Home Office

Cyber crime: A review of the evidence

Research Report 75

Chapter 1: Cyber-dependent crimes

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

October 2013

Cyber crime: A review of the evidence

Chapter 1: Cyber-dependent crimes

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

Cyber crime: A review of the evidence
Chapter 1: Cyber-dependent crimes

What are cyber-dependent crimes?

Cyber-dependent crimes (or ‘pure’ cyber crimes) are offences that can only be committed using a computer, computer networks or other form of information communications technology (ICT). These acts include the spread of viruses or other malware, hacking and distributed denial of service (DDoS) attacks. Definitions of these are outlined below. They are activities primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks. For example, data gathered by hacking into an email account may subsequently be used to commit a fraud. This chapter refers only to cyber-dependent crimes in their primary form – as offences ‘against’ computers and networks.

Main forms of cyber-dependent crime

Cyber-dependent crimes fall broadly into two main categories:

- illicit intrusions into computer networks (for example, hacking); and
- the disruption or downgrading of computer functionality and network space (for example, viruses and DDoS attacks).

The main forms of cyber-dependent crime are outlined below.[1]

Malware is a general label for malicious software that spreads between computers and interferes with computer operations (Kirwan and Power, 2012). Malware may be destructive, for example, deleting files or causing system ‘crashes’, but may also be used to steal personal data. There are a number of forms of malware.

- *Viruses* are one of the most well-known types of malware. They can cause mild computer dysfunction, but can also have more severe effects in terms of damaging or deleting hardware, software or files. They are self-replicating programs, which spread within and between computers. They require a host (such as a file, disk or spreadsheet) in a computer to act as a ‘carrier’, but they cannot infect a computer without human action to run or open the infected file (Moir, 2008).

- *Worms* are also self-replicating programs, but they can spread autonomously, within and between computers, without requiring a host or any human action. The impact of worms can therefore be more severe than viruses, causing destruction across whole networks (Beal, 2011). Worms can also be used to drop trojans (see below) onto the network system.

- *Trojans* are a form of malware that appear to be legitimate programs, but facilitate illegal access to a computer. They can perform functions, such as stealing data, without the user’s knowledge and may trick users by undertaking a routine task while actually undertaking hidden, unauthorised actions.

[1] See Furnell, 2010; Kirwan and Power, 2012 for further description.

- *Spyware* is software that invades users' privacy by gathering sensitive or personal information from infected systems and monitoring the websites visited. This information may then be transmitted to third parties. Spyware can sometimes be hidden within *adware* (free and sometimes unwanted software that requires you to watch advertisements in order to use it). One example of spyware is *key-logging software (see Case-study 1),* which captures and forwards keystrokes made on a computer, enabling collection of sensitive data such as passwords or bank account details. Another kind of spyware captures screenshots of the victim's computer. Spyware is considered to be one of the most dangerous forms of malware as its objective is purely to invade privacy (Furnell, 2010).

Case-study 1

Key-logging spyware used in cyber crime: A case-study

"[A hacker who] posed as a student in order to unlawfully gain access to the emails of hundreds of unsuspecting fellow students has been given a suspended prison sentence and ordered to pay over £20,000 in costs and compensation. [He was] arrested ... after being caught in the act of installing password-capturing software.

"[He] falsely claimed to be a student in order to gain access to a computer room on the campus. Once in, he used various hacking techniques [including the use of key-logging software] on a number of machines, which in turn enabled him to collect further student passwords and to covertly gather traffic passing through the university's computer network. [The cybercriminal] used these passwords to gain access to student email accounts to identify and target bank accounts linked to these email addresses. Police were able to establish that a number of these compromised accounts were subsequently the victims of fraud."

Metropolitan Police, 2010

http://content.met.police.uk/News/Computer-hacker-who-posed-as-student-sentenced/1260267431754/1257246842383*]*

Hacking
Hacking is a form of trespass. It is the unauthorised use of, or access into, computers or network resources, which exploits identified security vulnerabilities in networks. Hacking can be used to:

- gather personal data or information of use to criminals;
- deface websites; or
- be employed as part of denial of service (DoS) or DDoS attacks (see below).

Denial of service or distributed denial of service attack
DoS and DDoS relate to the flooding of internet servers with so many requests (for example, links that have been clicked) that they are unable to respond quickly enough. This can overload servers causing them to freeze or crash.

Spam
Spam is unsolicited or 'junk' email, typically sent in bulk to countless recipients around the world and is often related to pharmaceutical products or pornography. Spam email is also used to send phishing emails or malware and can help to maximise potential returns for criminals.)

Botnets
'Botnets' refer to clusters of computers infected by malicious software. They are used to send out spam, phishing emails or other malicious email traffic automatically and repeatedly to specified targets (Alhomoud *et al*., 2013). They are often termed 'zombies' as the networks are controlled centrally by a 'botmaster' (or 'herder').

Motivations behind cyber-dependent crimes
Motivations for cyber-dependent crimes focus largely around personal profit or financial gain (for example, the use of malware to gain access to bank account details) or can also be a form of protest and/or criminal damage (for example, hacking and website defacement). Motivations can largely be inferred by examining the function of the programs or tools that are used. Some research also suggests that there are more unorthodox motivations, for example, satisfying intellectual curiosity/challenge, general maliciousness, revenge, establishing respect and power amongst online communities, or even simply boredom (summarised in Kirwan and Power, 2012).

Cyber-dependent crimes vary in the extent to which they target specific victims, or are more random in nature. Viruses, for example, may be widely spread to infect large numbers of victims indiscriminately. Advanced persistent threats (APTs), on the other hand, refer to highly planned, sophisticated and prolonged attacks to achieve a specific goal, for example, in terms of taking down infrastructure or obtaining specific information about a person or organisation (Symantec, 2012). APTs are typically linked to state-sponsored cyber attacks e.g. Stuxnet and Flame[2].

