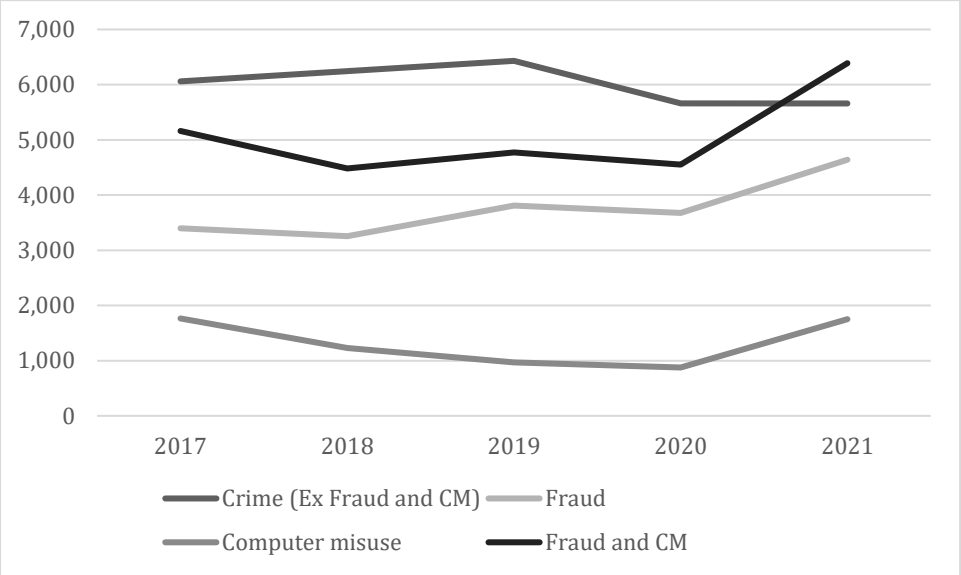
The CMA is similar to burglary under the Theft Act 1968 s9 as it involves digital versions of trespass and the commission of further offences, such as stealing digital material, harassment, extortion, fraud and computer damage. Computer misuse offences can be discrete cyber-dependant offences, for example person A hacks the email account of person B to read their email (CMA section 1). They can also form the basis of other cyber-enabled offences, for example person A hacks the email account of person B looking for information and opportunities to defraud B, such as a request for payment to specific bank account, which is then resent with alternative bank details (CMA section 2 and fraud by false representation). Often such secondary crimes are more serious and become the primary offence thus leading to lower figures in the recorded computer misuse statistics.

*The extent of computer misuse crime*

Recognising the scale of the computer misuse crime threat and its intersection with fraud under CMA section 2, the ONS introduced computer misuse and fraud into the 2016 CSEW household victimisation survey (ONS, 2017). Figure 1 shows the CSEW trends since 2016 (ONS, 2020 & 2021). All CSEW crime (excluding fraud and computer misuse) has remained steady at around 6 million. Fraud has increased from around 3.5 million to just

almost 4.6 million. Computer misuse crime has halved from around 2 million to 1 million. However, during the Covid 19 lockdowns (March 2020-April 2021) computer misuse substantially increased to almost 1.7 million (although the pandemic led to a change in data gathering for the CSEW from face-to-face interviews to telephone and ONS are suggesting caution in comparing with previous years). The decline in computer misuse before the pandemic is largely attributed to a reduction in computer virus offences from around 1.1 million to 360,000. Some of this fall could also be accounted for by a shift of ransomware targets from individuals to organisations, which are not covered by the CSEW. Figure 1 also shows how together fraud and computer misuse are now greater than all other CSEW crime.

Figure 1: CSEW computer misuse offences in comparison to fraud and all other crimes (000s) year ending March 2017-2021




CMC=computer misuse crime

Computer misuse crime clearly represents a significant volume of the crimes afflicting society. However, compared to the high volume of computer misuse crimes experienced, very few are reported to the authorities. The police recorded just 29,651 incidents in 2020 (ONS, 2021). The 98% attrition rate can mainly be accounted for by non-reporting and in some cases by more serious offences taking precedence. It is not clear why people do not report computer misuse and there has been limited research on this but it may be because it is predominantly regarded as a nuisance rather than sufficiently serious to make out a complaint (van de Weijer et al, 2019). It is therefore important to undertake victim research to understand their perceived and experienced severity of the crime. The next section explores different approaches to the measurement of seriousness and compares computer misuse to equivalent traditional offences.

**Exploring Seriousness of Crime**

In the UK 'Serious Crimes' are defined in legislation and computer misuse offences are listed as such (added to the list by Serious Crime Act 2015). The list includes a wide range of offences from drug trafficking, people trafficking, terrorism offences, firearms offences, fraud, bribery and intellectual property offences to name some. These different 'serious' offences would be rated differently by different groups: victims, police, judges, politicians etc in terms of their seriousness. Attempts at rating the seriousness of a particular crime is a subjective enterprise which has been the focus of a small number of studies (Levi and Jones, 1985; Pease, 1988; Sherman et al., 2016). At an individual level seriousness could be measured by the harm caused and the culpability of the offender. Such dimensions are, however, peculiar to a particular case and offer little in generalisability in terms of judging the seriousness to society relative to other crime types and measures built upon such approaches can also be very complex (Greenfield and Paoli, 2013). A simple means of assessing severity is to rank

offences according to the listed maximum sentences prescribed in law, a 'lawmaker's ranking' which is a gauge of the government's perception of seriousness. However, the maximum sentence is rarely used except in the most serious cases such as murder. An alternative lawmaker's ranking is to use the sentencing guidelines issued to judges. Sherman et al. (2016) based the Cambridge Crime Harm Index (CCHI) on the sentencing starting point for a first time offender in the UK sentencing guidelines. The CCHI accommodates non-custodial sentences by counting the minimum tariff for community service as days in prison, and by converting fines to the number of days required to pay the fines at minimum wage (Sherman et al., 2016). The CCHI is not suitable for the present project because sentencing guidelines have yet to be developed for computer misuse offences. Furthermore, collapsing a wide range of offences onto common sentencing start points produces odd rankings. For example, with a score of 19 days (a community order) *attempted* voyeurism ranks the same as *actual* sexual assault on a female. Such anomalies are a consequence of the CCHI ignoring the sentencing range available to the courts: the maximum sentence for attempted voyeurism is 2 years and the maximum for actual sexual assault is 10 years. The government lawmakers clearly understand that sexual assault can be far more serious than attempted voyeurism, which is reflected in average sentences handed out by the courts: the average sentence for sexual assault is 68 months, nearly 4 years in excess of the maximum for attempted voyeurism.

