2019-02-28

Cyber crime: A portrait of the landscape

Furnell, SM

10.1108/JCRPP-07-2018-0021
Journal of Criminological Research, Policy and Practice
Emerald

Cyber crime: A portrait of the landscape

Journal:	*Journal of Criminological Research, Policy and Practice*
Manuscript ID	JCRPP-07-2018-0021.R1
Manuscript Type:	Review Paper
Keywords:	Cyber crime, Malware, Hacking, Ransomware, Fraud, Internet

Invited Paper

Cyber crime: A portrait of the landscape

Introduction

The almost ubiquitous use of information technology, and modern society's increasing dependence upon it, has ushered in new opportunities for criminal activity. Potential victims now have to protect themselves against perpetrators that they cannot see, and against a variety of crime types that can have a significant impact upon both the IT systems and those that use them. The resulting cyber crime has the potential to affect everyone, from large multinational organisations down to individuals. While this also applies to crime in general, a significant difference with cyber crime is that, with large-scale attacks like malware and phishing, the same incident can affect multiple parties at the same time. The Internet has enabled global reach between attackers and victims, as well as the potential for the attacks themselves to have instantaneous effects, irrespective of distance.

The cyber crime problem is not a new one, and related incidents have been occurring in various forms for well over three decades. Cyber security industry reporting suggests that the problem has not been static - the scale and breadth of some particular forms of cyber attack reported by industry appears to have been increasing, as the use of technology has become more widespread and its criminal potential has become more widely recognised. In parallel, the recognition by governments, business, and legal systems has also increased, as has public awareness of at least some of the issues. However, our ability to accurately measure scale and changes in trends for cyber crime (not just attacks), as well as to accurately assess the impacts and harms deriving from successful attacks, has generally been limited.

The aim of the paper is to present a picture of the cyber crime landscape, including the nature of the problem and its prominence within the broader context of reported crime as a whole. Consideration is also given to the tension that exists between usable and accurate classification of cyber crime incidents, recognising the importance of categorisation in terms of what is then measured, which in turn influences how fully we can understand the landscape in practice. In order to frame the discussion alongside clear data, the paper draws upon crime survey findings and reporting structures from relevant UK sources. While these will differ from approaches in other locations, this in itself provides some further evidence of the challenge in assessing cyber crime on a wider, international scale. The discussion ultimately leads to a recognition of the prevalence of technology within the context of crime in general, and a resulting consideration of what should truly be regarded as *cyber* crime, as opposed to cases in which technology has simply become a natural factor within traditional crimes.

Defining Cyber Crime

The problem of crime linked to our use of computers is hardly new, and related literature can be found dating back to the 1970s (McKnight, 1973). However, the nature of the crimes has significantly changed over the years as organisations (and society in general) have become more technology-dependent, and others have found more ways to attack and exploit it. As an

example, back in 1981 the UK Audit Inspectorate's survey of computer fraud was essentially focused around a few categories relating to fraud and theft. By the time the last survey in this series was conducted in 2005[i], the survey title had changed to ICT Fraud and Abuse, and the list of reporting categories had grown to include hacking, denial of service, viruses, and various other entries driven by our widespread technology uptake (Audit Commission, 2005). Mass adoption of the Internet has added various further dimensions to the problem (Jewkes and Yar, 2010), and current surveys routinely add yet more terms, including phishing and ransomware, to the related vocabulary (reflecting the ongoing advance of both the technology and the ways in which users and systems can be attacked). All the while, there remains a lack of clear agreement and consistency around the classification of threats and the crimes related to them.

Indeed, much of the discussion on cyber crime is still dominated by debates around the definition of the term, with an increasing tendency to treat every negative online experience (e.g. bullying, fraud, harassment) as 'cyber crime'. Indeed, a recent volume from McGuire and Holt (2017) encompasses sexual offending, interpersonal violence and intellectual property theft amongst the various categories of digital crime under consideration. Such discussion shows that while cyber crime is a global issue, we are still far from having a harmonised global agreement on either the types of crime, how many there are, or how to handle them. Whilst a seemingly academic debate, a clearer and more consistent understanding of what is meant by cyber crime and how best to record and capture it, is important for informing not only how we understand the threat, but also how we tackle the resulting problems (e.g. from directing the use of suitable safeguards within individual systems and organisations through to the appropriate allocation of policing resources and targeting of public awareness initiatives).

The varying definitions arise in part because the problem is dynamic and changes over time, but also because different sources have tended to assess things from differing perspectives (e.g. some may look particularly at external attacks and consequently exclude internal abuse, whereas others may focus upon malicious code threats and thereby omit other forms of attack) (Furnell et al. 2015). However, from a top-level perspective, definitions provided by the UK's Serious and Organised Crime Strategy usefully distinguish two broad categories as follows (Home Office, 2013):

- **Cyber-dependent crimes**. These are offences that can only be committed by using a computer, computer networks, or other form of ICT. These acts include the spread of viruses and other malicious software, hacking, and distributed denial of service (DDoS) attacks (i.e. the flooding of Internet servers to take down network infrastructure or websites). Cyber-dependent crimes are primarily acts directed against computers or network resources, although there may be secondary outcomes from the attacks, such as fraud.
- **Cyber-enabled crimes**. These are traditional crimes that are increased in scale or reach by the use of computers, computer networks or other ICT. Unlike cyber-dependent crimes, they can still be committed without the use of ICT. Examples can include fraud (including phishing and other online scams), theft, and sexual offending against children.

Beyond this level, there is no definitive (i.e. internationally accepted and consistently used) classification of the cyber crimes themselves, which makes it difficult to track and measure in

[i] Then under the guise of the Inspectorate's successor, the Audit Commission.

terms of both scale and costs. Various other definitions and taxonomies of cyber crime can be readily identified. For example, Anderson et al. (2012) used a definition that incorporates traditional forms of crime, publication of illegal content, and crimes unique to electronic networks. This set is essentially similar to an earlier classification offered by Wall (2007a), which identified computer integrity crime (e.g. hacking and denial of service), computer-assisted crime (e.g. scams and thefts), and computer content crime (e.g. offensive communications). Meanwhile, Wall also splits cyber crime into three alternative categories, namely crimes against the machine, crimes using machines, and crimes in the machine (Wall, 2007b). However, none of these can be considered definitive and so surveys and studies readily classify and count the same aspects in different ways.