Key findings: What is known about cyber-dependent crimes?

Scale and nature of cyber-dependent crimes

Victimisation surveys

Most surveys of the general public and businesses capture information on internet users' negative online experiences. The most robust of these, and conducted on a regular basis, are the Crime Survey for England and Wales (CSEW; for example, see ONS, 2012), and surveys by the Oxford Internet Institute (Dutton and Blank, 2013) and Ofcom (2013). One-off surveys have also been conducted by the ONS (2010) and Ipsos MORI (2013). Amongst businesses, one of the most robust surveys available is the 2012 Commercial Victimisation Survey (CVS).

These surveys do not, however, measure criminal activity or police recorded crime. So whilst they can be useful indicators, they do not give firm measures of prevalence for cyber-dependent (or cyber-enabled) crimes. It is unlikely that many of the experiences recorded in these surveys would meet the specific criteria to be classified as a 'crime' under Home Office Counting Rules[3] (HOCR) (see also p 11).

[2] Stuxnet was a highly sophisticated worm which targeted Iranian infrastructure linked to uranium enrichment processes. It caused failures in nuclear centrifuges by subverting SCADA systems. Flame was a specific malware device that was utilised for cyber espionage in the Middle East.
[3] For example, they do not determine whether the individual concerned was a 'specific intended victim', which is a key determinant in distinguishing between an actual crime or a crime-related incident, under HOCR. HOCR state, for example: *"Where viruses or malware, are launched onto the World Wide Web to infect any computer they come across, victim's computers that are infected are not generally specific intended victims. Where police receive reports under these circumstances, that computers have been infected by or received a virus or malware, then a crime related incident should be recorded."*

Public experiences of cyber-dependent crimes

Around one-third (37%) of adult internet users in the CSEW 2011/12 reported one or more 'negative online experiences' in the year prior to being interviewed (ONS, 2012). This was a small, but statistically significant decrease from 39 per cent in 2010/11 (ONS, 2011a), occurring largely as a result of a statistically significant decrease in the proportion of users experiencing a computer virus. Similarly, Ipsos MORI (2013) found that 36 per cent of adult internet users had experienced one or more negative incidents online in the year to March 2012.[4]

Table 1.1: Negative experiences in the last year among internet users aged 16 and over, Crime Survey for England and Wales, 2010/11 and 2011/12

	A computer virus (%)	**Unauthorised access to/ use of personal data (%)**	**Upsetting/ illegal images (%)**	**Loss of money (%)**	**Abusive/ threatening behaviour (%)**	**One or more negative incidents online (%)**
All internet users 2010/11 (unweighted base = 8,383)	33	6	4	3	2	39
All internet users 2011/12 (unweighted base = 8,373)	31	7	4	3	2	37

Source: ONS, 2011a; 2012.

Viruses are one of the most common negative online experiences reported (for example, in the CSEW; Oxford Internet Survey; Ipsos MORI). According to the 2011/12 CSEW, almost one-third (31%) of adult internet users experienced a virus in the 12 months prior to interview (ONS, 2012, Table 1.1). This compares with just three per cent reporting 'loss of money' in the same time period. Only receipt of spam has featured more highly in other surveys – reported by 54 per cent of internet users surveyed by ONS (2010) – though these surveys are not directly comparable.

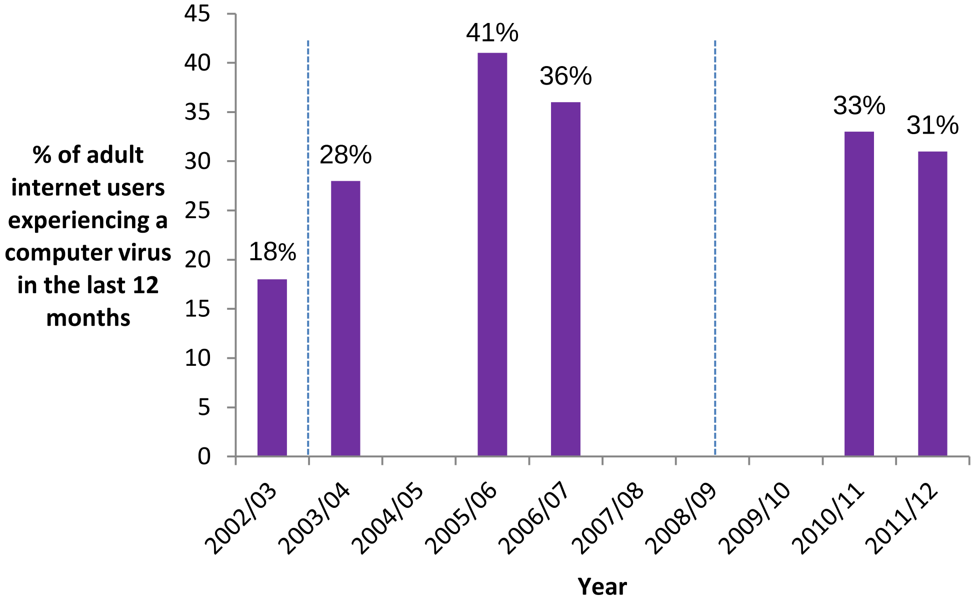
The proportion of adult internet users experiencing computer viruses appears to have decreased since the mid-2000s. Earlier data from the CSEW (formerly known as the British Crime Survey, see Figure 1.1) shows that the proportion of adult internet users experiencing computer viruses fell from a high point in 2005/06 (41%), to 31 per cent in 2011/12 (ONS, 2006; ONS, 2012). However, it should be noted that the wording of the question changed during this time period so the figures are not directly comparable and also the survey questions were not asked every year. The Oxford Internet Survey (Dutton and Blank, 2013) presents a slightly different trend, showing an increase in virus experiences from 31 per cent in 2009 to 38 per cent in 2011, followed by a fall in 2013 to 30 per cent.[5] The questions asked in these surveys do

[4] To note, 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.