A second group of methods involve 'judicial rankings' based on actual sentencing practices reflected in court records. The simplest method involves ranking crimes according to the average sentences handed out for each crime type. The drawback of this method is that it cannot take into account non-custodial sentences and out of court disposals such as fines and community orders (ONS, 2016), and the averages are substantially affected by previous

offending history (Sherman et al., 2016). Nevertheless, the average sentence approach has merits in comparing offence types as it a measure of actual judicial outcomes. The Justice Sector Seriousness Score (JSSS) in New Zealand addresses the non-custodial problem by using a calculation to convert non-custodial sentences to an equivalent prison sentence, for example a $117 fine is equivalent to 1 day in prison (New Zealand Ministry of Justice [NZMOJ], 2017a). The JSSS scores unauthorised access to a computer for dishonest purposes at 373 days and burglary by day worth up to $5,000 at 318 days. It also scores unauthorised computer access with the intent to cause damage at 93 days and physical criminal damage at the equivalent of 0.9 days (see also NZMOJ, 2017b). In both these comparable cases, the New Zealand judiciary regard the cyber variants as more serious than the traditional, physical crimes. Although the JSSS may have value within New Zealand, it is not applicable to the UK because the legal definitions of the crimes are not directly comparable.

The UK's Crime Severity Score (CSS) performs a conversion calculation similar to the JSSS, but weights the average sentences by multiplying them by the proportion of offenders receiving the punishment types (ONS, 2016). Unfortunately the CSS does not yet cover computer misuse crime. Francis et al. (2001) proposed an alternative court record method involving the analysis of paired sentencing decisions where offenders have been found guilty of multiple crimes. In these cases the offence attracting the most severe sentence is regarded as more serious than the other offences. A thorough analysis of thousands of cases could create a comprehensive ranking of crime seriousness, but the analysis has yet to be done.

Other researchers have ranked crime seriousness based on the perceptions of particular groups, such as the police, the public and victims (Levi and Jones, 1985; O'Connell and Whelan, 1996; Pease, 1988; Wolfgang, 1985). Unlike the objective judicial scores, these methods face subjectivity challenges: public perceptions are highly variable and can be influenced by the media or personal experiences, the scales used might be misunderstood by respondents or constrained scales may be inadequate in differentiating the level of seriousness between different crime types (Francis et al., 2001; O'Connell and Whelan, 1996; Sherman et al., 2016). Despite these criticisms, surveys have long been an important research method for gauging the public's perception of relative seriousness (Levi and Jones, 1985). In rare research into cybercrime, Holt et al. (2019) included a direct comparison of one crime type: they found that nearly 20% of police officers in the UK clearly felt online harassment is less serious than traditional harassment, although the majority regarded it as equivalent. A number of other researchers have also explored law enforcement attitudes towards cybercrimes (Bossler and Holt, 2012; Bossler et al., 2019; Cross et al., 2021; Hadlington et al., 2018; Holt and Bossler, 2012a and b; Notté et al, 2021; Paek et al., 2021).

## Method

The scope of this research was computer misuse offences. As noted earlier these are cyber-dependent crimes, which are specific offences in the UK. This meant many cyber-enabled cybercrimes covering areas such as harassment and certain online frauds were beyond the remit of this paper. However, in the UK it is also important to note the majority of computer misuse offences are financially related: largely through frauds based upon hacking

or ransoms. Some computer misuse crime does, nevertheless, involve harassment and voyeurism.

Three methods were employed to examine the level of seriousness attached to computer misuse crime. Firstly, objective lawmaker and judicial rankings were collected: the maximum tariffs in the Acts of Parliament and the average prison sentences for the 11 years 2008 to 2018 from the offence dataset published by the ONS (2019). Burglary data was collected for comparison purposes as its physical world characteristics are commensurate with the computer misuse crime variant. They both contain elements of trespass, illegal acquisition, personal harm and damage. Fraud data was also included because it is the most common consequential crime associated with computer misuse (CPS, 2019).

The second method was a UK survey of n=252 adult victims of computer misuses crimes. Qualtrics were engaged to recruit fraud victims. Qualtrics is a research company that retains a very large standing panel to conduct surveys. This means there are research limitations as the sample frame is a non-probability, convenience sample (Etikan et al., 2016). This is a large sample size as the research instrument uses a 20-point interval scale to enable ANOVA significance testing. capture perceptions of the seriousness of a range of crimes.

The questionnaire was designed to explore a wide range of views and experiences, including consequential harms, the process for reporting the crimes, the response of law enforcement, and perceived seriousness. This paper focuses on the victims' perception of the seriousness of computer misuse crime compared to burglary, non-invasive minor theft and murder using a 20-point interval scale (Table 1) and the impact. The sample is large as the research instrument uses the 20-point interval scale to enable ANOVA significance testing at the 95% confidence level with a probability threshold of p=0.001. Except for the

regular Crime Survey for England and Wales, this is the largest survey to date of computer misuse victims in the UK the researchers are aware of.