As an example, Table 1 compares threat/attack categories from two survey reports that were current at the time of writing, namely the Cyber Security Breaches Survey 2018 from the UK's Department for Digital, Culture, Media and Sport (DCMS, 2018), and the Global Information Security Survey 2017-18 from the professional services and accounting firm Ernst & Young (EY, 2018). Looking at the items listed, there is little doubt that all would have the potential to be regarded as cyber-related criminal activities. However, aside from the fact that the CSBS list has almost twice as many entries, there are also notable differences in both the groupings and granularity, which makes direct comparison rather challenging. For example, 'Phishing' from the GISS set maps onto both 'Fraudulent emails or being directed to fraudulent websites' and 'Others impersonating organisation in emails or online' from the CSBS list (and could also relate to the rather specific category of 'Hacking or attempted hacking of online bank accounts'. Similarly, the GISS item 'Malware' could clearly link to both 'Viruses, spyware or malware' and 'Ransomware' from the CSBS categories. Meanwhile, both lists contain some categories that are presented according to the *type* of attack (e.g. Denial-of-Service, Malware, Phishing), while also having others that are instead linked to the *motive* or *target* of the attack (e.g. bank accounts, to steal financial information, to steal intellectual property).

<Insert Table 1 here>

Of course, each of the surveys would doubtless justify and defend its approach, and none of the categories are argued to be wrong. Nonetheless, the resulting differences certainly do not aid the task of developing a harmonised view, and the two specific examples are indicative of a wider challenge. Indeed, this disparity between different categorisations can fundamentally affect the way in which cyber crime is both understood and measured, the implications of which are further explored in later sections. Prior to this, however, it is also relevant to consider how cyber crime now fits within the overall picture of criminal activity that we are now seeing.

A changing picture of crime

The ability to assess the scale and nature of cyber crime experienced amongst the general public in England and Wales has improved over recent years, particularly with the introduction of new questions and categories in related surveys and reporting. However, in terms of understanding the cyber crime 'landscape' and the scale and nature of these crimes it is important to place it in context of wider, historical crime trends. We know that overall crime volumes (excluding fraud and cyber crime), as measured by the Crime Survey for England and

Wales (CSEW), have been declining since the mid-nineties[ii]. The CSEW is one of the most robust measures for assessing long-term trends in crime victimisation amongst the general public. It is a face-to-face household survey of adults aged over 16, with a nationally representative sample of around 35,000 adults[iii]. However, the CSEW has not historically captured fraud and cyber crime and improvement of cyber crime measures more generally is only something that has happened relatively recently (see discussion in McGuire and Dowling, 2013). January 2017 saw the first published statistics where cyber crime and fraud data were added to the headline crime count in the survey[iv]. The new data showed that in the year ending September 2016, traditional crime totalled 6.2m, but with the inclusion of fraud and cyber crime, the headline crime estimate totalled 11.8m (ONS, 2017). The following year then saw a statistically significant drop of 10% in the estimated total volume of crimes, falling to 10.6m. This also included a 24% fall in the volume of computer misuse crimes recorded and a 10% fall in fraud (ONS, 2018a). Overall, these developments in measurement have dramatically changed our understanding of the crime landscape. In the year ending September 2017, computer misuse crimes formed a larger proportion of CSEW crimes than criminal damage and violence, whilst fraud was on a par with theft (see Figure 1)[v].

<Insert Figure 1 here>

Further breakdown of the CSEW reveals there were an estimated 1.5m computer misuse crimes in the year ending September 2017 (ONS, 2018a). The majority (64%) of computer misuse crimes were computer virus reports, and the remainder (36%) related to unauthorised access (including hacking)[vi]. Interestingly, over half of frauds (56%) were regarded by victims to have been "cyber-related". The definition of cyber-related in this case is fairly broad and can include any use of the Internet or online activity in the commission of the crime. As a result, the "cyber" aspect of the crime may have related to anything from someone installing spyware to undertake an online banking fraud, to a non-existent item being advertised as part of an online shopping fraud. There was an (non-significant) increase in such cyber-related frauds from 53% in year ending September 2016 to 56% in year ending September 2017 (ONS, 2018a). As Table 2 outlines, consumer and retail frauds are notable for their volumes of cyber-related frauds.

<Insert Table 2 here>

Rather than relying upon a single source, the cyber crime landscape needs exploring from a range of perspectives and sources in order to gain a fuller understanding of its scale, nature and changes over time. As such, it is interesting to contrast the CSEW findings against other

[ii] Although more recently the trend has become more stable.

[iii] A major strength of the CSEW is that it captures crimes that are not necessarily reported in an official capacity to the police or other organisations, and is not impacted by changes in police crime recording practices. This makes it an excellent measure of trends over time.

[iv] Fraud and cyber questions were first added to the CSEW in October 2015 as experimental statistics, and asked of a half sample.

[v] CSEW figures are published quarterly on the ONS website and should be consulted to assess the most recent changes in trends.

[vi] Other types of computer misuse (e.g. DDoS) are captured in the survey but exceptionally few are reported.

nationally representative data, and an example here is police recorded crime. Whilst police recorded crime is vulnerable to changes in reporting and recording practices by the public and police, it has a broader coverage than the CSEW as it also includes businesses, tourists and other institutions. It is also a useful source of more high-harm low-volume crimes which are not necessarily picked up by the CSEW. Action Fraud (the national reporting centre for fraud and cyber crime in the UK) and the National Fraud Intelligence Bureau (NFIB) took over responsibility from police for reporting and recording cyber crime and fraud from 2011/12 (although police still hold responsibility for investigating these crimes). Analysis of cyber crime reports made to Action Fraud reveal a different picture to the CSEW. Whilst one in seven crimes recorded by the CSEW in the year to September 2017 was a computer misuse offence, just one in 245 of all Police Recorded crimes was a computer misuse offence (ONS, 2018a). There was a total of 21,745 reported cases of computer *misuse* in England and Wales in the year ending September 2017. Even though this was an increase from the prior year (a 63% increase from 13,309 reports), computer misuse crimes accounted for less than one per cent of all reported crimes.

The disparity between CSEW and recorded crime data serves to highlight the high level of under-reporting that occurs[vii]. Only 4.3% of computer misuse incidents were reported to the police or Action Fraud in the year ending March 2018 (ONS, 2018b). The most commonly reported reason for non-reporting was "haven't heard of Action Fraud", but other reasons (such as not thinking the incident was worth reporting, or not realising it was a crime) also played a part. This probably gives some indication of the perceived seriousness and impact that some of these crimes have upon victims. Reporting of crimes however is important in order to better understand crime patterns and inform the policing response.