[5] Survey differences may be due to survey coverage, for example the Oxford Internet Survey includes those aged 14 and over in Britain (n=2,657 in 2013); the CSEW includes those aged 16 and over and covers England and Wales only (n=8,373); it also has a considerably larger sample size.

not, however, take into account whether the virus had an effect on the computer or, for example, whether it had been successfully blocked by anti-virus software.

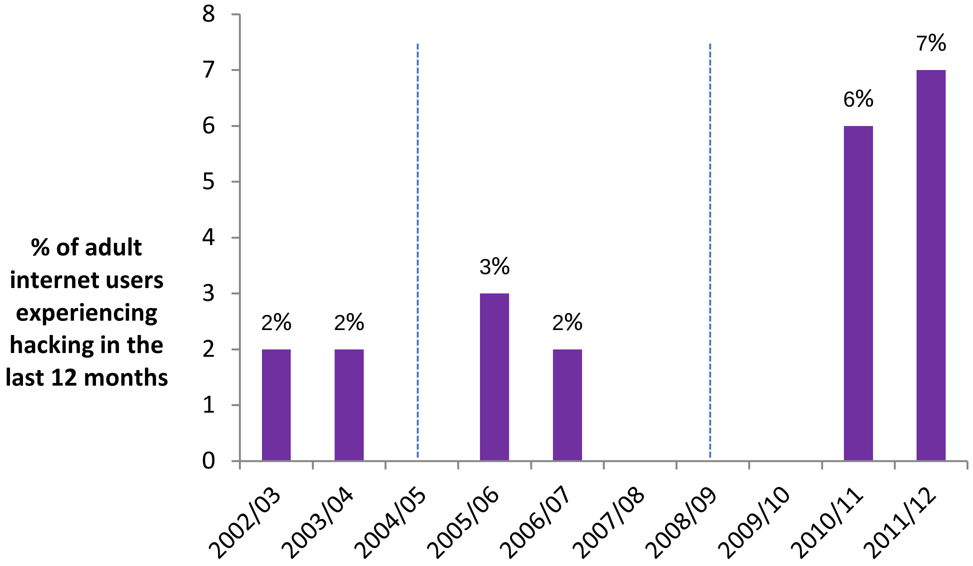
Figure 1.1: Experiences of a computer virus, by adult internet users in the last year, Crime Survey for England and Wales 2002/03 to 2011/12



Source: ONS, 2003; 2004; 2006; 2007; 2011a; 2012.
Note: The dotted lines relate to changes in the wording of the question. Due to these changes figures are not directly comparable. In 2002/03 the question asked: *"Has your HOME computer been affected by a computer virus?"* In 2003/04–2006/07 the question asked: *"Has your home computer been damaged by a virus, [or] been infected by a virus but not actually damaged?"* In 2010/11–2011/12 the question asked: *"Have you personally experienced a computer virus?"*

The proportion of adult internet users experiencing hacking is smaller than for those experiencing computer viruses, but the experience appears to be increasingly reported amongst internet users (see Figure 1.2). There was a statistically significant increase in the proportion of adult internet users who had their personal computers accessed, or hacked, without their permission from two per cent in 2006/07 to seven per cent in 2011/12 (ONS, 2007; ONS, 2012). However, there was a change in the wording of the question during this time. Ipsos MORI (2013) also found that five per cent of adult internet users had experienced unauthorised access to, or use of, their personal data in the year prior to March 2012.

Figure 1.2: Experiences of hacking, by adult internet users in the last year, Crime Survey for England and Wales, 2002/03 to 2011/12



Source: ONS, 2003; 2004; 2006; 2007; 2011a; 2012.
Note: The dotted lines relate to changes in the wording of the question. Due to these changes, figures are not directly comparable. In 2002/03–2006/07 the question asked: *"In the last 12 months, has anyone accessed or hacked into the files on your home computer without your permission?"* In 2010/11–2011/12 the question asked: *"Have you personally experienced unauthorised access to/use of personal data (e.g. email account, bank account?"*

Business experiences of cyber-dependent crime

The 2012 CVS is a survey of crime, including online crimes, experienced by businesses operating in four sectors: manufacturing; wholesale and retail; transportation and storage; and accommodation and food. The results of the CVS are representative of online crime incidents against the four sectors covered, but are not representative of businesses as a whole. In addition, the CVS is a premises-based (rather than head office-based) survey and many types of online crime may therefore not be picked up by the CVS as they do not affect businesses at the premises level. In addition, not all incidents reported in the survey would be classed as a crime under Home Office Counting Rules.

Across the four sectors surveyed eight per cent of business premises experienced at least one type of online crime in the 12 months prior to the survey (Home Office, 2013a, see Table 1.2). This equated to an estimated 180,000 incidents of online crime in total across the four sectors. Three-quarters of the incidents (135,000) related to viruses. The manufacturing sector was the most likely to experience online crime, with 12 per cent of premises experiencing at least one form.

