Home Office

Cyber crime: A review of the evidence

Research Report 75

Summary of key findings and implications

Dr. Mike McGuire (University of Surrey) and
Samantha Dowling (Home Office Science)

October 2013

Cyber crime: A review of the evidence

Summary of key findings and implications

Home Office Research Report 75

October 2013

Dr. Mike McGuire (University of Surrey) and Samantha Dowling (Home Office Science)

Acknowledgements

With thanks to: Andy Feist, Angela Scholes, Ian Caplan, Justin Millar, Steve Bond, Jackie Hoare, Jenny Allan, Laura Williams, Amy Everton, Steve Proffitt, John Fowler, David Mair, Clare Sutherland, Magali Barnoux, Mike Warren, Amanda White, Sam Brand, TSIP, Prof. Majid Yar, Dr.Steve Furnell, Dr. Jo Bryce, Dr Emily Finch and Dr. Tom Holt.

Disclaimer

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).

Contents

Introduction	4
Defining cyber crime	5
Key findings	6
References	16
Annex A: Methodology	21
Annex B: A survey of public attitudes to internet security : Key findings	23

Introduction

The development of the internet and digital technologies represent a major opportunity for the UK – transforming businesses and providing new tools for everyday communication. According to survey data from the Office for National Statistics (ONS), 80 per cent of households in Great Britain had an internet connection in 2012, up from 77 per cent in 2011 (ONS, 2012a). Internet users are spending increasing amounts of time online and undertaking a greater range of online and social networking activities (Ofcom, 2012). In terms of business, online retail spending in 2012 accounted for around 10 per cent of all retail spend each month in Great Britain. The average weekly spend online was £586.6 million in July 2013 – an increase of almost 11 per cent compared with July 2012 (ONS, 2013a). The internet and online activities have now become central to the way people live their lives.

However, the internet also presents opportunities to cyber criminals. The nature of some 'traditional' crime types has been transformed by the use of computers and other information communications technology (ICT) in terms of its scale and reach, with risks extending to many aspects of social life, such as:

- financial transactions;
- sexual offending;
- harassment and threatening behaviour; and
- commercial damage and disorder.

New forms of criminal activity have also been developed, targeting the integrity of computers and computer networks such as the spread of malware and hacking. Threats exist not just to individuals and businesses, but to national security and infrastructure. Furthermore, the borderless nature of cyber crime means that the UK can be targeted from jurisdictions across the world, making law enforcement particularly challenging.

The cyber threat has been assigned a 'Tier One' threat status in the national security strategy (HMSO, 2010) – one of the highest priorities for action. To assist in tackling the cyber threat, £860 million of public funding was set aside as part of a five-year National Cyber Security Programme. The national cyber security strategy (Cabinet Office, 2011) sets out the key objectives that the Government intends to achieve by 2015 in relation to cyber security and cyber crime, to both tackle the threats and reap the benefits of cyberspace. Additionally, in 2013 the new National Crime Agency (NCA) brought together specialist law enforcement capability into a National Cyber Crime Unit (NCCU) to address some of the most serious forms of cyber crime. The new Serious and Organised Crime Strategy, issued alongside the launch of the NCA, sets out the framework and direction for those tackling on serious and organised crimes, which can also include cyber crimes.

It is critical for policy makers to have knowledge of the scale and nature of cyber crime, how it is changing over time and whether interventions to tackle the problem are having an impact. This will help to drive forward policy decisions with a sound evidence base in this area and is vital in the context of emerging forms of cyber crime and technological developments.

This paper provides an overview of the current published evidence on the scale and nature of cyber crime in the UK – to identify what is known, where evidence is most reliable and where major gaps remain. The paper:

- collates a comprehensive evidence base regarding cyber crime in the UK, identifying data, analysis and research from published academic, industry and government sources;
- considers the reliability, objectivity and quality of available evidence, indicating the extent that available data sources can be relied on; and

- focuses on cyber-dependent crime and specific forms of cyber-enabled crimes – fraud and theft, and sexual offending against children. These are areas where there is more, higher-quality evidence available than for other forms of cyber crime.

This summary paper is accompanied by four additional detailed chapters.

- **Chapter 1:** Cyber-dependent crime.
- **Chapter 2:** Cyber-enabled crime: Fraud and theft.
- **Chapter 3:** Cyber-enabled crime: Sexual offending against children.
- **Chapter 4:** Improving the cyber crime evidence base.

A brief outline of findings relating to online stalking and hate crime is included in this summary, but given the limited evidence available is not discussed in a more detailed chapter. Cyberbullying was excluded from discussion as the focus of this review is on crime and cyberbullying is not classed as a crime. Research on cyberbullying has also been covered extensively in other literature, see, for example, Livingstone *et al*. (2011). Cyberterrorism was outside the scope of this review.

Defining cyber crime

This review is set within the context of 'what is illegal offline is illegal online'.[1] Specific offences most commonly associated with cyber-dependent crimes, such as hacking and the creation or distribution of malware, are defined in the Computer Misuse Act 1990[2].

Cyber crime is an umbrella term used to describe two distinct, but closely related criminal activities: cyber-dependent and cyber-enabled crimes. In this review the use of 'cyber crime' refers to both forms of criminal activity, and we distinguish between them as outlined below.

- *Cyber-dependent crimes* 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* are traditional crimes that are increased in their 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. For the purposes of this review the following types of cyber-enabled crimes are included:

    - fraud (including mass-marketing frauds, 'phishing' e-mails and other scams; online banking and e-commerce frauds);
    - theft (including theft of personal information and identification-related data); and
    - sexual offending against children (including grooming, and the possession, creation and/or distribution of sexual imagery).

The methodology for the review is set out in **Annex A**. Key findings from a survey of public attitudes towards internet security conducted by Ipsos MORI (2013) are also published alongside the evidence review and are outlined in **Annex B**.

[1] http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf
[2] As amended by the Police and Justice Act 2006.

Key findings

Cyber-dependent crime

Public and business experiences of negative online incidents

In 2011/12 over one-third (37%) of adult internet users reported experiencing a negative online incident in the past 12 months, but these experiences would often be below the threshold of a recorded crime. According to the Crime Survey for England and Wales (CSEW), the proportion of adult internet users reporting a negative online experience declined from 39 per cent in 2010/11 to 37 per cent in 2011/12 (ONS, 2011; ONS, 2012b). This was a small but statistically significant decrease, occurring largely as a result of a significant decline in the proportion of users experiencing viruses. The CSEW data does not, however, relate to criminal activity per se and these negative experiences would often not be classed as 'crimes' under the usual Home Office Counting Rules (HOCR) for Notifiable Crime[3].

Computer viruses are one of the most common negative experiences reported, although the proportion of adult internet users experiencing them appears to have declined. Experiences of hacking, on the other hand, appear to have increased. Almost one-third (31%) of adult internet users in 2011/12 reported receiving a computer virus[4] in the past year (ONS, 2012b). CSEW data also show that the proportion experiencing viruses appears to have fallen – from a high point of 41 per cent in 2005/06 (ONS, 2006) [5]. The proportion of adult internet users experiencing hacking were lower than for viruses – seven per cent of adult internet users experienced unauthorised access to, or use of, personal data in the past 12 months (ONS, 2012b). This was a statistically significant increase from two per cent in 2006/07 (ONS, 2007). In comparison, three per cent of adult internet users had lost money[6] whilst using the internet in 2011/12. As above, these incidents do not necessarily relate to criminal activity.

In 2012, eight per cent of business premises (across four business sectors: accommodation and food; wholesale and retail; manufacturing; and transportation and storage) experienced at least one type of online crime during the past 12 months. According to the 2012 Commercial Victimisation Survey (CVS; Home Office, 2013a) this equated to an estimated 180,000 incidents of online 'crime' in total across the four sectors in the 12 months prior to the survey. Three-quarters of these incidents (135,000) related to viruses. The results of the CVS are representative of crime against the four sectors covered, but are not representative of crime against businesses as a whole. In addition, the CVS is a premises-based (rather than head office-based) survey and so many types of online crime may not be picked up by the CVS as they do not affect businesses at the premises level. Whilst the CVS asked respondents about online crime, as with the CSEW, it is not necessarily the case that all of the incidents would be classed as 'crimes' under the HOCR.