Survey respondents were asked to concentrate for most of their responses on the most serious computer misuse incident they had experienced in the previous two years. Only 39% of the respondents experienced a net loss as a result of the incident and this ranged from £2 to £10,000 with an average of £657. The sample included the following offence frequency:

- 49% - hacking of an online account to access personal information or services [email, social media, bank account etc.]
- 29% - a computer virus, or other form of malicious infection, which caused damage or disruption to your device
- 13% hacking of a computer or other device in your possession [laptop, smartphone, desktop computer etc.] to access personal information
- 8% - ransomware - where a form of malicious software caused your device to malfunction and where the perpetrator requested money, or another form of ransom, to restore your device's functions
- 1% - denial of service attack - where your internet access was deliberately disrupted, or services and information you provide on the internet were deliberately disrupted [e.g. your website or blog was crashed]

The third method involved interviews with n=52 adult victims. The researchers used a non-probability, purposive sampling approach to recruit the participants. The aim was to secure a diversity of victims based upon the different types of computer misuse offences, victims

who reported the offences to the authorities ('reporting victims'), those who did not report to the authorities ('non-reporting victims'), individuals, and owners or senior managers of small and medium sized enterprises/organisations (SME/O) victims. The n=52 sample included 38 individuals and 14 SME/Os. This is also a large sample size in that it exceeds the minimum level for interview data saturation by a factor of four. Guest et al. (2006) advocate a sample size of 12 is adequate to capture 97% of thematic codes. Francis et al. (2009) found that saturation occurs between n=10 and n=13. The samples for both the individuals and the SME/Os exceed these thresholds.

The participants were recruited with the assistance of the National Fraud Intelligence Bureau, the National Crime Agency, the police and by promotion through professional networks. Not all leads proved accurate as some cases had been mislabelled by the authorities. For example, one potential participant was rejected when it transpired the offenders had spoofed his email account, which he thought had been hacked. There were several other potential participants that were excluded and a lesson for future researchers investigating this area is to carefully check the status of potential participants before arranging interviews.

The vast majority of interviews were conducted face-to-face, with a very small number conducted via Skype or telephone (either because the victim was now abroad or the victim preferred not meet physically because of the sensitivity of their case). One SME contacted refused an interview but provided written responses to prepared questions (they are not included in the 52, but some of their responses were coded and analysed). All interviews were transcribed and then analysed using content analysis, which resulted in multiple codes and themes. Similar to the survey, the largest offence group is hacking. Most of the individual

victims did not experience a significant financial loss as the offence was an attempt (ie a fraudster got unauthorised access to their account) or the victim secured reimbursement after such access (which because of the Home Office counting rules meant classification of computer misuse)

- 34 hacking victims (or where hacking primary offence)
- 7 computer virus/malware victims;
- 7 ransomware victims;
- 2 denial of service victims;
- 2 victims of multiple offences; and
- 1 harassment victim (Wayne) (this victim was listed by the NFIB as a 'hacking' victim, but had experienced cyber harassment where his personal email address was used by an unknown perpetrator to sign him up to groups/newsletters he would find offensive such as the British National Party. The unique experience warranted inclusion in the sample).

The methods for this research received approval from the university Ethics Committee and as part of that process all victims' names have been changed to avoid identification in the presentation of quotes from them. It is important to recognise the limitations of the research. Firstly, as the interview sample is dominated by 'reporting victims' and the vast majority do not report it is possibly biased towards those who consider the offence more serious, although some non-reporters and attempted reporters did consider the offence to be serious, so this might not be such an important consideration. Secondly, both the interviews and survey are based on victims, non-victims may have a different perspective on these offences. Third, some of the older victims' recall of the exact details of the incident

was not brilliant. Fourth, some of the NFIB classifications of victims were wrong, such as computer virus victims classified as hacking and vice versa. Nevertheless, the data provides an important, rich insight into the seriousness of computer misuse crime victimisation. Table 1 below provides further demographics on the sample.

Table 1. Key demographics of survey and interview sample

| | Survey | | Interviews | |
|---|---|---|---|---|
| Categories | N | % | N | % |
| **Gender** | | | | |
| Male | 112 | 44.4% | 25 | 48.1% |
| Female | 140 | 55.6% | 26 | 50% |
| Prefer not to say | | | 1 | 1.9% |
| **Age** | | | | |
| 18-24 | 52 | 20.6% | 2 | 3.8% |
| 25-34 | 103 | 40.9% | 11 | 21.2% |
| 35-44 | 59 | 23.4% | 11 | 21.2% |
| 45-54 | 30 | 11.9% | 9 | 17.3% |
| 55-64 | 5 | 2.0% | 10 | 19.2% |
| 65-74 | 2 | 0.8% | 5 | 9.6% |
| 75+ | 1 | 0.4% | 4 | 7.7% |
| **Occupational Status** | | | | |
| Non-manual: professional | 41 | 16.3% | 30 | 57.7% |
| Non-manual: employers and managers | 47 | 18.7% | 7 | 13.5% |

| | | | | |
|---|---|---|---|---|
| Non-manual: intermediate and junior non-manual | 39 | 15.5% | 3 | 5.8% |
| Manual: Skilled manual and own account non-professional | 46 | 18.3% | 2 | 3.8% |
| Manual: Semi-skilled manual and personal service | 38 | 15.1% | 1 | 1.9% |
| Manual: Unskilled | 15 | 6.0% | 0 | 0% |
| Other | 16 | 6.3% | 8 | 15.4% |
| Prefer not to say | 10 | 4.0% | 1 | 1.9% |
| **Race** | | | | |
| White and Black Caribbean | 1 | 0.4% | 0 | 0% |
| English/Welsh/Scottish/Northern Irish/British | 207 | 82.1% | 48 | 92.3% |
| Irish | 4 | 1.6% | 0 | 0% |
| Gypsy or Irish Traveller | 0 | 0.0% | 0 | 0% |
| Any other white background | 7 | 2.8% | 2 | 3.8% |
| Any other Black / African / Caribbean background | 1 | 0.4% | 0 | 0% |
| Indian | 5 | 2.0% | 0 | 0% |
| White and Black African | 3 | 1.2% | 0 | 0% |
| White and Asian | 6 | 2.4% | 0 | 0% |
| Any other Mixed / Multiple ethnic background | 0 | 0.0% | 0 | 0% |
| Caribbean | 4 | 1.6% | 0 | 0% |
| Any other ethnic group | 2 | 0.8% | 0 | 0% |
| African | 3 | 1.2% | 0 | 0% |

| | | | | |
|---|---|---|---|---|
| Arab | 0 | 0.0% | 1 | 1.9% |
| Pakistani | 4 | 1.6% | 0 | 0% |
| Bangladeshi | 0 | 0.0% | 0 | 0% |
| Chinese | 2 | 0.8% | 1 | 1.9% |
| Any other Asian background | 2 | 0.8% | 0 | 0% |
| Prefer not to say | 1 | 0.4% | 0 | 0% |