Table 1.2: Proportion of business premises that experienced online 'crime' in the last 12 months, by industry sector, Commercial Victimisation Survey 2012

	Manufacturing (%)	Wholesale and retail (%)	Transportation and storage (%)	Accommodation and food (%)	All four sectors
Hacking	4	1	1	1	2
Phishing	0	0	0	0	0
Theft of money (online)	1	1	1	0	1
Theft of information (online)	0	1	0	0	0
Website vandalism	0	0	1	1	0
Computer virus	11	6	9	4	7
All online 'crime'	12	7	10	6	8

Source: Home Office (2013a)

The PwC survey of business security breaches has run annually for a number of years. It is one of the most in-depth surveys of security breaches available, although the methodologies used for the survey have varied over time. In earlier years, the survey adopted a more robust random probability sampling method, showing a decline in the proportion of businesses reporting any security incident from 62 per cent in 2006, to 45 per cent in 2008 (BERR, 2008). There was also a decline in businesses reporting a malicious security breach, falling from 52 per cent in 2006 to 35 per cent in 2008. From 2010 onwards, the methodology changed to a self-selecting, non-random sample. The most recent survey (PwC, 2013) found that 93 per cent of large organisations and 87 per cent of small organisations reported any kind of a security incident. It is not possible to compare these later figures with the earlier trend data.

Police recorded crime and Action Fraud

For more traditional types of crime, data sources such as Home Office police recorded crime would be consulted. However, police recorded crime does not distinguish online from offline offences, making it difficult to identify both cyber-dependent and cyber-enabled crimes.

Police record crime in accordance with the provisions of the 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 1990 – police recorded crime does not generally distinguish between online and offline 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, 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 offences and classifies them in a way which allows distinctions to be made between computer misuse, online fraud and offline fraud offences. 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 data rollout period show that a total of 7,427 crimes and incidents relating to computer misuse and extortion were reported to Action Fraud between January and December 2012 (Action Fraud, 2012). These accounted for five per cent of incidents and crimes reported to Action Fraud during this time. The most common incident reported was illicit distribution of viruses, spyware or other malware (3,949 reports), closely followed by hacks into social media and email accounts (1,603 reports). These new data provide an indication of the type of information that is 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.
As awareness of the reporting facility increases, it is expected that there will be an increase in reporting, which will be captured in the 2013 data.

The HOCR set out the principles under which reports received from victims are recorded and whether an incident is counted as a 'crime'. Police recorded crime statistics are based on a notifiable list of offences. The HOCR set out the broad classification groups into which those offences are managed for statistical purposes. One of the general rules for counting a crime in HOCR relates to whether the individual concerned was a 'specific intended victim'. The HOCR state, for example:

"Where viruses or malware are launched onto the World Wide Web to infect any computer they come across, victim's computers that are infected are not generally specific intended victims. Where police receive reports under these circumstances, that computers have been infected by or received a virus or malware, then a crime related incident should be recorded."

Victims therefore need to have been specifically targeted for it to be recorded as a crime. Another element to this is action taken by the victim. If the victim reports that they knowingly took a positive action that led to receipt of the virus, for example, clicked on a link in an email that led them to an internet page that downloaded malware onto their computer, then a crime would also be recorded (as 'unauthorised modification of computer material') as they were also a 'specific intended victim'.

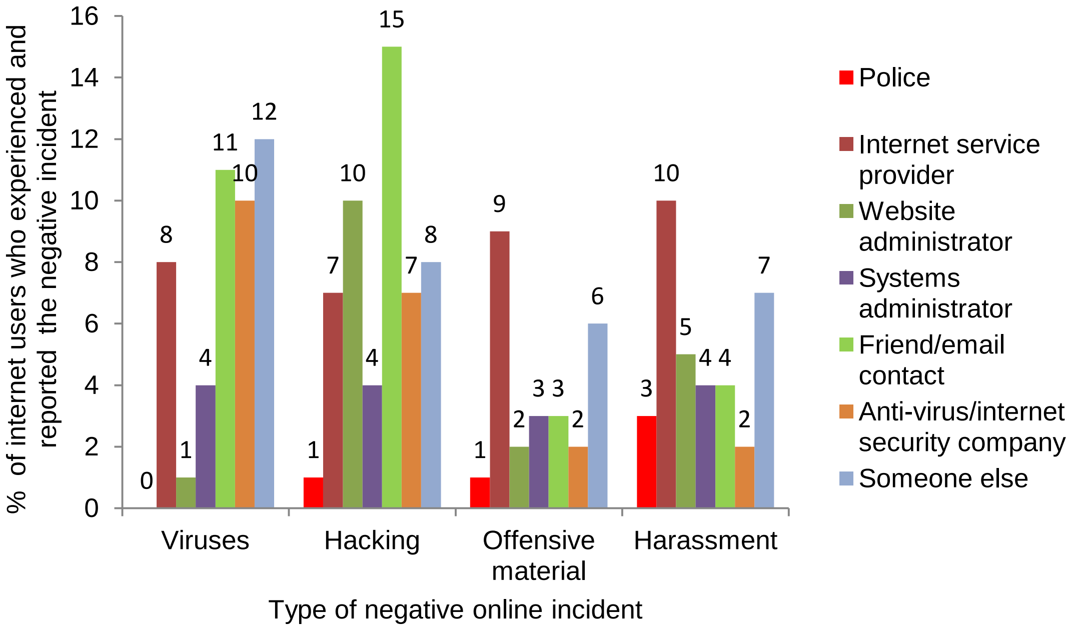
Further details surrounding Home Office Counting Rules for cyber-dependent crimes are outlined at:
www.gov.uk/government/uploads/system/uploads/attachment_data/file/210800/count-fraud-april-2013.pdf.

Under-reporting amongst the public and businesses

A particular challenge for determining the levels of cyber-dependent crime amongst the general public and businesses relates to under-reporting. Survey data show that levels of reporting to the police are low compared with other crime types.