Under-reporting of both cyber-dependent and cyber-enabled crimes is an issue amongst the general public and businesses. Businesses across the four sectors

[3] Police recording of crimes is governed by the National Crime Recording Standard (NCRS) and the Home Office Counting Rules. These set out the principles under which reports received from victims are recorded. Police recorded crime statistics are based on a notifiable list of offences. The Home Office Counting Rules set out the broad classification groups into which those offences are managed for statistical purposes.
[4] Although it is not clear from the survey question whether computers were actually infected and some damage was caused, or if this relates to viruses captured by anti-virus software, for example.
[5] There was a change in question wording in the CSEW during the time so figures are not directly comparable. Questions were also not asked every year.
[6] However, it is not known how the money was lost and whether all responses relate to criminal activity.

reported just two per cent of online crime incidents to the police (CVS; Home Office, 2013b). Under-reporting occurred because incidents were perceived as too trivial and/or were dealt with internally. Other research suggests that concern over reputational damage further contributes to under-reporting (Fafinski and Minassian, 2009). Earlier findings from the CSEW (ONS, 2007) reveal a similar picture for members of the public – just one per cent of adult internet users who experienced hacking or unauthorised access to their data in the 12 months prior to the survey reported this to the police. Under-reporting occurs for several reasons:

- not perceiving that what had taken place was a crime (or worth reporting);
- not knowing where to report;
- believing that the police cannot do anything; and
- individuals not realising that they are actually a victim (Fafinski and Minassian, 2009).

Whether or not an increase in the proportion of victims reporting negative online incidents will result in a subsequent increase in police recorded crime depends on the nature of the crime reported and whether it meets criteria under the HOCR.

Industry estimates of cyber-dependent crimes

Anti-virus providers generally conclude that security 'attacks' globally are in the billions and levels are increasing. Symantec (2012) reported blocking 5.5 billion 'attacks' globally in 2011, an increase of over 81 per cent from 3 billion reported blocks in 2010. They also reported detecting 403 million unique variations of computer viruses or other malware[7] globally in 2011, compared with 286 million in 2010. Reports from security providers often relate to the global rather than the UK situation, and there are limitations with their estimates. There tends to be a lack of transparency in how estimates are produced and figures are often not comparable between anti-virus providers as they use different units of measurement, with different geographical coverage and customer bases. The British Society of Computing (BSC) has recommended 'caution' with the use of industry figures (House of Commons Science and Technology Committee, 2012).

Reports compiled by anti-virus providers are helpful in understanding the nature of various threats, even if they may not accurately measure the scale of cyber-dependent crime in the UK. For example, industry reports have observed the increase in trojans – a virus that masquerades as a legitimate program, but collects personal data from a user's computer. They have also identified the emergence of fake anti-virus software, which imitates legitimate anti-virus software but is actually a form of malware that can be used to extract users' personal information (Sophos, 2011; Microsoft, 2012; PandaLabs, 2012).

Anti-virus providers state that the level of unsolicited emails (or 'spam') received by users, as a proportion of all email, is falling, although spam is still a common experience amongst internet users. Over half (52%) of adult internet users reported spam as the most common negative experience online (OfCom, 2013). Symantec (2013) reported that spam traffic, as a proportion of all emails, has fallen annually, from 89 per cent of all email in 2010 to 69 per cent in 2012. Some of this decline has been attributed to the closure of 'botnets' responsible for driving large amounts of spam. Botnets refer to clusters of computers infected by malicious software that are subsequently used to automatically and repeatedly send out spam or other malicious email traffic to specified targets.

Security providers generally find that the UK compares well with other countries in terms of exposure and vulnerability to security threats, but lack of clarity and

[7] Malware is malicious software that spreads between computers and causes various forms of computer dysfunction, including deleting files and system crashes. The most well known form of malware is the virus. Some forms of malware may also steal personal data from computers (for example, spyware).

comparability between reports means that clear conclusions cannot be drawn. Sophos (2013), for example, suggested that the UK's 'threat exposure rate' – the proportion of PCs experiencing a malware attack, whether successful or failed, over a three-month period – was almost four per cent. The UK was ranked as the fourth 'safest' country, with Norway ranked first (1.8%). In comparison, the 'riskiest' countries were Indonesia (23.5%), China (21.3 per cent) and Thailand (20.8%). Microsoft (2013) however, placed the UK as tenth in the world ranking of 'most infected nations', with the US at number one (in relation to the total number of computers reporting detections and removals by Microsoft desktop anti-malware products in the second half of 2012).

Police recorded crime and Action Fraud

Police recorded crime does not distinguish between online and offline offences, making it difficult to identify cyber crimes. Police record crime in accordance with the provisions of HOCR, which set out that the crime to be recorded, is determined by the law. Since there is no specific offence (or offences) of cyber crime – aside from those specified in the Computer Misuse Act – police recorded crime does not generally distinguish between offline and online offences. Whether or not the offence was committed online or offline, is cyber-enabled or cyber-dependent, the offence recorded is on the basis of the offence in law. For example a fraud committed using a computer would usually be recorded as a fraud under police recorded crime.

Before the roll out of Action Fraud as the national reporting centre for fraud and financially motivated cyber crime, both computer misuse and fraud offences were recorded by individual police forces. Action Fraud completed roll out in April 2013 and has since taken responsibility for the recording of all fraud and computer misuse offences. Action Fraud captures reports from public and businesses on these crimes and classifies them in a way which allows distinctions to be made between computer misuse, online fraud and offline fraud. Action Fraud also assesses them against the provisions of the law and the requirements of HOCR. Where a report falls short of being recorded as a crime under HOCR, Action Fraud has the facility to record it as an incident, for intelligence and information purposes.

Initial data from the Action Fraud roll-out period show that a total of 7,427 crimes and incidents of computer misuse and extortion were reported to Action Fraud between January and December 2012. These accounted for five per cent of all incidents and crimes reported to Action Fraud during this period. The most common incident reported was illicit distribution of viruses, spyware or other malware (3,949 reports), which accounted for over one-half of computer misuse incidents, followed by reports of individuals hacking into social media and email (1,603 reports) (Action Fraud, 2012). These new data provide an indication of the type of information now available, although the initial data present only a partial picture as they occur in a transitional period of time when Action Fraud had not yet rolled-out to all forces. Action Fraud was initially rolled out to five forces in January 2012, rising to 24 forces by December 2012 and to all forces by April 2013.

Data from the Ministry of Justice reveal far more people have been sentenced under the Fraud Act than under the Computer Misuse Act (CMA) 1990[8]. The CMA 1990 captures four offences centred on technology crime, which make hacking, creation and distribution of malware, and other instances of computer misuse, an offence. Between 2007 and 2012 initial proceedings were taken against 101 people and 88 people were sentenced with a primary offence under the Act. The seemingly low level of sentencing under the CMA reflects the fact that individuals are being proceeded against for cyber offences under other Acts such as the Fraud Act (for example, 45,687 people were sentenced for fraud and forgery offences in the year to end March 2012).

[8] As amended by the Police and Justice Act 2006.

Cyber-enabled crime: fraud and theft

Victimisation surveys indicate that only a small proportion of internet users report being victims of cyber-enabled frauds and mass-marketing scams. This suggests that the public largely ignore unsolicited communications, although victims may not perceive themselves as 'victims' if a loss is refunded by a bank. Just five per cent of internet users reported experiencing financial loss from credit/debit card misuse online in the 12 months prior to March 2012 (Ipsos MORI, 2013). Surveys generally report low levels of response to both online and offline mass marketing scams, with two per cent overall falling victim according to an Office of Fair Trading (OFT) survey (OFT, 2006). Less than one per cent of internet users reported losing money to a romance scam (Whitty and Buchanan, 2012). However, the embarrassment felt by the victim is likely to influence reporting rates in this type of online fraud. In terms of online retail frauds, 16 per cent of UK internet users have reported the non-arrival of purchased goods, goods being counterfeit, or not as advertised (Eurobarometer, 2012).

Industry sources and victimisation surveys suggest that the number of fraudulent emails that attempt to get users to relinquish personal information (so-called 'phishing' emails) are rising in the UK. Financial Fraud Action (2012) reported over 51,000 phishing websites directed against UK banks in 2009, increasing annually to 256,641 reports by 2012.[9] The Oxford Internet Institute found 22 per cent of UK internet users reported an attempt to acquire their banking details in 2011, statistically significantly higher than the 12 per cent reported in 2005, but this has since fallen to 19% in 2013 (Dutton and Blank, 2013).