**Lawmaker and Judiciary Rankings**

Table 2 sets out the measures of seriousness of the computer misuse crimes based on the maximum sentence tariff, the average prison sentences handed out by the courts between 2008 and 2018, and the annual average number of offenders sentenced to prison for each of these offences over the 11 years (ONS, 2019). The table is organised according to the level of harm caused to victims as described in the statutes, and each group compares a computer misuse offence from the CMA to the nearest equivalent physical crime. Thus, the first group is the supply, acquisition and possession of articles in 'preparation' of committing offences against victims. The 'trespass only' group does not involve loss or damage, and compares unauthorised access to a computer (CMA s1) with physical trespass. However, physical trespass is generally a civil tort and not a criminal offence. Adverse occupation of residential premises (squatting) under the Criminal Law Act 1977 s7 is the nearest criminal equivalent. Attempted burglary is also included as it involves trespass with the intent to steal. The 'consequential harm' group involves the criminal acquisition of property, damage and personal harm by computer misuse crime, fraud and burglary.

Table 2: Maximum and average sentences 2008-2018

| | Offence | Sentence (months) | | Average number of persons sentenced to prison per year for listed offences |
|---|---|---|---|---|
| | | Maximum | Average | |
| Preparation | Supply / possession of articles for cybercrime CMA s3A | 24 | N/A[1] | 0.1 |
| | Equipped for burglary TA s25 | 36 | 4 | 414 |
| | Possess articles for fraud FA s6 | 60 | N/A[1] | N/A[1] |
| | Supply articles for fraud FA s7 | 120 | N/A[1] | N/A[1] |
| Trespass only | Unauthorised access CMA s1 | 24 | 9 | 1.6 |

| | | | | |
|---|---|---|---|---|
| | Property trespass | Civil tort, not criminal offence | | |
| | Adverse occupation CLA s7 | 6 | N/A[1] | N/A[1] |
| | Attempted domestic burglary – trespass with intent to steal TA s9 | 168 | N/A[2] | N/A[2] |
| Consequential harm | Unauthorised access to facilitate further crime CMA s2 | 60 | 16 | 3.5 |
| | Unauthorised access to impair computer CMA s3 | 120 | | |
| | Unauthorised access causing damage / harm to human welfare /economy / national security CMA s3ZA | 168 | | |
| | Fraud by false representation FA s2 | 168 | 15 | 1,406 |

| | | | | |
|---|---|---|---|---|
| | Domestic burglary – trespass to steal or cause harm TA s9 | 168 | 30 | 6,406 |
| | Damaging property with endangerment to life CDA s1(2b) | Life | 51 | 50 |

Notes:

(1) No average sentences reported due to insufficient prosecutions (ONS, 2019).

(2) No separate category for attempted burglary in sentencing data (ONS, 2019).

CLA = Criminal Law Act 1977; CDA = Criminal Damage Act 1971; CMA = Computer Misuse Act 1990; FA = Fraud Act 2006; TA = Theft Act 1968

Despite the millions of computer misuse offences that have been committed in the UK (ONS, 2020), prosecution is very rare: just 384 court proceedings over 11 years, 309 sentenced and 55 offenders imprisoned, an average of five per year (ONS, 2019). The low prosecution figure rate is an explanation for the current absence of sentencing guidelines: there are simply too few cases to be concerned about sentencing uniformity. For the comparable offences of domestic burglary an average of 6406 were sentenced to prison each year compared to 3.5 for computer misuse.

Many computer misuse crimes are difficult to investigate and emanate from other countries (Gundur et al., 2021). Lots involve high volumes of victims with few offenders. Some within

the police might also argue they lack capability through adequate resources, appropriate equipment and trained staff. Nevertheless, the authors would contend that the capability developed is ultimately the result of political choices made by the politicians and senior police leaders that reflects the priorities they perceive as important.

Computer misuse crime has largely been down that list of priorities and a serious crime would surely receive a higher priority and a better response (although this is changing). It is therefore indicative of the regard that police leaders have had for computer misuse in the recent past. An influential report by Her Majesty's Inspectorate of Constabulary Crime, Fire and Rescue Services (2019) noted a wide range of inadequacies (as well as some positives) in the police response to cyber-dependent crime, which can be attributed to the interest and priority of many police leaders. These included:

- Precarious short-term funding of specialist police capacity putting it at risk of cuts because of pressures on police budgets;
- Limited understanding of the demand for cyber-dependent investigations and planning to meet it;
- Some forces did not have any specialist cyber-dependent staff, many had vacancies they couldn't fill and suffered high staff turnover;
- They found 17 forces couldn't even tell them how many cyber-dependent investigations they had undertaken; and
- The report also highlighted, 'considerable variation in the quality of the investigations and their subsequent outcomes. The investigations by the regional and national teams were, in our view, of considerably better quality overall than those done by local forces' (p. 65)

Some of these findings from HMICFRS can be linked to the constrains on the police by the funding and priorities set by their political masters, but several clearly relate to the interest and priority of the police.

An earlier report by the HMICFRS (2015) regarding digital crime had also highlighted problems in the police prioritisation and response to fraud and cybercrimes. Other studies have also found evidence of gaps. Holt et al (2019) in a large survey of frontline police officers noted gaps in the perception against the reality of different some cybercrimes. Forouzan et al (2018) found in a survey of Metropolitan Police Officers the majority generally did not feel adequately trained or educated to deal with cybercrime and that almost a third had not completed a compulsory training package on cybercrime or even aware of it. This study also involved interviews with victims of cybercrime who were also generally unhappy with the response they received. Loveday (2018, p. 400) in reviewing the police response to the changing nature of crime noted, 'One interesting feature of the dramatic rise in fraud and cybercrime has been the slow reaction by the police service to this development' and Levi et al (2017, p. 94) came to a similar conclusion, "There is widespread agreement that policing in the UK and also around the world has fallen behind the curve of evolving patterns of crime, especially cyberfrauds and the cyber-forensic aspects of police investigations."