According to the 2006/07 CSEW (ONS, 2007), just one per cent of adult internet users who experienced hacking or unauthorised access to their data in the year prior to interview reported this to the police. Almost no one reported experiences of viruses (see Figure 1.3). This compares with 81 per cent who reported a burglary to the police and 55 per cent who reported a robbery in the same year. Victims were more likely to report to internet service providers or website administrators (for example, 8% reported a virus to an internet service provider and 10% reported a hacking incident to an administrator).

Figure 1.3: Reporting of negative online experiences to different organisations, by adult internet users who had the experience in the last year, Crime Survey for England and Wales 2006/07



Source: ONS (2007)

There are a number of reasons why victims may not report, for example, if they do not realise the incident is a ‘crime’ or if it is perceived as too trivial. Some people may not even realise that they have been a victim – some sophisticated forms of malware may operate without individuals being aware of them and victims may not be able to identify the cause of a financial loss. Even if victims are aware of what has happened, they may still not perceive themselves as a ‘victim’, particularly if they are reimbursed by their bank. Unlike other forms of crime, there is no need to report to Action Fraud and receive a crime reference number in order to be reimbursed.

Broadly, it is a similar picture amongst businesses. Just two per cent of online crime incidents experienced by businesses in the 2012 CVS (2013a) were reported to police. This compares with 88 per cent of incidents related to burglary with entry that were reported to police. The most common reasons for non-reporting were because the incidents were perceived as too trivial or regarded as private and dealt with internally. Available research (for example, Fafinski and Minassian, 2009) outlines other common concerns amongst businesses regarding damage to reputation from cyber crimes and a desire to avoid publicity of any problems. BERR (2008) found that 97 per cent of the worst security incidents were only shared internally.

Prosecutions and convictions

Another potentially useful source of data is held by the Ministry of Justice (MoJ), which holds data on numbers of offenders proceeded against and convicted under particular criminal legislation. The Computer Misuse Act (CMA) 1990[6] captures four cyber-dependent offences, which make hacking, creation and distribution of malware and other instances of computer misuse, an offence.[7] However, MoJ data reveal that very few people have been sentenced under the CMA (see Table 1.3). Between 2007–12 101 people were initially proceeded against and 88 people were sentenced with a primary offence under the CMA (Ministry of Justice, 2013). The seemingly low level of sentencing under the CMA can be explained by individuals being proceeded against for cyber offences under other Acts, such as the Fraud Act 2006 (where 45,687 people were sentenced in the year to end March 2012 for fraud and forgery offences). However, the number of individuals sentenced under the Fraud Act 2006, or other Acts, for offences that had a cyber-component is not known.

Table 1.3: Numbers of individuals proceeded against, found guilty and sentenced under the Computer Misuse Act, 2007–12

Computer Misuse Act 1990	2007	2008 (note 2)	2009	2010	2011	2012	Total
Proceeded against	19	17	19	10	11	25	101
Found guilty (note 3)	10	12	10	18	11	27	88
Sentenced	9	13	10	18	11	27	88

Source: Ministry of Justice (2013)
Note 1: The figures given relate to persons for whom these offences were the principal offence for which they were dealt with. However, it is important to note that these data have been extracted from large administrative data systems generated by the courts and police forces. As a consequence, care should be taken to ensure data collection processes and their inevitable limitations are taken into account.
Note 2: Excludes Cardiff Magistrates' Court records for June, July and August 2008.
Note 3: The number of defendants found guilty in a particular year may differ from the number proceeded against as the proceedings in the magistrates' courts took place in an earlier year and the defendants were found guilty at the Crown Court in the following year; or the defendants were found guilty of a different offence to that for which they were originally proceeded against.
Note 4: The number of offenders sentenced can differ from those found guilty as it may be the case that a defendant found guilty in a particular year, and committed for sentence at the Crown Court, may be sentenced in the following year.

Industry sources

A lot of information on cyber-dependent crimes comes from industry reports, notably security and anti-virus (AV) providers. AV providers generally conclude that security ‘attacks’ globally are high (in the billions) and levels are increasing. Symantec (2012) for example, reported blocking 5.5 billion ‘attacks’ in 2012, an increase of over 81 per cent from 3 billion reported blocks in 2010. It also reported detecting 403 million unique variants of malware globally in 2011, compared with 286 million in 2010.

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

[7] Section 1 of the Act covers *“unauthorised access to computer material”* along with Section 2 *“unauthorised access with intent to commit or facilitate commission of further offences”*. These sections primarily make hacking an offence. Section 3 covers *“unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer”*, which makes it an offence to modify a computer (for example, via malware). Section 3A (introduced in 2008) makes it a further offence to *“make, supply or obtain articles for use”* in Section 1 and 3, which includes individuals writing malware for others.

However, there are limitations with the data generated by AV providers, particularly when comparing data from different providers. They may adopt:

- different names for malware families and the variants or strains of these;
- different or inconsistent units of measurement, such as unique incidents; whether malware is 'in the wild', versus those which are confined to AV laboratories; zero-day attacks (the use of a previously unknown exploit in a target system); detections and removals from AV systems;
- different geographical and customer base coverage; and
- largely ill-defined terms (such as 'attacks') along with a lack of transparency in how figures are produced.

The majority of AV reports are also global rather than UK-specific, which limits the extent to which they can shed light on the UK situation. The British Society of Computing (BSC) has recommended caution with the use of industry figures (House of Commons Science and Technology Committee, 2012).