Only a small proportion of phishing attack victims experience financial losses from phishing attacks. ONS (2010) and Ipsos MORI (2013) both found that around 3 per cent of internet users had experienced financial loss from fraudulent messages or being sent to fake websites asking for information in the 12 months prior to each of the surveys. However, since it is challenging for victims to accurately attribute the source of their financial loss to a phishing email, levels of phishing are likely to be under-reported.

Initial data from Action Fraud show that one-third of all reports received by Action Fraud between January and December 2012 related to cyber-enabled fraud. Online shopping and auctions represent the largest proportion of cyber-enabled frauds during this time. Action Fraud received 47,980 reports of cyber-enabled fraud between January and December 2012, comprising 35 per cent of all crime and incident reports made to Action Fraud during this time. The largest proportion of these was for online shopping and auctions (39%), followed by other advanced fee frauds (11%)[10] and computer software service frauds (nearly 8%). As awareness of the Action Fraud reporting facility grows amongst the public and businesses, reports of computer misuse and fraud offences are expected to increase. Fraud figures published by the ONS (2013b) already show a volume increase of 27 per cent in fraud offences recorded for the year ending March 2013, compared with the previous year. The change to a centralised reporting mechanism through Action Fraud is likely to play a key role in this increase, although there are a number of possible contributing factors which makes comparison over time difficult (ONS, 2013b).

Costs from internet-enabled card-not-present fraud and online banking fraud, as recorded by the banking/payments sector, have been declining. Most published

[9] Although it is not clear how much of this relates to increases in awareness/availability for reporting and how much is due to an actual increase.

[10] Other Advance Fee Fraud refers to advance fee frauds that do not fall under other categories such as 419 frauds. For example: 'Mr A' has advertised his car for sale online. He is emailed by someone saying that they have a buyer for his car. If he pays them £100 he will put them in touch with him. 'Mr A' transfers £100 to an account that was provided but hears nothing further. The person who made contact never had any details of any buyer for the car.

data on cyber-enabled fraud relates to estimates of the cost to the banking/payments industry, rather than prevalence. Costs recorded by Financial Fraud Action (2013) show a decline in internet-enabled card-not-present fraud[11] to the banks/payment card industry, from a peak of £181.7 million in 2008 to £135.1 million in 2010, although reported costs have increased since then to £140.2 million in 2012. The costs recorded from online banking fraud have also been declining – peaking in 2009 at £59.7 million and falling to £35.4 million in 2011, with an increase to £39.6 million in 2012. Such estimates are partial though, representing losses to the banks/payments industry and not to the retail sector or the public. Recent attempts to estimate the loss from cyber crime to the retail sector by the British Retail Consortium (2013) reported overall losses of £205.4 million. The estimate focuses on e-commerce frauds and comprises £77.3 million in direct losses (most notably, identification-related frauds, card and card-not-present frauds, and refund frauds), £16.5 million in online security measures and £111.6 million in lost revenue from online fraud prevention. However, it is difficult to estimate such losses accurately. Many of the survey-based estimates of loss that have been undertaken are likely to represent just a fraction of the individuals/organisations surveyed and may be skewed upwards by extreme losses reported by a few respondents.

'Insider-threats' are a prominent issue reported in business surveys. However, the limited evidence available is mixed on whether they are a bigger problem than outsider attacks. Insider threats may be malicious or targeted activity, but may also be accidental or negligent. The majority (86%) of recent online crime incidents reported by businesses in the CVS (Home Office, 2013b) were thought to be external attacks from outside the organisation, with just 2 per cent thought to be internal (for the remaining 12% of cases, respondents did not know if they were internal or external). However, it is not possible to verify the accuracy of these reports. Another survey of 1,007 businesses in 2008 reported that over half of the most serious incidents (57%) were believed to have an internal cause, whereas 38 per cent had an external cause (BERR, 2008). However, this difference may simply reflect the different scope of the two surveys, making direct comparisons problematic.

Despite concerns over personal details and online security, consumer online confidence appears to be growing and users continue to shop and transact online. The OFT found that the proportion of online shoppers with no concerns doubled from 12 per cent in 2006 to 28 per cent in 2009. An increased proportion also felt that online shopping was as safe as shopping in store, rising from 26 per cent in 2006 to 54 per cent in 2009 (OFT, 2009).

Cyber-enabled crime: sexual offending against children

Few studies distinguish between online and offline forms of sexual offending against children. The Child Exploitation and Online Protection Centre (CEOP) found ten per cent of the 3,652 reports they received during 2009/10,[12] related to online grooming and 16 per cent related to online distribution of images. A further 15 per cent of reports related to possession of indecent images, although it is not clear if all of these were online offences. The remaining reports included contact abuse (both online and offline, 14%), offline grooming (32%) and offline distribution of indecent imagery (12%) (Child Exploitation and Online Protection Centre, 2010).

[11] Internet-enabled card-not-present fraud relates to transactions conducted remotely where neither cardholder nor card are present, specifically where transactions are conducted over the internet.

[12] These are reports that related to sexual offending against children only. In total 6,291 reports were made to CEOP during this time period, which also included other types of incidents. Reports were made by the public and other stakeholders (for example, charities)

Surveys of young people suggest that meeting new people online is a common occurrence and very few offline meetings appear to lead to harm. In an EU study of over 25,000 children aged 9 to16 years (Livingstone *et al*., 2011) 1 per cent of children reported expressing some concern about what happened at an offline meeting that followed online contact. Overall, less than 0.1 per cent reported some form of sexual contact (approximately 28 children). Whilst serious in nature, the numbers of police recorded grooming offences are low compared with other types of serious sexual offending. There were 371 grooming offences recorded in 2011/12 compared with 4,991 offences of rape of a female child under the age of 16. However, for grooming to be a recorded offence in accordance with the HOCR, there must also be an offline meeting. In a case where there was only an online meeting, this would not be recorded as 'grooming' and is likely to be recorded under another sexual offence category. Crime recording rules also set out that it is the most serious offence recoded by police, which may result in grooming cases being recorded under other serious sexual offence categories, such as rape of a child.

Twelve per cent of UK children surveyed aged 11 to 16 years reported receiving or seeing sexual messages online in the previous 12 months (Livingstone *et al.,* 2010; 2011). However, by no means would all of these types of messages constitute an offence and the study does not specify if they were received from adults or peers.

Under-reporting of online grooming is likely. The similarities between the online grooming process and the initial process of building online relationships can mean that some victimisation is going unnoticed. Some victims may perceive offenders as friends or romantic partners, rather than as abusers or offenders (Wolak *et al*., 2004), which may contribute to under-reporting. Offenders may also create fake online personas to portray themselves as a similarly aged peer, often of the opposite sex. They can use these personas to trick victims into sending self-generated indecent imagery (CEOP, 2013b). Offenders may coerce children not to report and some children may be too embarrassed to report or unsure who to tell. On the other hand, some children may be able to deal with unwanted advances online. In an EU survey of 11- to 16-year-olds, only 7 per cent of those who had received or seen messages that upset them said that they had done nothing to tackle it. Others undertook activities such as blocking the sender or changing filter settings (Livingstone *et al.*, 2011), although these messages did not all necessarily relate to sexual messages.

More than one-fifth (22%) of the 2,293 industry reports submitted to CEOP in 2011/12 related to self-generated indecent imagery (SGII), involving practices such as 'sexting'. The emergence of 'sexting' – the self-generation and exchange of indecent user imagery – indicates a shift in the nature of online risks. In 2012, CEOP suggested that SGII represents one of the biggest risks to young people (CEOP, 2012b) and survey data concur (for example, Phippen, 2009).

The Crown Prosecution Service (CPS) recorded over 14,000 charges[13] of making an indecent photograph of a child in 2012/13 (Protection of Children Act 1978) and over 3,800 of possession of an indecent photograph of a child (Criminal Justice Act 1988). Estimating levels of indecent imagery of children online is challenging, yet whilst it is not clear whether all these prosecutions relate to electronic or online images, it is likely that a substantial proportion do. The Internet Watch Foundation (IWF) reported that almost 13,000 URLs in 2010/11 contained child sexual abuse content, this declined to just under 10,000 in 2012 (Internet Watch Foundation, 2011; 2012). Most of these appeared to originate from outside the UK. There were 214 UK-hosted URLs.