Nevertheless, to be fair to police leaders, as has already been noted, they have had to work within the constraints that politicians set them through budgets and priorities. The police service, prior to the recent General Election, had undergone a decade of cuts. The Institute for Government in 2019 noted a 16% decline in spending on the police since 2009, while at the same time illustrated increasing demands on them, particularly for resource intensive investigations such as child exploitation and human trafficking. The police's hands have

therefore been tied by the resources they have been given and not surprisingly, as the report noted, 'Freedom of Information (FoI) requests to the Metropolitan Police revealed internal guidance for officers to consider the proportionate level of investigation, stressing the need to focus on serious crime and incidents which are more likely to be solved' Institute for Government, 2019). Computer misuse crimes rarely meet these criteria.

The recently published Government plan on beating crime set out an agenda to tackle a variety of crime problems. It included a chapter on fraud, cyber and online crime with a variety of proposals. A welcome recognition of the importance of this and related crime. However, it notes a past investment of £195 million over five years to develop a specialist network of cyber investigators, some £39 million per year. To put this in context Deloitte (2020) found in a survey of financial institutions an estimated spend of US$2691 per full-time employee on cyber security. For a bank such as Barclays based in the UK with 83,500 employees globally this would amount to US$225 million or £191 million. Thus in one year, one organisation – albeit a high risk one – spends virtually the same as this Government investment for five years. The numbers invested should also be set against a past conservative estimate of the cost of cybercrime at £27 billion per year, further illustrating the relatively small amount (Cabinet Office/Detica, 2011). Ultimately while the proposals are positive as is the investment, it is not enough in the context of the scale of the problem of these types of crimes.

If the maximum sentences to computer misuse offences to comparable physical there are also gaps. The maximum sentences in all three categories in Table 2 indicates that the government lawmakers regard computer misuses as less serious than domestic burglary and fraud except when the disruption of a computer system causes wide societal, economic or

national security harm, including loss of life under CMA s3ZA. In this instance the maximum sentence is the same as domestic burglary (168 months), yet the disruption to the national health, welfare, police or banking systems could cause far more harm than a physical intrusion into a person's home. It is arguable that this type of egregious cybercrime is at least equivalent to criminal damage that endangers life, which attracts a maximum life sentence under the CDA 1971. The average sentences in the harm category suggests that the judiciary also regards computer misuse crime and its most frequently associated economic offence, fraud, as less serious than burglary and grievous criminal damage. Although computer misuse offences are perpetrated on an industrial scale, often using automation, by individuals or small groups, the lower sentences do not acknowledge the breadth of the personal, social and economic impacts of the crimes.

**Victims' Views on the Seriousness of Computer Misuse Crime**

The victim survey (n=252) aimed to rank the victims' perceptions of the seriousness of computer misuse crime and burglary relative to a minor crime, the non-invasive theft of milk bottles from a doorstep, and to the very serious crime of murder. Based on a 1 to 20 scale, with 1 being the minor theft and 20 being murder, all the cyber offence ratings are similar to burglary, but with important differences (Table 3). The 'trespass only' offences, which do not cause direct harms, are viewed as less serious than those which cause consequential damage, financial loss or the serious invasion of privacy. The respondents regard sending a virus and burglary as equivalent in seriousness, whilst hacking for fraud, ransomware and online voyeurism are viewed as more serious than burglary. The data was subjected to ANOVA, which found that the differences between the offence perceptions are highly

significant [F(6,1757)=8.56, p<0.001). However, there is no statistical difference between the genders (p=0.770), thus indicating that the order of severity by gender is the same. The key finding from this survey is that the victims view computer misuse which involves a consequential harm (fraud, ransomware, and voyeurism) as more serious than burglary.

Table 3: Survey respondents' views on the seriousness of computer misuse crime

| | **Offence** | **Mean Score on scale of 1-20 All** | **Male** | **Female** |
|---|---|---|---|---|
| Trespass only | Hacking for thrill | 8.26 | 7.92 | 8.54 |
| | Hacking to view personal information | 8.98 | 8.79 | 9.14 |
| Consequential harm | Sending a virus | 9.40 | 9.21 | 9.56 |
| | **Burglary** | **9.48** | **9.29** | **8.54** |
| | Hacking for fraud | 10.30 | 10.73 | 9.95 |
| | Sending ransomware | 11.06 | 11.38 | 10.80 |
| | Hacking for voyeurism | 11.08 | 11.29 | 10.91 |

N=252

Mirroring the survey data, the majority of the interview participants regarded computer misuse as equivalent to, or more serious than burglary, but as with the survey there were some who did not:

> But I find things like that quite minor, like they're just irritating, they're not doing anything serious. But, if it's obviously more severe, in terms of, like, somebody could potentially steal your data, somebody could hack into your bank, then obviously, I'd cast that as more serious. Vanessa. [Computer virus - Individual].

> I don't think computer misuse is as bad because obviously burglary, people have been into your house and they've rooted through your things. Okay, someone's been into my computer and they've rooted around, but they haven't physically touched things … Liz. [Hacking, fraud - Individual].

> But again, I just feel like, you know, someone going into the physical space of the computer, is not going to stop me from using the computer, whereas someone coming into my house, burgling my house, is likely to make me want to stop going into the house. Does that make sense? Paul. [Hacking, fraud - Individual].

Arnold, a ransomware victim, highlighted the additional risks of physical violence in burglary incidents compared to computer misuse crime:

> I think it's less important than burglary. I mean, burglary to me is a potential lead into violent crime. You know, if somebody had to be burglaring [sic] the place here and I had to come in for whatever reason and catch the person in the act, you've then got

> quite a high potential of some sort of violence happening. I think theft, fraud and what was the other one? Arnold. [Hacking, ransomware - SME].