On the other hand, AV reports are helpful in informing on the nature of various threats even if they do not present a reliable measure of the scale of the UK problem. For example, reports by Symantec (2012) and Sophos (2012) outlined the emergence of new threats such advanced persistent threats[8] (which include state-sponsored activity), the rise of mobile malware and the availability of 'fake anti-virus', which is a form of malware that can be downloaded online and imitates legitimate anti-virus software (*see Case-study 2*). Further evidence from industry reports on specific types of cyber-dependent crimes are outlined below.

Case-study 2

Fake anti-virus

"This malware … uses social engineering to lure users onto infected websites. Once the fake antivirus is downloaded onto the user's computer, the software attempts to scare them into believing that their system is infected with threats that do not really exist, and then push users to purchase services to clean up the non-existent threats. The fake antivirus will continue to send these annoying and intrusive alerts until a payment is made. The great threat of fake antivirus is the risk to victims' personally identifiable information, which is extracted and exploited by the affiliate networks that publish this malware."

Sophos, 2011

Malware and potentially unwanted software

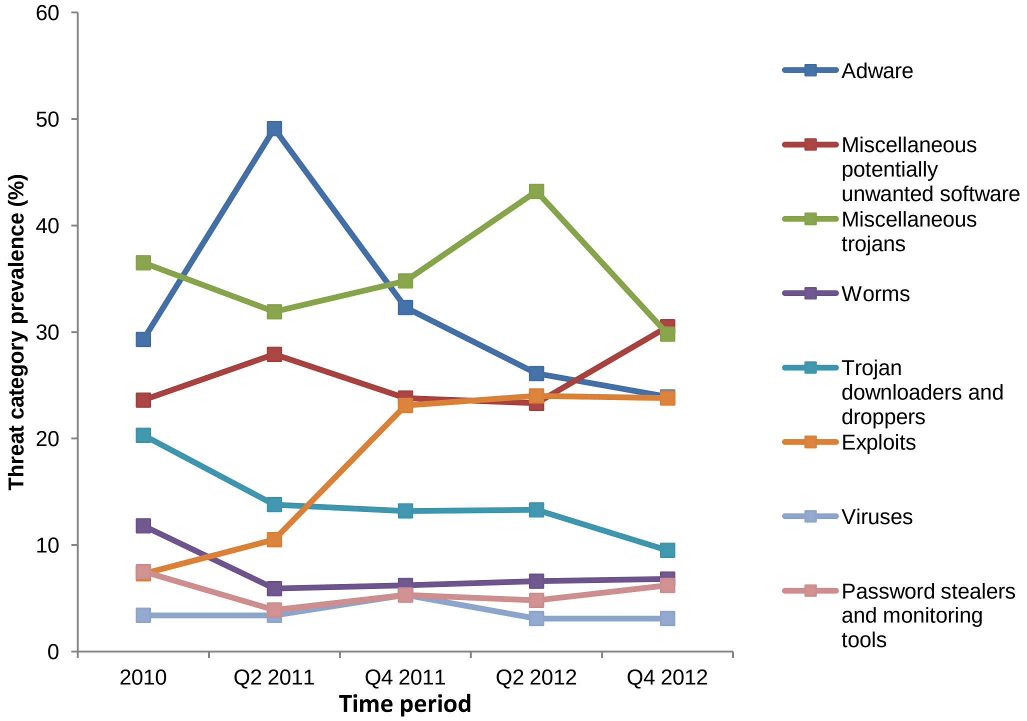
The BSC stated in its evidence to the Home Affairs Select Committee on Science and Technology, that there are no authoritative statistics on what proportion of cyber crime is associated with malware; nor on how many PCs in the UK are infected with a virus or other malware. It suggested a possible range of 1 to 15 per cent, with 5 per cent as a conservative estimate (House of Commons Science and Technology Committee, 2012).

[8] These are targeted attacks that use highly customised tools and intrusion techniques to gain access to high-value sensitive information of particular concern to high-profile businesses and state infrastructure (Symantec, 2012).

Some security providers report data on numbers of computers reporting detections and removals using their software. For example, Microsoft reported around 1.5 million detections in the second half of 2012 in the UK, a decrease of nearly 6 per cent from the first half of 2012 (Microsoft, 2013). However, its estimates relate only to those computers running the Microsoft removal tool and whose users are willing to share the data with the company. The results are not likely to truly reflect the population of Microsoft users with infections. The figures are also provided in absolute terms (and thereby skewed by size of population and numbers of computers).

In terms of the *types of malware threats* that appear most often, Microsoft (2011b; 2011c; 2012; 2013), suggest that trojans and adware were the most common forms of threat in the UK during 2011 and in the first half of 2012 (as detected by computers cleaned by their products, see Figure 1.4)*.* Adware also appeared to be declining whilst threats from trojans were increasing during this time. In the second half of 2012, the threat posed by trojans had receded somewhat, while 'miscellaneous potentially unwanted software' rose to become one of the most common forms of threat in the UK. The proportion of exploits[9] detected also increased from 11 per cent in the 2nd quarter of 2011, to nearly 24 per cent in the 4th quarter 2012. In comparison, the proportion of viruses and spyware detected was much smaller. A different analysis by PandaLabs (reported in APWG, 2012a; 2012b; 2012c; 2013) agreed with this trend (though the specific figures differ).

Figure 1.4: Malware threat category prevalence in the UK,(percentage of detections of each malware threat based on computers cleaned for every 1,000 executions of the Microsoft Malicious Software Removal Tool), Microsoft 2010–2012



Source: Microsoft (2011a; 2011b; 2011c; 2012; 2013)

[9] 'Exploits' are pieces of software, data or command sequences that take advantage of any vulnerability in a computer system to cause unintended and/or undesirable outcomes. Uses of exploits can vary, but may be used to gain unauthorised access to computers and aid with denial of service (DoS) or distributed DoS (DDoS) attacks (Szor, 2005).