Some online sexual offending may never progress into the 'offline' world. Offenders do not appear to be a homogeneous group and there is little consensus

[13] CPS data relate to total charges and not offenders – one offender may have multiple charges. CPS data are also not official statistics and are provisional data based on management information held centrally.

regarding the links between online and offline forms of sexual offending (Bryce, 2010; CEOP, 2012a; Whittle *et al.*, 2012). Sex offenders who access, share and create indecent images of children, along with those who groom children online, have been subject to more research than other cyber offenders, however most evidence relates to small samples of imprisoned offenders in the US. CEOP's 2013 threat assessment also outlines a new predominant trend of online-only child sexual exploitation, rather than offenders grooming victims with the intent to meet offline (Child Exploitation and Online Protection Centre, 2013).

Although some offenders who share and create indecent images use highly sophisticated, technical methods to conceal themselves online, these behaviours are by no means universal*.* CEOP (2012b) estimated that almost one-half of 'hidden' internet use, for example, through hidden forms of communication such as The Onion Router (ToR)[14] are involved in the proliferation of indecent imagery of children. Other research has also found evidence of technical methods being used, such as multiple identities incorporating several IP addresses, proxy servers to give the appearance of being in another country, and illicit images being accessed through 'disguised' websites (Internet Watch Foundation, 2011; Webster *et al.*, 2012;). However, other studies of convicted offenders suggest that these measures are by no means universal and many offenders who create, store and share indecent imagery take few security measures (Carr, 2004).

Online harassment – online stalking and hate crime

Less than one per cent of respondents aged 16-59 years reported experiencing one or more forms of online or 'cyberstalking' in the last year (CSEW, 2011/12). In this case, cyberstalking was defined as:

- having received unwanted emails that were threatening or obscene; or
- respondents having personal, obscene or threatening information posted about them on the internet.

To set this in context, 3.5 per cent had experienced *any* form of stalking in the last year (see ONS, 2012). Both men and women reported experiencing cyberstalking in the last year, although women experienced a higher proportion of incidents (0.9%), than men (0.5%). This was similar to the findings for all forms of stalking (where 4.2% of women and 2.7% of men were victims on one or more occasion in the last year).

Overall, there is limited evidence available regarding the nature and extent of online stalking in the UK. In terms of other evidence, one of the few UK-specific cyberstalking studies available involved a pilot online survey of 353 people reporting to the Network for Surviving Stalking website. Online tools played a role in around 70 per cent of these reported incidents (Maple *et al*., 2011).

Evidence relating to online hate crime is even sparser than information regarding online stalking. Attempts have been made to calculate numbers of online hate websites, for example, the Internet Watch Foundation (2010) reported 982 websites hosted by the UK inciting racial hatred in 2010. However, these figures cannot be regarded as a true reflection of the prevalence of these forms of website.

The Home Office response to the 2012 consultation on stalking (Home Office, 2012b) and the Home Office '*Challenge it, Report it, Stop it'* plan to tackle hate crime (Home Office, 2012c) both state that further consideration of these online crime types is required.

[14] The ToR helps anonymise online interactions by directing internet traffic through a worldwide network of servers to conceal a user's original location.

Other aspects of cyber crime

Cyber offenders

There are a range of motivations behind cyber crimes. They focus largely around financial gain (for example, the use of malware or phishing emails to gain access to bank account details) or can be a form of protest and/or criminal damage (for example, hacking and website defacement). For child exploitation, the motive is clearly not always for profit. More unorthodox motivations for cyber crimes include intellectual curiosity/challenge; general maliciousness; revenge; gaining power/respect in online communities; or even simply boredom (Kirwan and Power, 2012).

In-depth technical skills are not necessarily required for offenders to commit cyber-dependent and cyber-enabled crimes. The emergence of sophisticated and automated 'do-it-yourself' malware kits and hacking tools, available for purchase on online forums, means that opportunities for complex forms of offending have been opened up to a much wider range of lower-skilled individuals (Holt, 2013a). A small, but elite group of cyber offenders are thought to be responsible for creating these sophisticated tools, which can subsequently be used by a wide pool of semi- and unskilled offenders (Holt and Kilger, 2012).

Cyber crimes are not, however, just about technical skills and rely heavily on the behaviour of the intended victim. Social engineering tactics are key to deceiving computer-users about the purpose of a file or an email they have been sent (Furnell, 2010; Kirwan and Power, 2012). Phishing emails, for example, can be carefully designed to look like they are from a bank or other organisations in order to deceive individuals into parting with personal information or money. Computer-users may also unknowingly download viruses in attachments if they are led to believe the email is from someone else.

Most published evidence regarding cyber offenders is drawn from handfuls of case-studies or interviews and tends to focus on offender motivations and methods. There is little comprehensive published evidence regarding other key information, such as offender characteristics, career pathways and the links between online and offline offending.

Organised cyber crime

Case-study evidence has identified that some traditional hierarchical organised crime groups have recognised the value of new technologies in facilitating the commission of crimes, for example, through extortion, money laundering, scams, credit card forgery and other online frauds (Choo and Smith, 2008). Whilst these types of groups may not be working online themselves, evidence suggests that they may be prepared to pay for the information that cyber criminals have available, in order to carry out crimes in the physical, rather than the virtual world (McCusker, 2006).

However, many 'organised' cyber criminals do not operate in this traditional way. They work as looser online networks of organised cyber criminals as part of global online marketplaces where they can buy and sell the technical tools or services used for, or products derived from, cyber crime attacks (Holt, 2013b). These groups are working within an organised structure, but unlike traditional organised crime groups the individuals in these online forums are not bound by the same hierarchy and governance, and tend to work together as loose affiliations for shorter, finite periods of time rather than on a continuing basis (Lusthaus, 2013). Researchers in the US (for example, Holt, 2013a) have explored the organisation of these types of cyber criminals through their interactions in online forums, with a view to informing disruption activities.

At present, there are no reliable estimates of the precise scale or cost of organised cyber crime.

Costs of cyber crime

Estimating the costs of cyber crime is challenging and there are limitations with previous research that has attempted to produce estimates. As outlined by the Home Affairs Select Committee report on e-crime (Home Affairs Select Committee, 2013), the precision of Detica's (2011) £27 billion estimate has been questioned due to the lack of robust and transparent data upon which their estimates were based. Progress in this complex area has been made with work conducted by Anderson *et al.* (2012) who estimated separate costs for different cyber crimes, opting not to produce one total estimate given the paucity and reliability of the data available. However, there are also limitations with Anderson *et al.*'s approach, which relies partly on scaled down global estimates and case-studies, based on the UK being five per cent of the world gross domestic product (GDP). The UK cyber security strategy (Cabinet Office, 2011) recognised the challenges in this area and noted *"a truly robust estimate will probably never be established, but it is clear the costs are high and rising"*. Based on the limited research available at present, for example, drawing upon Anderson *et al.* (2012), the costs of cyber crime could reasonably be assessed to equate to at least several billion pounds per year.

Improving the cyber crime evidence base

Cyber crime is a complex issue. Some of the main challenges to improving understanding of cyber crime include:

- lack of recording mechanisms that accurately distinguish between online and offline crime;
- under-reporting of cyber crime from the public and businesses and a lack of awareness that some cyber incidents are actually crimes (although not all are);
- inconsistencies in the measurement and definition of cyber crime within the relevant research;
- information from industry sources often lacks transparency and comparability;
- few methodologically sound surveys of victims exist;
- cyber crime can be undertaken on a large scale, potentially resulting in a relationship between victims and offenders that is very different to 'offline' crime; and
- cyber crime is global in nature, it is not constrained by national boundaries.

Measuring cyber crime

Improving measurement and recording is critical to understanding whether the scale of cyber crime is increasing or decreasing and how the nature of the problem is evolving over time. Without a better understanding of these things, it is harder to allocate the right resources to different issues and to recognise what is working and what is not.

The introduction of Action Fraud reporting is one key element to improving understanding of the scale and nature of cyber crime, but other improvements are also needed, including the following.

- *Systematically improving the quality and range of individual measures of cyber crime.* Following the establishment of Action Fraud cyber crimes are more

systematically identified and recorded. In order to capture more information on the types of cyber crimes not covered by Action Fraud, the Home Office:

- has introduced a voluntary cyber 'flag' onto police recorded crime;
- has been encouraging new questions to be added to the CVS and the CSEW; and
- will continue to review the effectiveness of these improvements.

Markedly improving and expanding the data on the prevalence of different types of cyber crime will be a prerequisite to developing more informed estimates of cost, and so this is where the Home Office has been placing most of its recent efforts.