Some of the participants viewed burglary and computer misuse as equivalent property crimes. In contrast to Arnold, Ralph, who was also a ransomware victim, regarded the offences as equivalent property crimes, and Bernard characterised cybercrime as the 'new burglary':

> It's virtually the same thing. I think it's the same thing, because you're stealing someone's property. It doesn't matter if it's an object you can see or an object you can't see, it's still stealing. Ralph. [Hacking, ransomware - SME].

> Well, it's the new burglary, isn't it. Not through living here, although I have been burgled here but you don't expect to be burgled anymore, you expect this sort of stuff to happen. Bernard. [Hacking, fraud - Individual].

Both Claire's and Sarah's computers were hacked and money was subsequently taken from their bank accounts. Mathew owned a small business and his website was hacked to steal customer data for fraudulent purposes. All three victims experienced the intrusion on an emotional level and likened it to burglary:

> To me, it felt the same as if they had been in the house, you know, it was personal, so I felt that they had. And the fact that they'd been on to my... You know, they could get access to my phone and everything, I felt like they had been in the house. So to me it's the same. Claire. [Hacking, fraud - Individual].

So, I don't know, they are very different crimes, but at the same way, in one way they do affect you, there is no question about it. It's a violation of you and your belongings and the way you do things, and I think that can be very hard. Sarah. [Hacking, fraud - Individual].

Oh, it affects you emotionally so much and also you're completely unaware that it's happened. So, yeah, I do think it's right up there with the most invasive things that can happen to you ... But, yeah, no, I would rank it right up there with...it has a huge impact. Mathew. [Hacking, theft of customer data - SME].

Several victims, however, described the crimes as more serious than burglary. Joanna identified higher financial risks in computer misuse crime, whilst Sam observed how criminal damage can be quickly resolved by insurance whilst the effects of intrusive cybercrime can be enduring:

Oh, far higher than burglary. 'Cause, I…burglary, these days, what can you steal from a house, you don't have cash, you've got a television, who wants a great big television you can get them really cheap now. What can you steal from a house, jewellery, I don't have any jewellery so no, I think, hacking you can take a lot more. Joanna. [Hacking, fraud - Individual].

I believe it affects the person more long term. Criminal damage, you've got insurance, you can replace the things quicker, where cybercrime it takes longer to recover, I find. It's still affecting me this far on, it's almost a lifetime thing you've got

> to deal with. Where criminal damage, you can call up your insurance company, get it repaired, done. Cybercrime is more complicated than that. Sam. [Hacking, voyeurism, blackmail - Individual].

Alex and Kellie felt that the stealth of computer misuse crime means it is more serious than burglary particularly as the offenders are untraceable and invulnerable to law enforcement:

> I think it's probably more serious, because it's hard to detect at times, so it can be operating, and you're not even aware of it. Kellie. [Ransomware - SME].

> I feel they are more serious because the person who commits the crime feels like there is no recourse for their actions. They feel like once they've done it they feel like they're completely untraceable, they're completely untouchable. Alex. [Hacking, harassment - Individual].

These survey and interview findings indicate a range of factors influencing the perceived seriousness of computer misuse. The attitude of some victims aligns with law enforcement and the justice system, regarding computer misuse as less serious than burglary. These victims have a relatively low level of psychological and emotional investment in their digital lives and property, and therefore regard physical threats as more serious than cyber offences. In contrast, the subjective perception of those with a higher attachment to their digital lives is that the personal intrusiveness of computer misuse crime is at least equivalent to burglary. Finally, computer misuse crime is associated with distinctive toxic characteristics that make it more serious, that is, the conniving stealth and arrogance of untraceable offenders.

## Discussion

A central premise of this article is that it is important to understand the seriousness of different crimes, particularly new types as they emerge; so that the response to them in the form of police priority, action and results; as well as the sentences set and actually given, are commensurate with that seriousness. Gaps found deserve the attention of political and criminal justice leaders. There are a variety of crime areas where such gaps have been exposed in recent years leading to more action: rape, domestic violence and racially motivated crime are prime examples. Further, online fraud offences (which are closely related to computer misuse) stimulated the Sentencing Council to explore whether the increasing shift from physical to online warranted changes in sentencing guidelines, culminating in changes to the guidance Kerr et al., 2013; Sentencing Council, 2013).

Computer misuse crime is relatively new and with increasing use of ICT in the last 25 years has become one of the most common crimes people and organisations experience. There has been surprisingly little research on this crime and particularly the severity of it. This paper has illustrated findings from a significant constituent of interests – the victims. It has shown that majority of them regard this crime as at least equivalent if not more serious than traditional acquisitive crimes such as burglary.

Our findings indicate that for many victims interviewed for this research, digital intrusion is a deeply personal violation that leads to serious psychological harm and ill-health, and the assessment of seriousness based on relatively minor computer damage or modest financial loss cannot accommodate the invisible harm to victims. It is important to note that the majority of the interviews draw upon victims who have reported or tried to report their crime. The vast majority of victims do not and although the survey element of this research captured their perspective, there is a need to understand these victims more.

The increasing prominence of the virtual world in human life will only exacerbate these problems. The pandemic has shifted even more time we spend online and with that an increased numbers of computer misuse crime related incidents. The findings from this research illustrate the need to consider the wider impact of these offences, beyond whether there is a financial loss and particularly the the salience of digital personal violation.. It is important the actors within the criminal justice system recognise how serious many victims regard these offences, even when there is no financial loss. This implies the police taking more interest in encouraging victims to report and meeting their needs when they do. It means more resources dedicated to investigating these incidents and for the small numbers that do meet a judicial conclusion, appropriate sentencing.