The benefit of considering the CSEW and Action Fraud sources in more detail is the ability to consider cyber 'crimes', as opposed to cyber 'attacks'. Cyber security industry reports (e.g. from sources such as F-Secure, Kaspersky Lab, Microsoft, Symantec and others) regularly report changing trends in attacks and their findings are well documented elsewhere, along with the advantages and limitations of using these types of sources (see McGuire and Dowling, 2013). The picture that they tend to present is often a snapshot view of the specific moment in time, highlighting particular incidents or issues that have gained attention in the reporting period. For example, contrasting successive releases of Symantec's Internet Security Threat Report, we see that while the 2017 version gives attention toward targeted attacks, email threats, web attacks, and ransomware (Symantec, 2017), the 2018 release is structured notably differently. While some top-level categories (e.g. ransomware) remain the same, there are also entirely different headings, such as mobile threats and the software supply chain (Symantec, 2018). Thus, while they undoubtedly succeed in providing relevant and topical insights, such reports are less successful in offering a longitudinal view based upon tracking a consistent set of topics.

The challenge of measuring cyber crime

The earlier discussion highlighted the lack of uniform agreement and consistency in terms of defining and categorising cyber crime. Nonetheless, having some formal categorisation and consistency comes to matter when looking to count the related crimes. Moreover, the approach

[vii] Although this will in part be due to the difference coverage of the sources.

used to actually report and record crimes in a policing context can again differ from the categories used in more general business surveys such as those discussed in Table 1.

To look again at a UK example, such counting is based upon formal definitions for cyber crime put in place by the Home Office and the National Fraud Intelligence Bureau (NFIB). The Home Office Counting Rules (HOCR) set out how all reported crimes, as well as cyber crimes, are to be counted and recorded (Home Office, 2018a). Computer misuse crimes are officially recorded under the broader category of fraud. Action Fraud crime recorders are required to identify the relevant crime type based on information provided by the victim (see Table 3). These then go on to inform key measures on police recorded crime, published each quarter by the Office for National Statistics (e.g. ONS, 2017; ONS 2018a). Such crime recording helps to raise awareness of scale and changes over time regarding different crime types, helps with prioritisation and development of appropriate responses to crimes by law enforcement, and helps ensure that victims receive the appropriate service (Home Office, 2014).

<Insert Table 3 here>

The HOCR set out a number of important rules relating to defining and categorising crimes to help ensure consistency and accuracy in recording. These rules apply in principle for all crime types, and each specific crime type listed in the counting rules has its own description and examples of how the rules are to be applied. Key rules include the principal crime rule that relates to recording of the most serious offence where multiple offences occur, and the specific intended victim rule (Home Office, 2018b). These types of rules mean, for example, that 'phishing' would be regarded as an enabler of computer misuse or fraud and so would not be recorded as a crime in itself. The principal goal of the offender's crime (i.e. the resulting computer misuse or fraud) would be recorded instead[viii]. With this in mind, it is generally not possible to know from most of the surveys and other sources on cyber crime whether the crimes being recorded would have been classed as 'crimes' in accordance with the HOCR.

The linking of these rules and categories to recorded crime data gives the opportunity for more fine-grained analysis of the computer misuse crime types. As an illustration, Table 4 compares findings from 2016 and 2017, with notable increases observed in the volume of reported viruses or other malware (up 145%); and also hacking of social media and email accounts (up 92%).

<Insert Table 4 here>

While they provide a reference point for comparison in this context, the categories in Tables 3 and 4 are just one way of viewing the problem. As a contrast, Figure 2 presents the reporting categories offered to respondents in the aforementioned Cyber Security Breaches Survey 2018, along with the extent to which each had been encountered by respondents experiencing a breach in the prior year. While the key themes from the HOCR set are still there, they are

[viii] Furthermore, it is not sufficient to have just received a phishing *attempt* to have a crime recorded. The victim needs to have been specifically targeted and taken positive action in response (for example, upon receipt of the email, clicking the link directing them to a particular website, which then results in malware affecting their computer) – they then become the specific intended victim'.

grouped differently, with hacking-related incidents now getting two categories rather than five, and DoS attacks being covered in a single entry rather than two. Meanwhile, although the category "Viruses, spyware or malware" is ostensibly similar to NFIB 50A, it is notable that ransomware is presented as a distinct issue from the rest of the malware, likely reflecting its prominence at the time[ix].

<Insert Figure 2 here>

Measuring cyber crime costs and harms

An alternative way to assess the cyber crime threat is through consideration of the costs and impacts experienced by individuals and businesses. Having an understanding of the costs of crimes is important to ensure that responses to crime are not simply targeted at those with the greatest volume of incidents, but also those with the greatest level of harm. It is important to know where costs fall (e.g. in prevention of a crime or in a response), what form those costs take and who is most affected (e.g. whether individuals or types of businesses) (Home Office, 2018c).

Available evidence suggests there are a variety of impacts that can result from cyber crime. For businesses, the Cyber Security Breaches Survey documents temporary loss of access to files or networks (reported by 23% businesses) and corruption or damage of software or systems (20%). However, the most commonly reported impact amongst businesses was the need for new security measures (38%), adding to staff time to deal with the breach or inform others about it (34%), and preventing staff from carrying out their daily work (24%). Other less commonly reported impacts included reputational damage, customer complaints, and loss of revenue.

Amongst members of the public, around one quarter of all computer misuse incidents reported in the CSEW resulted in the loss of money or goods, for year ending September 2017 (ONS, 2018a). Of those that did experience a financial loss, around one per cent received full reimbursement for this loss.

However, providing an accurate estimate of the total cost of cyber crime is no easy task. A report from the Costs of Cyber Crime Working Group (Home Office, 2018c) clearly outlines the challenges in formulating an accurate assessment and the limitations of a range of past efforts to calculate those costs. The report outlines how previous assessments of cost have typically been limited by inconsistent definitions of both 'cyber crime', insufficient consideration of the full range of potential resulting costs and varying types of costs being considered in the available estimates (e.g. sometimes intellectual property theft was included in an estimate, sometimes not). Fundamentally many studies simply did not measure the same thing (e.g. costs per incident vs, costs per year) making comparisons very difficult. The challenges in capturing more intangible costs associated with reputational damage from cyber attacks, was also noted.

[ix] Ransomware is not distinctly specified in the HOCR, but is an example of where it would actually be helpful to have more fine-grained breakdown of some of the recorded crimes, in order to see how much of an issue ransomware has become when compared to other problems.

Overall, the Costs of Cyber Crime Working Group report recommended further research for understanding costs of cyber crime, suggesting a broad framework to enable more consistent assessments of costs and harms. This framework draws upon three key dimensions previously used to assess costs associated with traditional crime:

- Costs in anticipation - e.g. defensive measures taken to prevent crime, such expenditure on anti-virus software.
- Costs as a consequence – e.g. those occurring as an immediate result of a crime, such as property damage or money lost, but also potentially encompassing emotional and physical harms from the crime. Victims may have little control of these costs.
- Costs in response – e.g. responses provided by police forces and the criminal justice system. These are costs for which there is likely to be more control.