- *A new external working group will be set up by the Home Office, focusing on improving the estimates of the cost of cyber crime*. The group will seek to agree on the best available data for formulating any estimates, develop an agreed model for assessing costs and look to improve these estimates over time. Given that cyber crime relates to multidisciplinary, yet complementary areas (for example, cyber security, criminology, law, psychology and economics), the group is likely to benefit from bringing together and drawing upon such multidisciplinary expertise. The group may also wish to consider further engagement and partnership with private sector businesses and industry partners (including anti-virus companies) in order to help to explore the potential use of other data sources

References

Action Fraud (2012) Unpublished data. London: National Fraud Authority.

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M. J. and Levi, M. (2012) *Measuring the cost of cybercrime*. Retrieved September 2013. Available as: <http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf>.

BERR (2008) *Information Security Breaches Survey.* London: Department for Business, Innovation and Skills. Retrieved from BIS, September 2013. Available at: <http://www.bis.gov.uk/files/file45714.pdf>.

British Retail Consortium (2013) *BRC Retail Crime Survey 2012.* BRC.

Bryce, J. (2010) 'Online sexual exploitation of children and young people'. In *Handbook of Internet Crime,* Jewkes, Y. and Yar, M., pp 320–342. Culhompton: Willan Publishing.

Cabinet Office (2011) *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* London: Cabinet Office.

Carr, A. (2004) *Internet traders of child pornography and other censorship offenders in New Zealand.* Retrieved from the Department of Internal Affairs, September 2013. Available at: <http://www.dia.govt.nz/Pubforms.nsf/URL/entirereport.pdf/$file/entirereport.pdf>.

Child Expoitation and Online Protection Centre (2010) *Strategic Overview 2009–2010.* London: CEOP.

Child Exploitation and Online Protection Centre (2012a) *A Picture of Abuse.* London: CEOP.

Child Expolitation and Online Protection Centre (2012b) *Threat Assessment of Child Sexual Expoitation and Abuse 2012.* London: CEOP.

Child Exploitation and Online Protection Centre (2013a) *Threat Assessment of Child Sexual Exploitation and Abuse.* Retrieved September 2013. Available at: <http://ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf>.

Child Exploitation and Online Protection Centre (2013b) *Children treated like 'slaves' to perform sexual acts*. Retrieved September 2013. Available at: <http://ceop.police.uk/Media-Centre/Press-releases/2013/Children-treated-like-slaves-to-perform-sexual-acts-/>.

Choo, K.-K. R. and Smith, R. G. (2008) 'Criminal Exploitation of Online Systems by Organised Crime Groups', *Asian Criminology*, 11, pp 37–59.

Computer Misuse Act 1990.

Criminal Justice Act 1988.

Detica (2011) *The Cost of Cybercrime.* London: Cabinet Office. Retrieved September 2013. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf>

Dutton, W. H. and Blank, G. (2013). *Cultures of the Internet: The Internet in Britain.* Oxford: Oxford Internet Institute, University of Oxford. Retrieved September 2013. Available at: <http://oxis.oii.ox.ac.uk/sites/oxis.oii.ox.ac.uk/files/content/files/publications/OxIS_2013.pdf>.

Eurobarometer (2012) *Cyber Security: UK.* European Commission.

Fafinski, S. and Minassian, N. (2009) *UK Cybercrime Report.* Retrieved September 2013. Available at: <http://www.garlik.com/file/cybercrime_report_attachement>.

Financial Fraud Action (2012) *Fraud the Facts.* Retrieved from UK Cards Association, September 2013. Available at: <http://www.theukcardsassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf>.

Financial Fraud Action (2013) *Fraud the Facts 2013.* Retrieved September 2013. Available at: <http://www.financialfraudaction.org.uk/publications/files/assets/basic-html/page1.html>.

Furnell, S. (2010) 'Hackers, Viruses and Malicious Software'. In *Handbook of Internet Crime,* Jewkes, Y. and Yar, M., pp 173–193. Culhompton: Willan Publishing.

HMSO (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* London: HMSO.

Holt, T. J. (2013a) 'Exploring the social organization and structure of stolen data markets', *Global Crime, 14*, pp 155-174.

Holt, T. J. (2013b) 'Examining the forces shaping cybercrime markets online', *Social Science Computer Review*, 31, pp 165-177.

Holt, T. J. and Kilger, M. (2012) 'Examining Willingness to Attack Critical Infrastructure Online and Offline', *Crime & Delinquency*, 58 (5), pp 798–822.

Home Affairs Select Committee (2013) *House of Commons Home Affairs Select Committee Report on E-crime.* Retrieved August 2013. Available at: <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf>.

Home Office (2011b) *The National Crime Recording Standard (NCRS): What you need to know.* London: Home Office. Retrieved August 2013. Available at: <https://www.gov.uk/government/publications/the-national-crime-recording-standard-ncrs-what-you-need-to-know>.

Home Office (2012a) *Counting Rules for Recorded Crime*. London: Home Office. Retrieved September 2013. Available at: <http://homeoffice.gov.uk/science-research/research-statistics/crime/counting-rules/>.

Home Office (2012b) *Review of the Protection from Harassment Act 1997: Improving protection for victims of stalking – Summary of consultation reponses and conclusions.* London: Home Office. Retrieved September 2013. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/157899/stalking-responses.pdf >.

Home Office (2012c) *Challenge it, Report it, Stop it: The Government's Plan to Tackle Hate Crime.* London: Home Office. Retrieved September 2013. Available at: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97849/action-plan.pdf>.

Home Office (2013a) *Crime against businesses: Headline findings from the 2012 Commercial Victimisation Survey.* Retrieved September 2013. Available at: <http://www.homeoffice.gov.uk/publications/science-research-statistics/research-statistics/crime-research/crime-business-prem-2012/crime-business-prem-2012-pdf?view=Binary >.

Home Office (2013b) *Commercial Victimisation Survey* [computer file]. UK: ONS. Retrieved September 2013. Available at: <https://www.gov.uk/government/publications/crime-against-businesses-detailed-findings-from-the-2012-commercial-victimisation-survey>.

House of Commons Science and Technology Committee (2012) *Malware and Cybercrime.* London: The Stationery Office Ltd.

Internet Watch Foundation (2010) *Annual Report.* Retrieved from IWF, September 2013. Available at: <http://www.iwf.org.uk/accountability/annual-reports/2010-annual-report>.

Internet Watch Foundation (2011) *Annual Report.* Retrieved from IWF, September 2013. Available at: <http://www.iwf.org.uk/accountability/annual-reports/2011-annual-report>.

Internet Watch Foundation (2012) *Annual Report*. Retrieved from IWF, September 2013. Available at: <https://www.iwf.org.uk/assets/media/annual-reports/FINAL%20web-friendly%20IWF%202012%20Annual%20and%20Charity%20Report.pdf>.

Ipsos MORI (2013) *A survey of public attitudes to internet security.* Home Office Research Report 75 (Annex B). London: Home Office.

Kirwan, G. and Power, A. (2012) *The Psychology of Cyber Crime.* Hershey: IGI Global.

Livingstone, S., Haddon, L., Gorzig, A. and Olafsson, K. (2010) *Risks and safety for children on the internet: the UK report.* London: LSE, EU Kids Online.

Livingstone, S., Haddon, L., Gorzig, A. and Olafsson, K. (2011) *Risks and safety on the internet: The perspective of European Children. Full Findings.* London: LSE, EU Kids Online.

Lusthaus, J. (2013) 'How organised is organised cybercrime?' *Global Crime*, 14 (1) pp 52–60.

Maple, C., Short, E. and Brown, A. (2011) *Cyberstalking in the United Kingdom: An Analysis of the ECHO Pilot Survey.* University of Bedfordshire.

McCusker, R. (2006) 'Transnational organised cyber crime: distinguishing threat from reality', *Crime, Law and Social Change*, 46 (4-5), pp 257–273.

Microsoft (2012) *Microsoft Security Intelligence Report,* vol. 13*.* Retrieved September 2013. Available at: <http://www.microsoft.com/security/sir/default.aspx>.

Microsoft (2013) *Microsoft Security Intelligence Report,* vol. 14, second half 2012. Retrieved September 2013. Available at: <http://www.microsoft.com/security/sir/default.aspx>.

Ministry of Justice (2011) Unpublished data. London: Ministry of Justice.

Ofcom (2012) *Communications Market Report.* London: Ofcom. Retrieved from Ofcom, September 2013. Available at: <http://stakeholders.ofcom.org.uk/binaries/research/cmr/cmr12/CMR_UK_2012.pdf>.