This research for this paper did not collect primary data from other significant constituents such as police leaders, police officers, judges, politicians and non-victims of such crimes. This is a limitation in this paper and area that needs more research. However, victims are the most important voice, after all it is them that have experienced the crime. The paper, however, did offer evidence from such groups in their actual actions towards this crime, such as evidence of the police response and sentences given. Arguably such actions are a better measure than views – it is very easy for a politician or police leader to say a crime is serious and promise action. This paper illustrated the potential sentences, successful prosecutions and police response all illustrated gaps. Some of these gaps can be explained by the challenges of policing cybercrime, such as the transnational nature, but not all. Some of the negatives are the direct result of political decisions, such as the limited funding offered by politicians. Given the seriousness with which computer misuse offences are regarded by victims, greater attention and resources should be directed at such crimes.

**Conclusion**

This paper has considered the seriousness of computer misuse crimes, which now account for a high proportion of crimes against individuals and organisations in England and Wales. Based on an analysis of both maximum and average sentences, computer misuse is perceived by the government and the judiciary to be less serious than its physical equivalent. Although the official crime statistics indicate that a large majority of these cybercrimes appear to be experienced as relatively trivial nuisances, our research demonstrates that many victims regard these crimes as at least equivalent to burglary if not higher. Moreover, it is apparent that an important minority of computer misuse incidents cause significant harms to victims including emotional, psychological and physical health impacts. The current policies of the police and many parts of the criminal justice system do not adequately account for these impacts on people's lives because the traditional official assessments of seriousness are based on visible property damage, personal injury and financial loss. Government policies and official assessment of these new crimes needs to acknowledge and include the invisible harms. The police and the criminal justice system may then treat it with the seriousness many victims deserve and to support the observations of HMICFRS (2019) 'keep the light on'.

**Funding**

This paper is based upon a research project funded by the UK Government Home Office.

**References**

Ashby, M. P. (2018). Comparing methods for measuring crime harm/severity. *Policing: A Journal of Policy and Practice, 12*(4), 439-454.

Birmingham Mail (2018) MP is victim of regular attempts to hack her email. Retrieved from https://www.birminghammail.co.uk/news/midlands-news/mp-victim-regular-attempts-hack-14513977

Blakeborough, L. and Correia, S. (n.d.). *The Scale and Nature of Fraud: A Review of the Evidence*. Home Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720772/scale-and-nature-of-fraud-review-of-evidence.pdf

Bossler, A. M., Holt, T. J., Cross, C., and Burruss, G. W. (2019). Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. *Security Journal*, 1-18.

Bossler AM & Holt TJ (2012). Patrol officers' perceived role in responding to cybercrime. Policing: An International Journal of Police Strategies & Management 35(1): 165–81

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, 64, 101675.

Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. Routledge.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36-54.

Cabinet Office/Detica (2011) The Cost of Cybercrime. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

Cambridge University (n.d.). *Cambridge Crime Harm Index*. https://www.crim.cam.ac.uk/Research/research-tools/cambridge-crime-harm-index/view

Carter, E. (2020) Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud. *British Journal of Criminology*. Retrieved from https://doi.org/10.1093/bjc/azaa072

Collins, M. F. (1988). Some cautionary notes on the use of the Sellin-Wolfgang index of crime seriousness. *Journal of Quantitative Criminology, 4*(1), 61-70.

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(1), 1-12.

CPS (2019). *Cybercrime – prosecution guidance*. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

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.

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.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2), 187-204.

Cross, C., Dragiewicz, M., and Richards, K. (2018). Understanding romance fraud: Insights from domestic violence research. *British Journal of Criminology*, *58*(6), 1303-1322.

Cross, C., Parker, M., and Sansom, D. (2019). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. *International Review of Victimology*, 25(1), 53-69.

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). Responding to cybercrime: Results of a comparison between community members and police personnel. Trends and Issues in Crime and Criminal Justice [electronic resource], (635), 1-20. https://www.aic.gov.au/publications/tandi/tandi635

Deloitte (2020) Reshaping the cybersecurity landscape. https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research*, 19(6), 537-549.

Edwards, I. (2012). Sentencing Councils and Victims. *The Modern Law Review, 75*(3), 324-346.

Forouzan, H., Jahankhani, H., & 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. *Cyber Criminology*, 307-323. https://link.springer.com/chapter/10.1007/978-3-319-97181-0_15

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., & Grimshaw, J. M. (2010). What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology and Health, 25*(10), 1229-1245.

Francis, B., Soothill, K., and Dittrich, R. (2001). A new approach for ranking 'serious' offences. The use of paired-comparisons methodology. *British Journal of Criminology, 41*(4), 726-737.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society*. Addison-Wesley.

Greenfield, V. A., and Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology, 53*(5), 864-885.

Guardian (2011). How an email hacker ruined my life and then tried to sell it back to me. https://www.theguardian.com/technology/2011/oct/16/email-hacker-identity-rowenna-davis

Guest, G., Bunce, A., and Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Family Health International*, 18, 59–82.

Gundur, R. V., Levi, M., Topalli, V., Ouellet, M., Stolyarova, M., Chang, L. Y.-C., & Domínguez Mejía, D. (2021). Evaluating Criminal Transactional Methods in Cyberspace as Understood in an International Context. https://www.crimrxiv.com/pub/48bmtkg0/release/3

Hadlington L, Lumsden K, Black A & Ferra F. (2018). A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. Policing: A Journal of Policy and Practice. 15(1), 34-43.

Henson, B., Reyns, B. W., and Fisher, B. S. (2016). Cybercrime Victimization. In, C., A. Cuevas and C., M. Rennison (eds) The Wiley Handbook on the Psychology of Violence (553-570). Chichester: Wiley.

HM Government (2021) Beating Crime Plan. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1015382/Crime-plan-v10.pdf

HMICFRS (2019) *Cyber: Keep the light on - An inspection of the police response to cyber-dependent crime*. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/cyber-keep-the-light-on-an-inspection-of-the-police-response-to-cyber-dependent-crime.pdf

HMIC (2015) *Real lives, real crimes: A study of digital crime and policing*. https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Holt, T. J., & Bossler, A. M. (2012a). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. American Journal of Criminal Justice, 37(3), 396-412.

Holt, T. J., & Bossler, A. M. (2012b). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. Cyberpsychology, Behavior, and Social Networking, 15(9), 464-472.