Further developments in this space can be found in a more recent Home Office publication, 'the economic and social costs of crime' (Home Office, 2018d). Using the above framework, this report included an estimate for the first time of the cost of cyber crime - estimating this to be £1.1bn in 2015/16. However, it should be noted the estimate is regarded as partial (it excludes some key costs, such as those to businesses) and it also draws upon experimental CSEW statistics.

Once again though, our ability to apply clear and consistent definitions in the way we capture data on cyber crime will be key to informing the understanding in this area. With this information we can further build knowledge of the changing threat picture, as well as raise awareness of cyber crime and its impacts amongst law enforcement and those who can help tackle the problem. This will help enable more informed decisions about priorities and direct the appropriate awareness raising and prevention initiatives towards those who are most vulnerable.

Adding depth of classification

As we have seen, the way things are labelled and grouped makes a difference to what is counted. So, for example, while there are five variants of hacking under NFIB 52, there is only a single entry for 'Computer viruses / malware / spyware', suggesting less granularity of recording in this area. Indeed, even the label itself prompts some discussion here, as the category might more reasonably be called 'Malware' (on the basis that viruses and spyware are actually two specific examples of the wider issue). Indeed, the broad category doubtless hides more specific issues within it, and so provides a good opportunity to show how a particular category of cyber crime can be decomposed to differing levels of detail – as well as the implications and value (or otherwise) of doing so.

Viruses were the first form of malware to come to widespread attention, in the latter half of the 1980s, and the term has tended to become lodged in the public consciousness as a catch-all label. However, there are several other top-level classifications of malware that sit equally alongside it, several of which have been the more prevalent problems in recent years:

- **Virus** - A *non-autonomous* program that replicates and spreads by infecting (attaching itself to) systems, programs or files.
- **Worm** - Code that is able to replicate and spread *autonomously* through systems and networks.

- **Trojan horse** - A program containing unexpected hidden functionality, potentially operating alongside expected behaviour
- **Software Bomb** – An element of malicious code, typically hidden within a larger program, that is activated on the basis of either a time-based trigger (time bomb) or a logical condition being met (logic bomb).

Although listed distinctly, these categories are not mutually exclusive, and may often be used in concert (e.g. a worm that distributes a Trojan, which then activates based on a particular date or after a period of time has elapsed). Moreover, the variety of malware classification does not end here, and there are further categories and variations that name the malware based upon the purposes for which the techniques are being applied (and it is worth noting at this point that even the definitions are not definitive):

- **Adware** – software that automatically displays banner or pop-up advertisements, or redirect search requests to advertising websites. Adware is not necessarily malware, can be classed as such when used in the hands of cybercriminals.
- **Crimeware** – a broad category, referring to malware designed to conduct or enable illegal online activities.
- **Ransomware** – malware that blocks users' access to their data (typically by encrypting it) unless a ransom is paid to recover it.
- **Spyware** – malware designed to gather and share information without the knowledge of the individual or organisation using the infected system.

Looking beneath this level there are various methods and techniques that can also be identified, such as keylogging and browser hijacking, which may be form part of the way in which categories such as spyware and crimeware conduct their activities. To add to the potential for confusion, however, it is not uncommon to find keyloggers and browser hijackers also being referred to as forms of malware in their own right! Cyber security industry sources are more likely to refer to more fine-grained detail when reporting on types of cyber crime, however even then there is variation amongst reports and companies in terms of what is being reported, how it's measured and what geographic coverage is being adopted (see McGuire and Dowling, 2013) for more discussion on these issues). So again, a clear understanding of the domain can be complicated by the varying ways in which different parties choose to view it. While on one level this may seem like a pedantic discussion of wording, it has a genuine impact in terms of the ability to count, analyse, and understand the nature of the issues being reported.

Indeed, such a breakdown could be further extended across other computer misuse categories as well[x]. However, aside from being potentially tedious, this would *still* not serve to yield a definitive or exhaustive list. It is also unlikely that any victims would be able to accurately categorise the more detailed crime types, or in many cases provide any clear sense of attribution to the crime they experienced (for example, was money stolen from their online bank account a result of a virus or some other fraudulent method to obtain their funds?). At best, it would be a point-in-time snapshot, as the field is dynamic and the underlying labels are liable to ongoing expansion as new attacks and exploits emerge. Indeed, experience suggests that threats rise and fall, and some tend to be more in focus than others at different points. For example, at the

[x] Phishing, for instance, can be further split down into categories including spear phishing (targeted at specific individuals or companies), whaling (targeting high-profile/high-value individuals within organisations), and catphishing (targeting individuals via online dating sites).

time of writing, significant attention has been devoted towards ransomware, in the wake of incidents such as WannaCry and Petya (Burgess, 2017). Meanwhile, phishing and mass exposure of user accounts are other examples of themes that have caught the headlines at different points. At the same time, other forms of cyber crime remain an ongoing concern, and nothing really disappears entirely.

As indicated, the specific fine-grained details of the incident types are not relevant to all scenarios. From the victim perspective, there is not necessarily anything they would need to *do* differently in order to protect themselves against ransomware versus other types of malware. However, the details *are* relevant in order to understand how the attackers are operating and the methods they are using (e.g. how easily others might adopt them, how they might use them, and the potential for related incidents to spike as a result).

Every crime a 'cyber' crime?

As we move forward, there will be an undoubted broadening of cyber crime into new contexts. One perspective here is which technologies will be targeted and exploited for criminal purposes. Experience has already shown that cybercriminals readily embrace new technologies as new routes, with attacks tailored to mobile devices having been a good example of this. As technologies advance, there are clearly new opportunities to be had via routes such as the Internet of Things (IoT), smart homes, and autonomous vehicles. Indeed, we have already seen early evidence of exploitation, with the Mirai botnet having caused a widespread denial of service attack via vulnerable IoT devices in late 2016 (US-CERT, 2016). Similarly, research published at the time of writing revealed vulnerabilities in the Controller Area Network (CAN) protocol used within the vehicular internal networks of modern vehicles, which could be used to disable safety features and other internal components (Greenberg, 2017).

The earlier section made the distinction between cyber-dependent and cyber-enabled crimes, and this is indeed relevant if looking to broadly categorise them or start to build a taxonomy. However, with technology becoming ever more pervasive, will there come a point that the *cyber* prefix essentially becomes redundant, because so many forms of crime involve an IT element that it just merges into the background and becomes implicit? Even now, what categories of physical world crime do not have a 'cyber', or 'cyber-enabled', equivalent? Financially-motivated crimes are already there. Fraud, theft, blackmail, and ransom – all have made a transition into the cyber context, not least because it now represents the natural one in which the opportunities will arise. Additionally, we have seen problems such as harassment, stalking, child sexual offences, and other interpersonal offences also acquire the cyber label. Indeed, in many ways the technology has again served the role as both an enabler and an amplifier for these, with online messaging and social networks providing the means to find, monitor and contact potential victims in a way that was not previously possible. Meanwhile, technology has also provided the means for perpetrators to try to hide and disguise their activities, through the use of techniques such as network anonymisers and cryptography.