Ofcom (2013) *Adults media use and attitudes report.* London: Ofcom. Retrieved September 2013. Available at: <http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/adult-media-lit-13/2013_Adult_ML_Tracker.pdf>.

OFT (2006) *Research on impact of mass marketed scams: A summary of research into the impact of scams on UK consumers.* London: Office of Fair Trading.

OFT (2009) *Findings from consumer surveys on internet shopping: A comparison of pre- and post-study consumer research.* London: Office of Fair Trading. Retrieved September 2013. Available at: <http://www.oft.gov.uk/shared_oft/reports/Evaluating-OFTs-work/oft1079.pdf>.

ONS (2006) *Crime Survey for England and Wales* (formerly known as the British Crime Survey, 2005-2006 [computer file]). Data set available at UK Data Service [distributor]. Retrieved September 2013. Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=5543&type=Data%20catalogue>.

ONS (2007) *Crime Survey for England and Wales* (formerly known as the British Crime Survey, 2006-2007 [computer file]). Data set available at UK Data Service [distributor]. Retrieved September 2013. Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=5755&type=Data%20catalogue#variables>.

ONS (2010) *Internet Access 2010: Households and individuals.* UK: Office for National Statistics. Retrieved September 2013. Available at: <http://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=2&ved=0CDgQFjAB&url=http%3A%2F%2Fwww.ons.gov.uk%2Fons%2Frel%2Frdit2%2Finternet-access---households-and-individuals%2F2010%2Fstb-internet-access---households-and-individuals--2010.pdf&ei=>.

ONS (2011) *Crime Survey for England and Wales* (formerly known as the British Crime Survey, 2010-2011 [computer file]). Data set available at UK Data Service [distributor]. Retrieved September 2013. Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=6937&type=Data%20catalogue>.

ONS (2012a) *Internet Access 2012: Households and individuals.* UK: Office for National Statistics. Retrieved September 2013. Available at: <http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/2012/stb-internet-access--households-and-individuals--2012.html>.

ONS (2012b) *Crime Survey for England and Wales, 2011/12* [computer file]. UK: ONS. Retrieved September 2013. Available at: <http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/focus-on-property-crime--2011-12/index.html>.

ONS (2013a) *Retail Sales, July 2013.* UK: ONS. Retrieved September 2013. Available at: <http://www.ons.gov.uk/ons/dcp171778_323522.pdf>.

ONS (2013b) *Crime in England and Wales, Year ending March 2013.* UK: ONS. Retrieved September 2013. Available at: < http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/period-ending-march-2013/stb-crime--period-ending-march-2013.html>.

PandaLabs (2012) *Annual Report (Summary).* PandaLabs.

Phippen, A. (2009) *Sharing personal images and videos among young people.* Retrieved from Blackpoollscb July 2013. Available at: <http://blackpoollscb.org.uk/contents/documents/sexting-detail.pdf>.

Protection of Children Act 1978.

Sophos (2011) *Stopping Fake Anti-Virus*. Retrieved from Sophos, September 2013. Available at: <http://www.sophos.com/en-us/security-news-trends/security-trends/fake-antivirus.aspx>.

Sophos (2013) *Security Threat Report 2013.* Retrieved from Symantec, September 2013. Available at: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf>.

Symantec (2012) *Internet Security Threat Report 2011 Trends.* Mountain View, CA: Symantec Corporation.

Symantec (2013) *Internet Security Threat Report 2013.* Mountain View, CA: Symantec Corporation.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V. and Pham, T. (2012) *European Online Grooming Report.* European Commission, Safer Internet Plus Programme.

Whittle, H., Hamilton-Giachritsis, C., Beech, A. and Collins, G. (2012) 'A review of online grooming: characterstics and concerns', *Journal of Aggression and Violent Behaviour*, 18 (1), pp 62–70.

Whitty, M. and Buchanan, T. (2012) 'The online romance scam: A serious cybercrime', *CyberPsychology, Behavior, and Social Networking*, 15 (3), pp 181–183.

Wolak, J., Finkelhor, D. and Mitchell, K. (2004) Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health*, 35 (5), pp 424.e11–424.e20.

Annex A: Methodology

As an evidence-based review, the authors sought to:

- conduct a rigorous and transparent search of the available research evidence;
- assess critically the quality of the evidence; and
- select the most relevant and robust evidence available for inclusion in the review.

The purpose was not to conduct a full 'systematic' review. Given the unknown nature and quality of evidence available, along with the breadth of the subject, a scoping approach was more appropriate. However, aspects of the systematic review method, for example, systematic search techniques, have been incorporated to add transparency and rigour. Gathering evidence posed particular challenges since it is widely dispersed across many source types, including industry reports, academic papers and government papers; evidence also stems from a wide range of disciplines (for example, cyber security/IT; law; criminology; psychology).

Inclusion/exclusion criteria for the review

Evidence was included for review where it:

- related to the UK;
- related to one of the key cyber themes identified – cyber-dependent crimes and cyber-enabled crimes: fraud and theft, and sexual offending (online stalking and hate crime were also included, but limited evidence was found in these areas, and cyberterrorism was outside the scope of this work);
- was dated 2000 to present; and
- was published evidence, drawn from academic, industry, government, law enforcement, non-governmental organisations or other relevant sources.

Both quantitative and qualitative evidence were considered for inclusion. In some instances unpublished data, for example, from the Ministry of Justice, the Crown Prosecution Service and Action Fraud, were directly requested to assist with the review.

In a small number of cases supplementary evidence from the US was also included (for example, research regarding online forums) where it could assist with evidencing particular topic areas. Please note that a rigorous review of international literature was not conducted as part of this research.

The aim within each area was to draw together best available evidence on:

- the scale, cost and nature of the problem;
- characteristics of victims and offenders.

Each section was structured to reflect these criteria. Gaps in knowledge and methodological limitations were identified throughout the process.

Search terms and techniques

Three types of searches were conducted:

- *High-level general searches* – these were aimed at quickly gathering material around key themes.

- *Directed searches within key sources* – these involved in-depth searches in major databases such as the BLPES, IngentaConnect, JSTOR, IEEE explore, Swetswise and Google Scholar. They largely helped with identifying key academic papers from a variety of disciplines (for example, cyber security, criminology, psychology, law). Searches were also made of key industry sources

and anti-virus providers (for example, Microsoft, Symantec, Sophos). Wherever possible, available literature of this kind was supplemented by up to date Government data and papers (for example, the Crime Survey for England and Wales).

- *'Snowball' search methods* – these types of searches were more unstructured and involved following 'leads' within evidence to identify other potential source documents and following up recommended literature from academic and other contacts working in the cyber area.

The *search terms* used reflected the broad range of areas under review and the extensive range of terminology used to describe cyber crimes. For example, higher-level searches were made using terms such as 'cyber crime'; 'online crime'; 'e-crime'; 'cyber-dependent crime'; 'cyber-enabled crime', 'computer-dependent crime'; 'computer-enabled crime'. More specific terms were also built into the searches, for example, 'hacking'; 'phishing', 'malware', 'identity theft'; and 'mass-marketing scams'. These were tailored specifically for each topic area.

Assessing quality of the evidence

A large volume of robust evidence was not anticipated in this field, so no piece of evidence was immediately excluded. Each piece of evidence was rated according to key variables: relevance, source reliability and methodology. Each was given a high/medium/low rating.

In summary, the evidence found held a number of limitations. For example:

- it did not distinguish between online and offline crimes;
- some surveys were based on small, non-random and unrepresentative samples, meaning that findings could not be inferred to the wider population;
- ambiguities and inconsistencies in measurement, definitions and methodology used;
- lack of transparency in methodologies (particularly amongst industry reports), which provided challenges assessing the quality of the evidence; and
- in some cases, a complete lack of UK-based evidence.

Ultimately the published review reports on evidence regarded as high/medium in terms of its quality and relevance. However, in some cases lower quality evidence is drawn upon where there is a lack of other evidence available.

Quality assurance

Throughout the review, academic, policy and law enforcement contacts were consulted to check particular aspects of the evidence to help with interpretation and to ensure that no obvious data sources had been missed. A full peer review of the paper was also conducted by experts in different areas.

Annex B

A survey of public attitudes to internet security

Summary of key findings

Published October 2013

Ipsos MORI

Contents

	Page
Introduction	24
Internet users' online behaviours	24
Negative online experiences and reporting	27
Additional security measures	28

Disclaimer

The views expressed in this report are those of the authors, not necessarily those of the Home Office (nor do they represent Government policy).