Spam

Security providers suggest that levels of spam traffic are falling as a proportion of all email traffic. Symantec (2013) reported that globally, spam fell from 75 per cent of all email in 2011 to 69 per cent in 2012. Other sources (for example, CISCO, 2013) have also reported declines in the levels of spam globally. McAfee (2012) and others (for example, Microsoft, 2013) reported pharmaceutical spam as the most common type in circulation both in the UK and globally.

Spam is generally considered a high-volume but low-impact threat (especially as many email providers automatically filter spam). It is of more concern in cases where users have pay-as-you-go or capped data tariffs, and the downloading of spam is consequently eating into their allowance, but it may be a particular threat if it is being used maliciously to send phishing emails or malware.

Distributed denial of service attacks

Limited industry data available suggest that the UK is not a key target for distributed denial of service (DDoS) attacks. Kaspersky (2011) reported that the UK was subject to less than four per cent of total DDoS attacks globally. Globally, online shopping sites were the most common targets for DDoS attacks (25%), along with banks and stock exchanges (23%) and gaming sites (20%).

Some small-scale surveys of businesses give evidence of experiences of DDoS attacks, although the self-selecting nature of these surveys means that the inferences that can be drawn from them are limited. For example, a DDoS protection provider called Neustar found that in a survey of 381 businesses, 22 per cent had experienced a disruptive DDoS attack in 2012 (Neustar, 2012). The largest proportions of respondents experiencing attacks were from the telecommunications (53%), internet/e-commerce (50%) and online retails sectors (43%). Over one-third (37%) of all DDoS attacks reported in the survey lasted over 24 hours.

Hacking

Limited international data available from industry sources on hacking suggest that hacking attempts are increasing. The NCC group (a US security company) analysed intrusion detection logs and reported 981 million hacks were attempted globally in the third quarter of 2012 (NCC, 2012). This was 23 million more than in the second quarter and followed four consecutive quarters of increase, as observed by the company.

NCC (2012) also reported that hacking activity originating from the UK appeared to decrease during 2012. In the 1st quarter of 2012 the UK was ranked 7th in the world for hacking activity (representing 2.4% of all attacks globally), falling to 12th by the 3rd quarter (representing 1.6% of all attacks). The US remained the number one country for the origin of hacks in the 3rd quarter of 2012, representing nearly 21 per cent of all attacks globally, followed by Russia (19.1%) and China (16.3%).

These data on hacking should be treated carefully though, as it is unclear exactly how the authors traced the origins of the unauthorised network access, how the data were counted or collected, and if this is representative of all such cases. The data appear to be based only on reports from companies (and not necessarily the public) using a specific security product called ‘DShield’. It is also uncertain how many of

these attacks were successful. There is little other evidence available to compare on this topic.
International comparisons

Industry reports find that the UK compares relatively well to other countries in terms of exposure and vulnerability to security threats, but lack of clarity and comparability in reporting means that there is no certainty about how robust this assessment is. 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%).

Analysis by PandaLabs (APWG, 2013) also suggests that the UK has low malware infection ratios compared with other countries. Taking samples from 50 countries worldwide, the average infection ratio (the average number of infected PCs) for these countries was around 30 per cent. European countries were typically the least infected and Asian and South American countries the highest.[10] In the last quarter of 2012, the UK ranked 37 out of the 44 countries sampled, with a malware infection ratio of just over 23 per cent. Finland held the lowest infection ratio (just over 18%).

Other reports, for example, Microsoft (2013) present a less positive picture. Microsoft placed the UK at tenth in the world ranking of *"most infected nations",* with the US at number one (based on the number of computers reporting detections and removals by Microsoft desktop anti-malware products).

Characteristics of victims

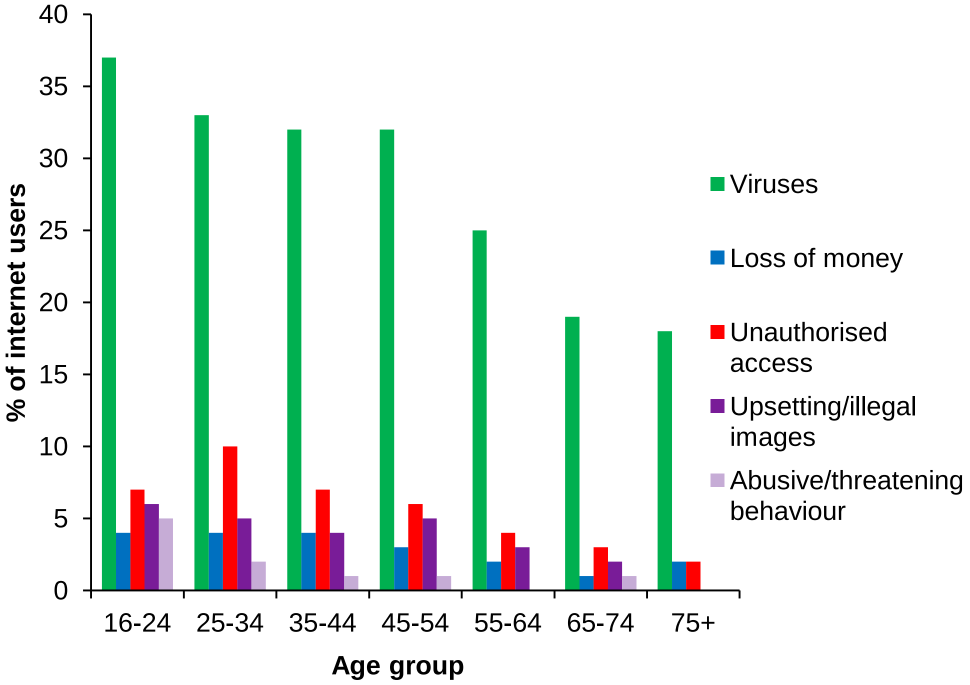
The general public

Victimisation surveys suggest that younger people and men who use the internet appear to be more vulnerable to computer viruses. The Crime Survey for England and Wales found that computer viruses in 2011/12 were statistically significantly more likely to be experienced by men (35%) than women (27%) (ONS, 2012). They were also more likely to be experienced by those in younger age groups (37% of 16- to 24-year-olds and 33% of 25- to 34-year-olds) compared with those aged 35 and over (for example, 25% of 55- to 64-year-olds).