It is interesting to get a direct measure of the extent to which this transition to the 'cyber' context has already taken effect. Unfortunately, there is no straightforward way to identify crimes conducted online in police recorded crime data, as enablers have not historically been captured in a systematic fashion. However, attempts have recently been made in England and Wales to better understand the volume of traditional crime that is conducted online via the introduction of an online crime 'flag' which police can apply to their crime reports. The

experimental data available for year ending September 2017, suggests that just 1% of all crime reports received by police was conducted online (ONS, 2018a). This appears instinctively too low and the reason the data remain experimental is that the quality being provided is poor and it is generally regarded that such crimes are not being flagged where they should be. Nonetheless, Figure 3 provides some sense of the distribution of all crimes flagged as 'online'. Unsurprisingly harassment crimes represent the highest proportion (61%) of all 'flagged' crimes. However, the published findings also indicate that for some crime categories flagging is not as prominent as might be expected. For example, 44% of all obscene publications offences (which is where indecent imagery offences would be recorded) were flagged as online, and is rather lower than might be expected. Further work needs to be done to improve the quality of the reporting to help improve our picture here.

<Insert Figure 3 here>

There is less direct parallel for some other physical crimes against people and things, but it is not infeasible to imagine a 'cyber' element becoming involved, particularly with the rise of the Internet of Things as an enabling platform. For example, hacking someone's medical device and causing it to kill them could easily justify the moniker of *cyber murder*, while causing a device to overheat could be a means of *cyber arson*. Offences such as *cyber assault* and even *cyber rape* are not inconceivable if one extends the use and potential exploitation of vulnerable technologies far enough. Indeed, using assault as an illustration, an example reported during the writing of this paper referred to a vulnerability in a car wash system being exploitable to cause to vehicles and physical attacks upon the people in them (Bisson, 2017).

However, while the Internet or other technology may be *involved in* the commission of many different types of crimes, it is arguable that the *cyber* part is not the aspect that we ultimately care about; in these cases it is part of the means rather than the end. Many are simply traditional crimes committed using a different medium – they are not new crimes, nor are they necessarily that different to their offline form. Arguably then, not all crimes should be classified as "cyber crimes". An alternative, purer framing of cyber crime would be one where only those offences that are cyber-dependent crimes (i.e. Computer Misuse Act crimes) are included. This would identify those crimes where the technology aspect is both the means *and* the target of the attack. The category of 'cyber-enabled' crime would then be reserved for offences where a traditional crime has been committed, but there has also been a clear Computer Misuse Act component involved (e.g. malware used to steal money from an online bank account). Collectively these offences would then be classed as true *cyber* crimes. This may help prevent increasing numbers of offences becoming classed as "cyber" crimes. All other crimes where the Internet or other technology is involved for purposes of communication, or facilitation - but has no element of computer misuse - would simply be labelled within the broader crime type that they represent. As such, online auction fraud would simply be classed as fraud; harassment via social media would simply be harassment, and so on.

Conclusions

Developments in how cyber crime is measured (e.g. through the Crime Survey, Action Fraud) means that we now have improved understanding of the scale and nature of cyber crimes experienced by the general population. We also have better understanding of how cyber crime

victimisation compares to other crime types. Better evidencing both scale and harms from cyber crime is important for informing appropriate responses to tackling cyber crime and also raising awareness amongst the general public and businesses of the need to undertake appropriate protective behaviours. In order to do this, there is a need to more consistently and accurately define what is meant by cyber crime and how to continue improving how we measure both the volume of incidents and the range of impacts or costs resulting from it.

Accurate measurement of the scale and harms associated with particular forms of cyber crime is crucial to informing the extent and nature of policy, law enforcement and other responses directed at these crimes. Whilst not all crimes committed using the Internet or technology would require the same *type* of law enforcement response, the key safeguards and protective measures used by the public and businesses to protect against cyber crime are often fairly standard, and many of them apply across several online threats, as well as to supporting security beyond the specific scope of cyber crime.

However, there is also the question of what definition, categorisation or information about a crime do victims need to know to determine when, if, or how to report it to the appropriate authorities; or to trigger them to enact the necessary behaviour changes to better protect themselves in future. Clearly there are a number of levels of detail at which cyber crimes could be classed. However only a small group of individuals involved in responding to the threat are likely to need the most granular information. In most cases we do not need to know the minutiae of the threats; we can simply accept that they exist, that they are significant, and that protection is required. Nonetheless, this is perhaps easier said than done for large proportions of the population. Indeed, there remain a number of challenges in informing public perceptions of cyber crime, raising awareness and changing behaviours – and based on the available evidence it would seem neither individuals nor businesses have yet developed sufficient awareness or the necessary behaviours. That being said, it is likely that a number of common cyber security behaviours (e.g. implementing strong passwords) may help to protect against a range of online threats. However, the human factors involved (e.g. being tricked into sharing a strong password) means that people may still be susceptible to a range of different crimes – some will be 'true' cyber crimes, others will be traditional crimes now conducted online.

Whilst the growing awareness of cyber crime is important, the varying definitions and the tendency to then treat every negative experience online as 'cyber crime' is probably less helpful. Not all crimes committed using the Internet or computers will require the same types of law enforcement response to tackle it. For example, a fraudulent eBay advertisement, an online harassment case, and a ransomware attack on a business are likely to warrant different responses and require different expertise to address. What degree of categorisation however is needed in order to provide the appropriate level of response? We would argue that at least generating a clearer distinction where 'true' cyber crimes are only those which are genuine cyber-dependent crimes and/or involve clear elements of Computer Misuse Act legislation, could help ensure that the appropriate response is directed to these types of crimes. It may also help to tackle general misnomers that anything with the prefix of 'cyber' is somehow scary, new, complicated or generally too difficult to deal with.

References

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T. and Savage, S. 2012. *Measuring the cost of cyber crime*. Available at: http://www.econinfosec.org/archive/weis2012/papers/Anderson_WEIS2012.pdf.

Audit Commission. 2005. *ICT fraud and abuse 2004 - An update to yourbusiness@risk. Public sector Update*. June 2005. ISBN 186240 507 7.