A survey of public attitudes to internet security

Ipsos MORI

1. Introduction

In 2012, the Home Office commissioned Ipsos MORI to conduct a survey on public attitudes and behaviours regarding internet security. The survey aimed to help understand awareness of cyber security amongst the public, the behaviours people undertake to protect themselves online and their willingness to undertake additional security measures. Ipsos MORI interviewed a representative sample of 2,015 members of the general public (aged 15 and over) in Great Britain between 16 and 22 March 2012[15]. Of these, 80 per cent per cent (1,518) were classed as 'internet users' (defined as having used the internet in the last 12 months, i.e. March 2011-2012). Eighty per cent of internet users were frequent users (using the internet everyday, or almost every day) and 96 per cent used the internet at least once a week.

Key findings from this survey are presented here, focusing on:

1) internet users' online behaviours;
2) negative online experiences; and
3) internet users' willingness to undertake additional security measures.

Key findings

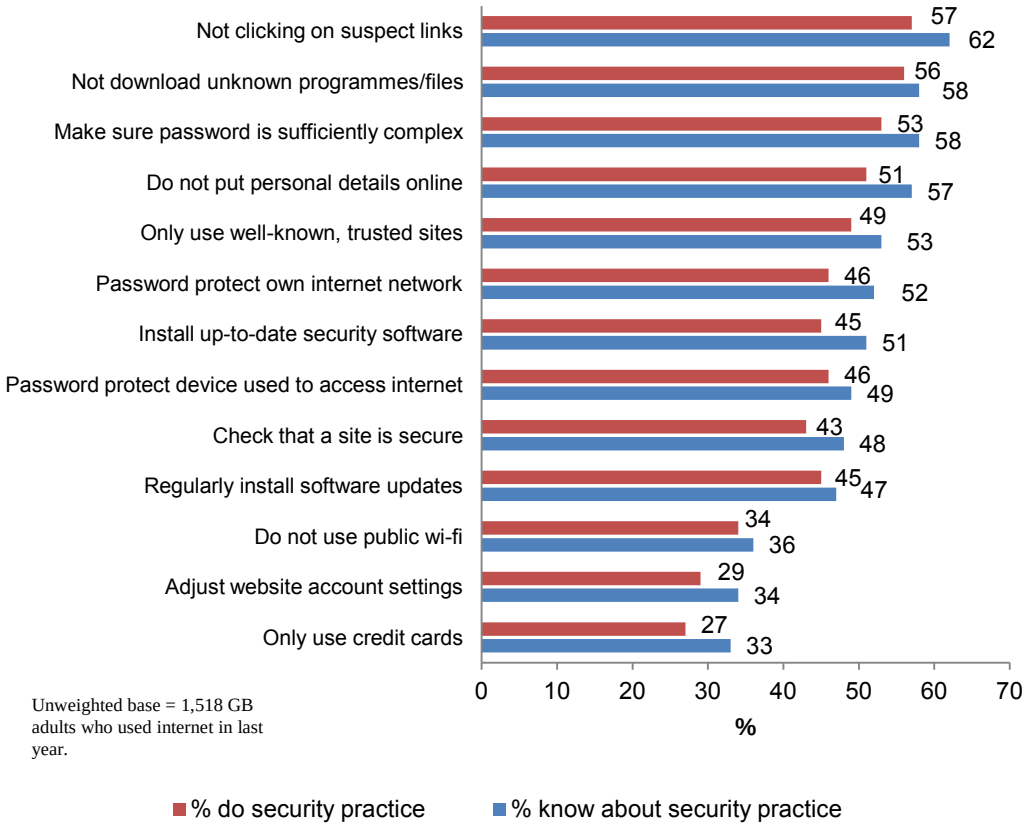
2. Internet users' online behaviours

Internet security software is commonly used, but other 'good practices' are less well adopted.

- Four fifths (78%) of internet users always used security software when connecting to the internet.
- One in ten never used security software (11%) and a further one in ten did not use it on all devices (9%).
- Those who used the internet more often were more likely to use security software on all devices (82% of those who used it every day/almost every day, compared with 63% of less frequent users).
- Wider internet security good practices were less well used – even amongst those who were frequent users. For example, just 43 per cent of internet users said they would check a site was secure and 34 per cent said they did not use public Wi-Fi. Figure 1 outlines the awareness and use of various security practices reported by internet users.

[15] Ipsos MORI used a controlled form of random location sampling, known as the 'random locale' approach, which combines aspects of random probability and quota sampling approaches.

Figure 1. Internet users who are know about and do various security practices



Younger users, those in Black and Minority Ethnic (BME) groups or less affluent social groups and mobile phone users appear less likely to take up security features.

- Users aged 15-24 years, were less likely to use internet security software on all devices (70%) compared to users aged 65 and over (92%). Whilst those aged 65 and over were less likely to have accessed the internet at all in the last year compared to younger users (for example, 44% of those aged 65 and over, compared to 93% of 15-24 year olds), they were still more likely to add security software to their devices when they do access the internet.
- BME users were less likely to use security software on all their devices (55%) compared to users who defined themselves as white (81%).
- Less affluent users were less likely to use internet security on all their devices compared with more affluent users. For example, 65 per cent of those in social grade DE[16] had internet security on all their devices, compared to 89 per cent in the AB[17] social grade.
- These patterns were also observed in relation to other security practices. For example:
    - younger users were less aware of ISP security features than those in other age groups (37% of users aged 15-34 years, compared to 47-57% among those aged 35-65 years);
    - less affluent users (DE grade) were less likely to state they did not click on suspect links (41%) compared to more affluent users (AB grade) (71%); and

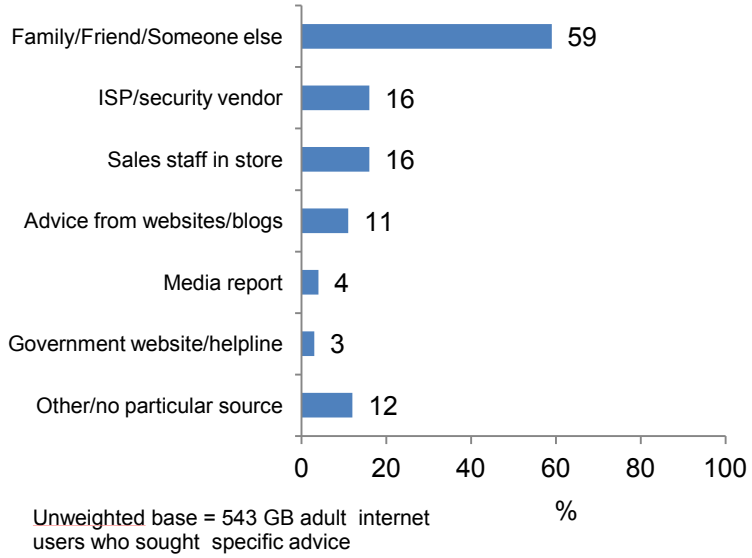
[16] DE includes semi and unskilled manual workers; as well as state pensioners, casual or lowest grade workers, unemployed with state benefits only.
[17] AB refers to high and intermediate managerial, administrative or professional workers.

    - BME users were less likely to state they did not click on suspect links (39%) compared to users defining as white (59%).
- The way in which users connect to the internet also makes a difference, with those who mainly connect through a mobile phone less likely to say that they have security software on all their devices than those whose main connection is through a personal home computer, personal computer at work, laptop, or other mode of connection (57% of phone users compared to 79% and 83% across other modes).

Many users do not seek security advice, but friends and family are key sources of information for those that do

- Less than one-half (43%) of internet security software users sought advice about different products. Figure 2 outlines the various sources of advice used amongst those who did seek advice. Where advice was sought, 59 per cent (n=543) went to family, friends or someone else. Others went to their ISP (16%) or to sales staff in a store (16%). Three per cent went to Government websites (e.g. www.gov.uk).