Holt, T., Burruss, G., and Bossler, A. (2019). An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society, 29*(8), 906-921.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44-57.

Institute for Government (2019) Police. https://www.instituteforgovernment.org.uk/publication/performance-tracker-2019/police

Jansen, J., and Leukfeldt, E. R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology*, 2(2), 205-228.

Kerr, J., Owen, R., Nicholls, C. M., & Button, M. (2013). Research on sentencing online fraud offences. London: Sentencing Council.

Leukfeldt, E. R., Notté, R. J., and Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims and Offenders*, 15(1), 60-77.

Leveson (2012). *An Inquiry Into The Culture, Practices and Ethics of The Press: Report*. Volumes 1 to 4. London: Stationery Office.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology and Criminal Justice*, *8*(4), 389-419.

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law & Social Change*, 67(1), 77-96.

Levi, M., Doig, A., Gundur, R., Wall, D., Williams, M. (2015). *The Implications of Economic Crime for Policing*. City of London Corporation. http://orca-mwe.cf.ac.uk/88156/1/Economic-Cybercrime-FullReport.pdf

Levi, M., and Jones, S. (1985). Public and police perceptions of crime seriousness in England and Wales. *British Journal of Criminology, 25*(3), 234-250.

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.

McGarry, R., and Walklate, S. (2015). *Victims: Trauma, Testimony and Justice*. Routledge.

McGuire, M., and Dowling, S. (2013). *Cyber crime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75*. Home Office.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

Miller, S. (2011) Witness Statement. Retrieved from http://webarchive.nationalarchives.gov.uk/20140122162525/http://www.levesoninquiry.org.uk/evidence/?witness=sienna-miller

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. International Review of Victimology, 27(3), 272-294.

NZMOJ (2017a). *Justice Sector Seriousness Score (2016 update): FAQs*. https://www.justice.govt.nz/assets/Documents/Publications/2016-FAQs-Seriousness-Scores2.pdf

NZMOJ (2017b). *Justice Sector Seriousness Score (2016 update): Table*. https://www.parliament.nz/resource/en-NZ/QWA_02191_2017/6f5506dca574bfa1ebb737556cd4294340e42278

O'Connell, M. and Whelan, A. (1996). Taking wrongs seriously: Public perceptions of crime seriousness. *British Journal of Criminology, 36*(2), 299-318.

ONS (2016). *Research outputs: developing a Crime Severity Score for England and Wales using data on crimes recorded by the police*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/researchoutputsdevelopingacrimeseverityscoreforenglandandwalesusingdataoncrimesrecordedbythepolice/2016-11-29

ONS (2017). *Crime in England and Wales: year ending Mar 2017*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017

ONS (2019). *Outcomes by Offence data tool*. https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-december-2018

ONS (2020). *Crime in England and Wales: year ending March 2019*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2019#fraud

ONS (2020a) Crime in England and Wales: year ending March 2020. Retrieved from https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2020#:~:text=The%20police%20recorded%205.8%20million,July%202019%20to%20March%202020.&text=Overall%2C%20theft%20offences%20fell%20by,the%20year%20ending%20June%202020

ONS (2021) Crime in England and Wales: year ending March 2021. Appendix Tables. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables

Paek, S. Y., Nalla, M. K., Chun, Y. T., & Lee, J. (2021). The perceived importance of cybercrime control among police officers: Implications for combatting industrial espionage. Sustainability, 13(8), 4351.

Pease, K. (1988). *Judgements of crime seriousness: evidence from the 1984 British Crime Survey*. Home Office.

Sentencing Council (2013) *Fraud, Bribery and Money Laundering Offences Guideline Consultation*. https://www.sentencingcouncil.org.uk/wp-content/uploads/Fraud_Consultation_-_web.pdf

Shapland, J., Willmore, J., and Duff, P. (1985). *Victims in the Criminal Justice System*. Gower Publishing.

Sherman, L., Neyroud, P. W., and Neyroud, E. (2016). The Cambridge crime harm index: Measuring total harm from crime based on sentencing guidelines. *Policing: A Journal of Policy and Practice, 10*(3), 171-183.

Shapland, J., Willmore, J., and Duff, P. (1985). *Victims in the Criminal Justice System*. Gower Publishing.

Spalek, B. (2006). *Crime Victims*. Palgrave.

van de Weijer, S. G., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. European Journal of Criminology, 16(4), 486-508.

Walklate, S. (2012). *Victimology: The Victim and the Criminal Justice Process*. Routledge.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age (Vol. 4)*. Polity.

Wall, D. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology, 22*(1-2), 45-63.

Wolak, J. and Finkelhor, D. (2016). Sextortion: Findings from a survey of 1,631victims. New Hampshire: Crimes Against Children Research Center. Retrieved from http://www.unh.edu/ccrc/pdf/Sextortion_RPT_FNL_rev0803.pdf

Wolfgang, M. E. (Ed.). (1985). *The national survey of crime severity*. US Department of Justice, Bureau of Justice Statistics.

**Author Biographies**

**Professor Mark Button** is Director of the Centre for Counter Fraud Studies at the University of Portsmouth and his research interests include fraud, economic cybercrime, private policing and economic criminology in general.

**Dr David Shepherd** is a Senior Lecturer in at the School of Criminology and Criminal Justice whose research interests include economic crime and economic criminology.

**Dean Blackbourn** is Senior Lecturer at the School of Criminology and Criminal Justice whose research interests include victims of economic crime.

**Dr Lisa Sugiura** is a Reader in Cybercrime and Gender at the School of Criminology and Criminal Justice, University of Portsmouth with a particular interest in researching misogyny online and communities and movements that propagate ideological hatred against marginalised groups.

**Dr Richard Kapend** is a Senior Lecturer at Winchester University specialising in quantitative methods.

**Dr Victoria Wang** is a Reader in Security and Cybercrime at the School of Criminology and Criminal Justice, University of Portsmouth with a particular interest in Phatic Technology Theory for applications in marginalised urban societies, and developing cybersecurity solutions for critical infrastructure.