Bisson, D. 2017. "Car wash security flaws let hackers 'physically attack' people", Cluley Associates Limited, 29 July 2017. https://www.grahamcluley.com/car-wash-security-flaws-let-hackers-physically-attack-people/

Burgess, M. 2017. "WannaCry and Petya are just the beginning. It's going to be an 'ugly few years'", Wired.com, 29 June 2017. http://www.wired.co.uk/article/whats-next-petya-ransomware-wannacry

DCMS. 2018. *Cyber Security Breaches Survey 2018*. Main report. Department for Culture, Media & Sport, April 2018, London, UK. https://www.ipsos.com/sites/default/files/ct/publication/documents/2018-04/cyber-security-breaches-survey-2018-main-report.pdf.

EY. 2018. *Cybersecurity regained: preparing to face cyber attacks: 20th Global Information Security Survey 2017–18*. EYG no. 06574-173Gbl. ey.com/giss

Furnell, S., Emm, D. and Papadaki, M. 2015. "The challenge of measuring cyber- dependent crimes", *Computer Fraud and Security*, October 2015, pp5-12.

Greenberg, A. 2017. "A deep flaw in your car lets hackers shut down safety features", Wired.com, 16 August 2017. https://www.wired.com/story/car-hack-shut-down-safety-features/

Home Office. 2013. *Serious and Organised Crime Strategy*. Cm 8715, October 2013. ISBN 9780101871525

Home Office. 2014. "Vision and Purpose Statements for Crime Recording (NCRS & HOCR)", *Home Office Counting Rules For Recorded Crime*, April 2014. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387762/count-vision-december-2014.pdf.

Home Office. 2018a. "Fraud", *Home Office Counting Rules For Recorded Crime*, April 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694449/count-fraud-apr-2018.pdf.

Home Office. 2018b. "Crime Recording General Rules", *Home Office Counting Rules For Recorded Crime*, April 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721595/count-general-jul-2018.pdf.

Home Office. 2018c. *Understanding the costs of cyber crime: A report of key findings from the Costs of Cyber Crime Working Group*. Research Report 96. Home Office Science Advisory

Council. January 2018. https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime

Home Office. 2018d. *The economic and social costs of crime, second edition*. Research Report 99. July 2018. London: Home Office. Available at: https://www.gov.uk/government/publications/the-economic-and-social-costs-of-crime

Jewkes, Y. and Yar, M. 2010. *Handbook of Internet Crime*. Willan Publishing, Cullompton, UK.

McGuire, M. and Dowling, S**.** 2013. *Cyber Crime: A Review of the Evidence.* Home Office Research Report 75. October 2013. London: Home Office. Available at: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

McGuire, M.R. and Holt, T.J. 2017. *The Routledge Handbook of Technology, Crime and Justice*. Routledge International Handbooks, Routledge, Abingdon, UK.

McKnight, G. 1973. *Computer Crime*. Michael Joseph Limited, London, UK.

ONS. 2017. "Crime in England and Wales: year ending Mar 2017", Statistical Bulletin, Office for National Statistics, 20 July 2017.

ONS. 2018a. "Crime in England and Wales: year ending September 2017", Statistical Bulletin, Office for National Statistics, 25 January 2018.

ONS. 2018b. "Crime in England and Wales: year ending March 2018" Statistical Bulletin, Office for National Statistics, 19 July 2018.

Symantec. 2017. Internet Security Threat Report. Volume 22. Symantec Corporation, April 2017. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Symantec. 2018. Internet Security Threat Report. Volume 23. Symantec Corporation, March 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

US-CERT. 2016. "Heightened DDoS Threat Posed by Mirai and Other Botnets", Alert TA16-288A, United States Computer Emergency Readiness Team, 14 October 2016. https://www.us-cert.gov/ncas/alerts/TA16-288A.

Wall, D.S. 2007a. *Cybercrime*. Polity Press, Cambridge, UK.

Wall, D.S. 2007b. "Policing cyber crimes: Situating the public police in networks of security within cyberspace", *Police Practice & Research: An International Journal*, 8 (2), pp 183–205.

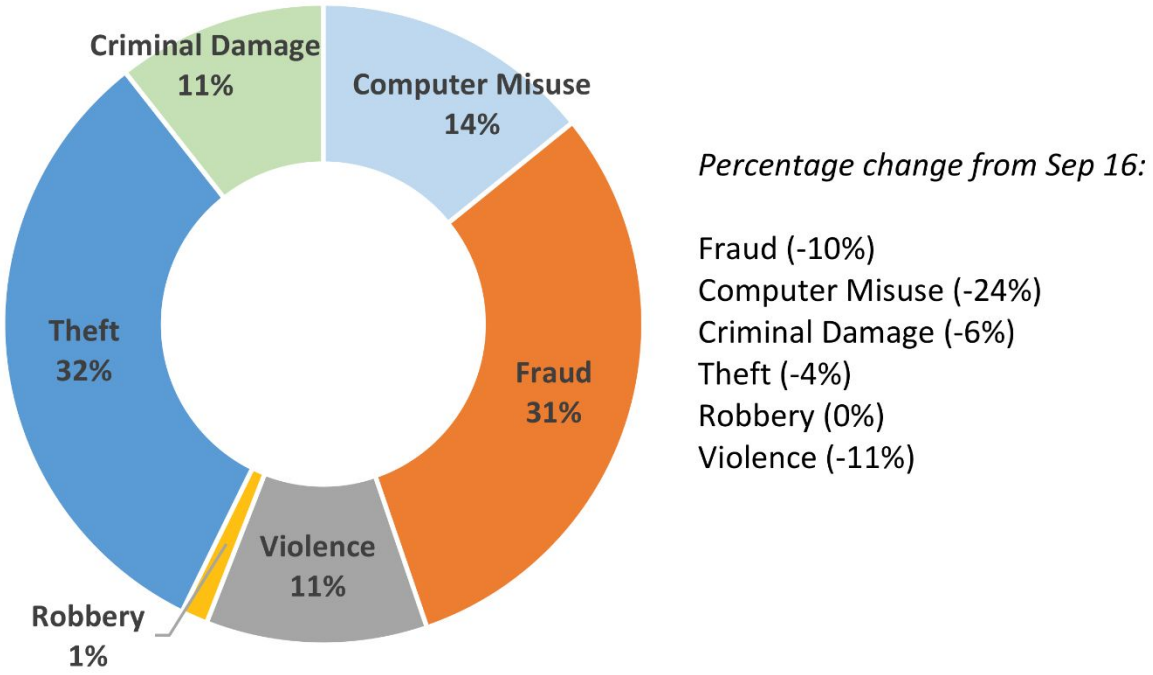

Figure 1: Breakdown of CSEW crime types (year ending Sept 2017) and percentage change from year ending Sept. 2016