Figure 2. Sources of advice for internet users who sought advice on internet security software



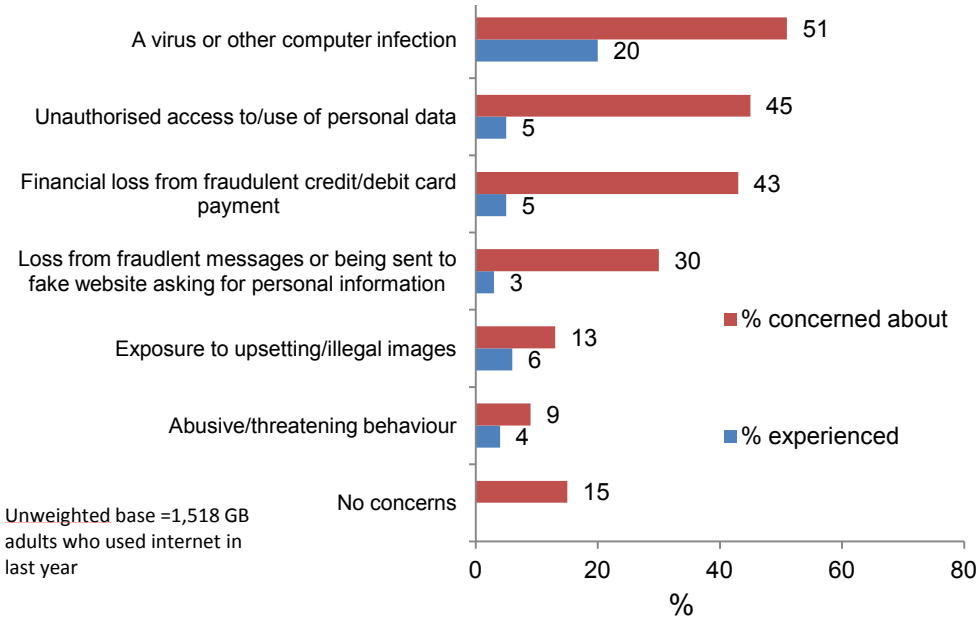
- Most of those who did not seek advice (n=545) either thought that it was not necessary (33%) or they knew enough already (31%); while a smaller proportion stated they had no interest in it (9%). Around one in ten did not know where to look (7%), whilst a small minority felt that it was the responsibility of their internet provider or security companies (4%).
- For those who undertook various internet 'good practices', the largest proportion (39%) said they did so because friends, family or someone else advised them to. Just 11 per cent did so because of government advertising/advice.
- Just over two in five of those who use security software bought it separately from a specialist company such as Norton or McAfee (43%). A quarter use free third party software (26%), one in five use software provided with their computer or device (19%), and one in seven have been provided it as part of their current internet package (14%).

3. Negative online experiences and reporting

Around one-third (36%) of internet users experienced one or more negative online incidents in the 12 months prior to the survey. Viruses were the most common experience, and were most frequently cited as a concern.

- The largest proportion of internet users (20%) had experienced a virus or other computer infection in the 12 months prior to the survey. Smaller proportions of internet users had experienced financial loss from fraudulent credit/debit card payments (5%) and unauthorised access to personal information (5%). Higher proportions of internet users were concerned about experiencing various online incidents than had actually experienced them (see Figure 3).
- There were no differences in experiences of viruses or other security breaches in relation to demographic groups or internet user types. Although other surveys such as the CSEW, have found differences between demographic groups and their negative experiences. Fifty-two per cent of individuals who connected to the internet through public Wi-Fi (n=1,458) experienced one or more security issues. In comparison, only 35 per cent of those who connected through a home network experienced these consequences. However, this analysis is based on very small sample of Wi-Fi users and we cannot be sure that the use of public Wi-Fi was directly related to the security breaches referred to in the survey.
- As with other surveys of negative online experiences, these incidents do not necessarily relate to criminal activity and many are unlikely to be classed as crimes in accordance with Home Office Counting Rules.

Figure 3. Internet users who were concerned about and experienced a negative online incident.



In March 2012, awareness of Action Fraud was low - just two per cent of internet users said they were of aware of Action Fraud as a place to report cyber crime.

- The police and the bank were the most common places internet users said they would report cyber crime incidents[18] (48% and 23% respectively). A further 16 per cent said they would report to an ISP and 5 per cent to a software company. Just two per cent said they would report to Action Fraud. It should be noted that this survey was carried out prior to full roll-out of Action Fraud, as the national reporting centre for fraud and financially motivated cyber crime; and therefore awareness of Action Fraud was not likely to be high. The Action Fraud roll-out was completed in April 2013.

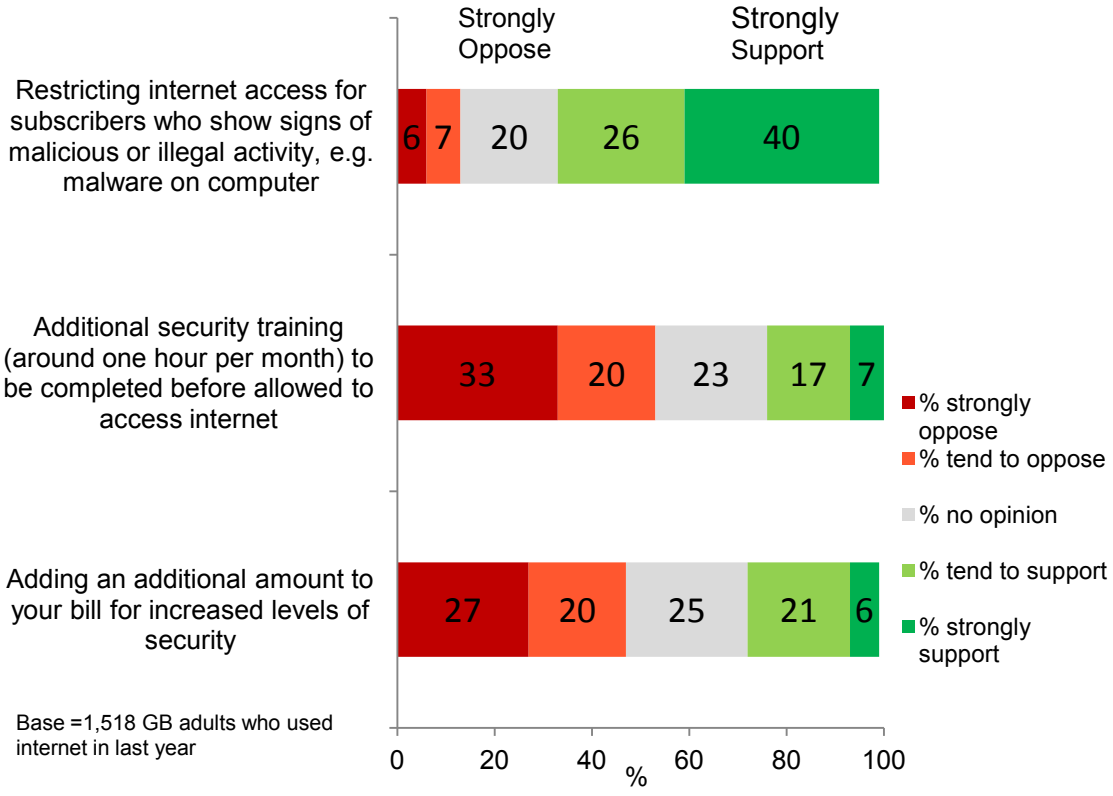
4. Additional security measures

Most internet users were unwilling to pay more or undertake training courses for additional online security. They were more in favour of restricting access for users who had undertaken malicious or illegal activity.

- When given three options for increasing online security (internet users paying more for increased security, internet users receiving ongoing training on computer security and best-practise, and restricting access to those found to be engaged in malicious or criminal computer activity), most respondents were opposed to making additional payments to ISPs (47% opposed, 27% supported) and undertaking training on security (53% opposed, 24% supported). Figure 4 reports these findings.
- Sixty-six per cent of respondents supported ISPs restricting access for people who showed signs of malicious online activity, such as sending viruses or malware from their computer. This compared with 13 per cent who opposed this measure.
- When internet users were asked to consider how much extra they would be willing to pay for improved security, the majority (62%) said nothing, whilst 15 per cent stated £1-2 a month and 6 per cent stated less than £1 per month.
- Those who support adding a monthly payment to their bill, and those who support having to undergo online training are less likely to have engaged with the security practises previously outlined in Figure 1 (such as regularly installing up-to-date security software).
- They are also more likely to have experienced one or more type of security breach than those who oppose either proposition (42% compared with 33% who oppose the payment proposition, and 46% compared with 30% who oppose the training proposition).

[18] Internet users were not asked where they had actually reported a cyber crime to, if they had been a victim. They were only asked about awareness of places to report cyber crime.

Figure 4. Levels of support amongst internet users for various measures to help increase online security



ISBN: 978-1-78246-245-3