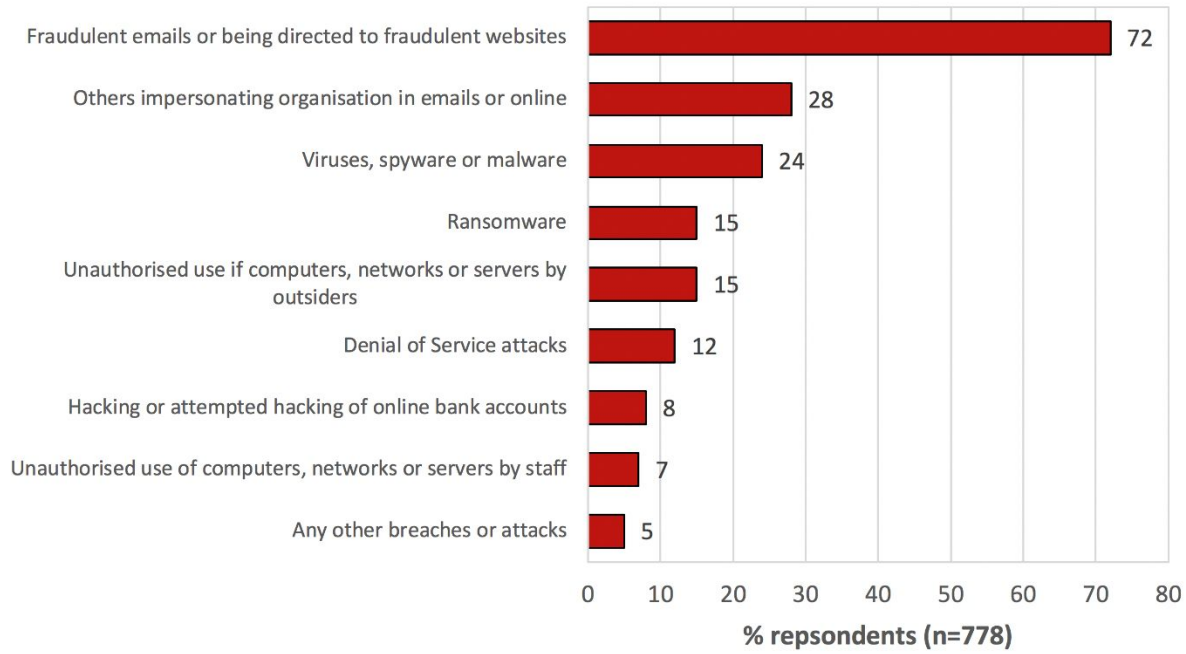

Figure 2: Attacks reported in the Cyber Security Breaches Survey 2018

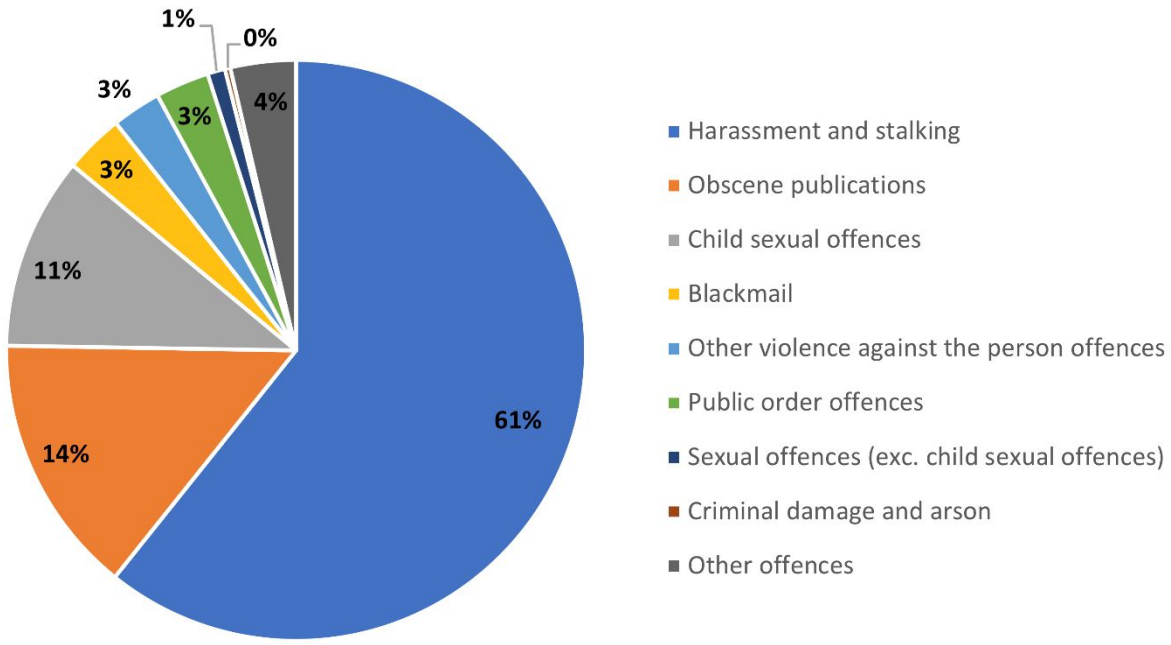

Figure 3: Proportion of all offences recorded by police and flagged as 'online' crime, experimental statistics, year ending Sept 2017

Types of breaches or attacks (CSBS 2018)	**Threats increasing risk exposure** (GISS 2017-18)
• Denial-of-service attacks • Fraudulent emails or being directed to fraudulent websites • Hacking or attempted hacking of online bank accounts • Others impersonating organisation in emails or online • Ransomware • Unauthorised use of computers, networks or servers by outsiders • Unauthorised use of computers, networks or servers by staff • Viruses, spyware or malware	• Cyber attacks to steal financial information • Cyber attacks to steal IP or data • Internal attacks • Malware • Phishing

Table 1: Comparison of attack categories used by prominent security surveys

	Number of CSEW crimes, Oct 15 - Sep 16 (thousands)	Number of CSEW crimes, Oct 16 to Sep 17 (thousands)	Percentage change (%)	Proportion flagged as cyber-related, year ending Sep 2017 (%)
Fraud	**3,617**	**3,239**	**-10**	**56**
Bank and credit account fraud	2,452	2,390	-3	49
Consumer and retail fraud	939	747	-20	81
Advance fee fraud	118	56	-53	-
Other fraud	108	46	-57	-
Computer Misuse	**1,966**	**1,503**	**-24**	**97**
Computer virus	1,300	962	-26	
Unauthorised access (including hacking)	667	541	-19	
Total fraud and computer misuse	**5,583**	**4,742**	**-15**	

Table 2: Breakdown of CSEW fraud and computer misuse crimes and proportion flagged as "cyber- related", year ending Sept 16 and Sept 17

NFIB Code	Crime type
NFIB50	Computer misuse crime
NFIB 50A	Computer viruses / malware / spyware
NFIB 51A	Denial of service attack
NFIB 51B	Denial of service attack (extortion)
NFIB 52A	Hacking - server
NFIB 52B	Hacking – personal
NFIB 52C	Hacking – social media and email
NFIB 52D	Computer hacking – pbx / dial through
NFIB 52E	Hacking / extortion

Table 3: Home Office Counting Rules for Computer Misuse Crimes

Computer misuse crime type	Year ending Sep 2016	Year ending Sep 2017	% change
Computer viruses/malware	3,389	8,292	145
Denial of service attack	571	315	-45
Denial of service attack (extortion)	394	288	-27
Hacking – server	564	699	24
Hacking – personal	3,053	3,584	17
Hacking – social media and email	3,710	7,116	92
Hacking – PBX/dial through	538	420	-22
Hacking (extortion)	1,090	1,031	-5
Total all computer misuse crimes	**13,309**	**21,745**	**63**

Table 4: Breakdown of computer misuse crimes reported to Action Fraud / NFIB, year ending Sept 2017

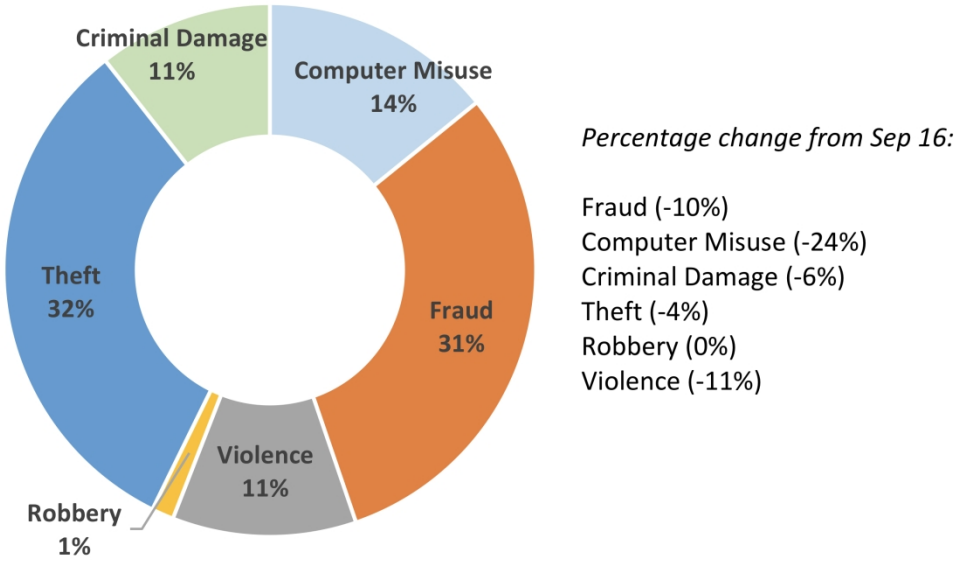

Figure 1: Breakdown of CSEW crime types (year ending Sept 2017) and percentage change from year ending Sept. 2016

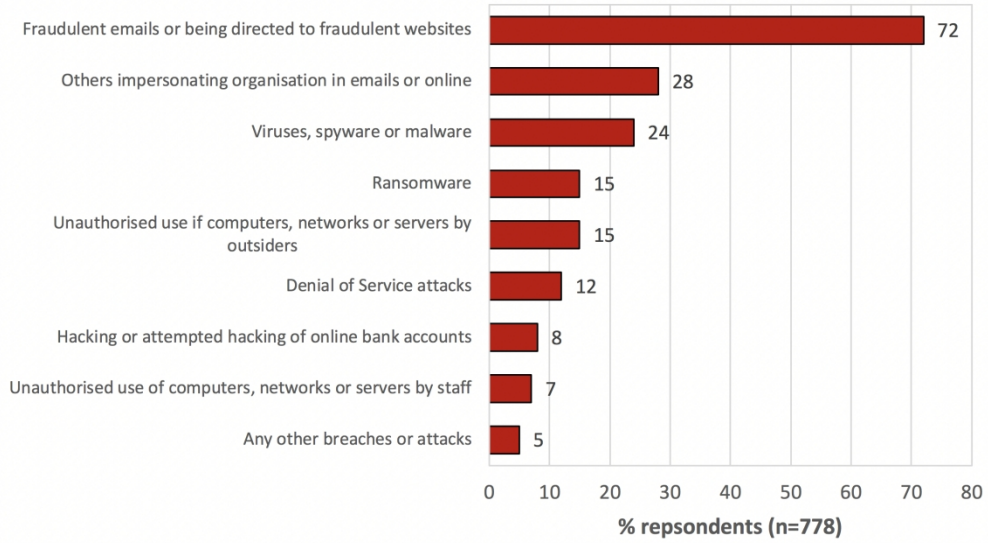

Figure 2: Attacks reported in the Cyber Security Breaches Survey 2018

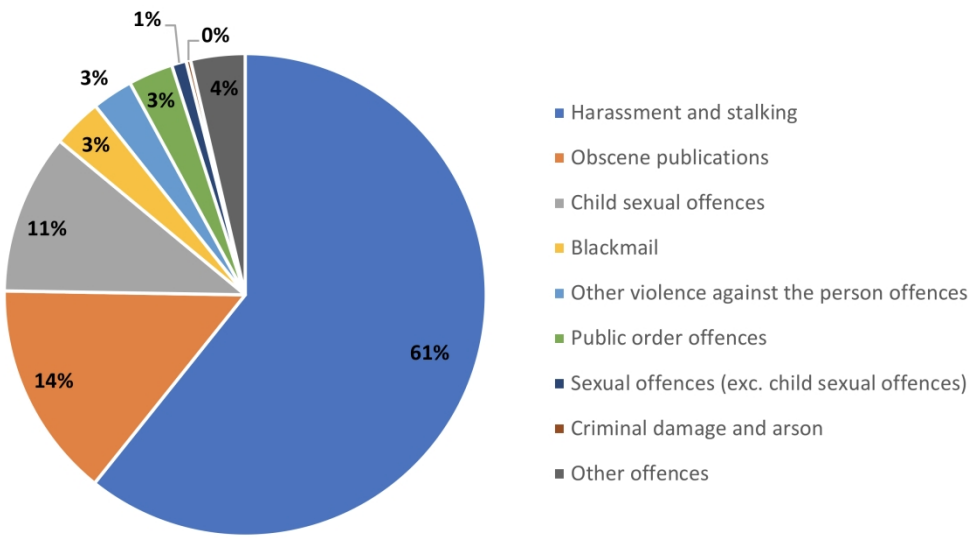

Figure 3: Proportion of offences recorded by police and flagged as 'online' crime, experimental statistics, year ending Sept 2017