Men (7%) were also more likely than women (6%) to have reported experiencing unauthorised access to/use of their personal data in the past year (ONS, 2012). The experience was statistically significantly less likely among the older age groups (those aged 45 and over) compared with other age groups and, specifically within this age range, men aged 65–74 were more likely to report than women aged 65–74.

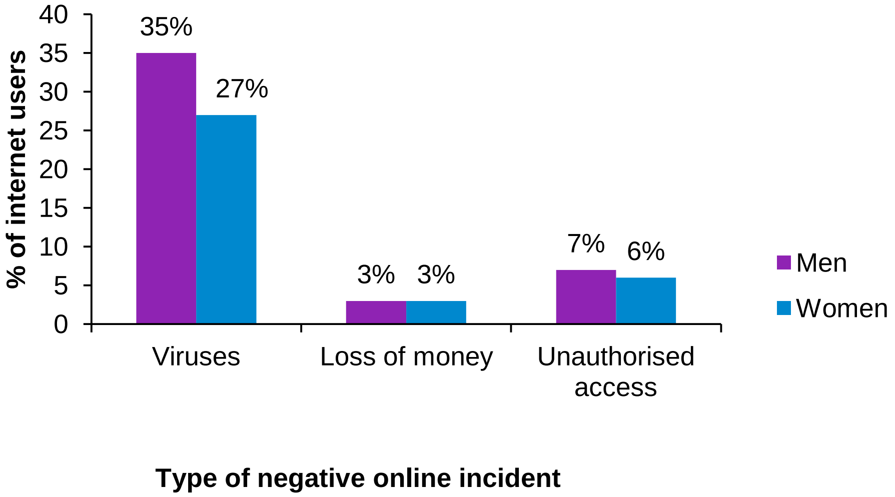
[10] This trend holds true in the first half of 2012, although only 32 countries were sampled.

Figure 1.5: Experiences of negative online incidents, by age group in the last year, Crime Survey for England and Wales 2011/12



Source: ONS (2012)

Figure 1.6: Experiences of negative online incidents for men and women in the last year, Crime Survey for England and Wales 2011/12



Source: ONS (2012)

Security behaviours amongst the general public

Take-up of anti-virus software by adult internet users generally appears high. Around two-thirds (67%) of adult internet users in the 2011/12 CSEW reported installing up-to-date anti-virus software (ONS, 2012).

However, 'up-to-date' could mean many things: yesterday or six months ago; or an up-to-date AV package rather than up-to-date malware signatures.[11] AV software also needs to be configured correctly and this is not always the case. Studies in the US, involving the National Cyber Security Alliance (McAfee-NCSA, 2007), have shown a frequent gap between user's beliefs about what they have running on their systems and what an inspection of their system actually reveals. Many were less well protected than they thought when answering surveys.

Beyond anti-virus, wider security practices are not universally undertaken. The CSEW (ONS, 2012) found that three in five (61%) adult internet users looked for secure sites, but just one in four (24%) only use credit cards (rather than debit/charge cards) when shopping online, and just over one in four (27%) stated that they avoided putting personal details online. Slightly different findings have been found in other surveys, for example, an Ipsos MORI (2013) survey found that just 43 per cent of adult internet users surveyed checked that sites were secure (i.e. displayed the closed padlock, or 'https' prefix). These differences are likely to be due to differences in terms of survey methodology and sample size. In terms of social networking behaviours, YouGov (2012) reported that 52 per cent of UK citizens indicated that they would accept a friend request on Facebook from someone they did not know directly.

The youngest and oldest user groups have been identified as less likely to adopt secure behaviours online (ONS, 2012; Ipsos MORI, 2013). For example, the 2011/12 CSEW reported that adults in the oldest age group (aged over 75) were statistically significantly less likely to have up-to-date security software than those aged 35–64, and less likely to use well-known or trusted sites than all those aged below 65. Those aged over 75 were also statistically significantly less likely to look for secure sites than all younger age groups (ONS, 2012). Ipsos MORI (2013) reported that younger users were statistically significantly less likely to use internet security software on all devices (70%) compared with older users aged 65 and over (92%). Black and minority ethnic (BME) and less affluent groups (defined in the survey as skilled or non-skilled manual labour and non-working employment roles) have also been identified as potentially vulnerable groups. Ipsos MORI (2013), reported that 55 per cent of ethnic minority groups and 65 per cent of less affluent users were statistically significantly less likely to have internet security software compared with 81 per cent of White users and 89 per cent of more affluent users (defined as those in managerial, administrative and professional employment roles) .

Platform use

Mobile phones and smartphones can be at risk of cyber crime in addition to desktop or laptop computers. Just 46 per cent of mobile phone users and 57 per cent of smartphone users were aware of AV for their phone or smartphone (Ofcom, 2013).[12] An even lower proportion reported using AV for their mobile phone (18%) or smartphone (27%). However, it is unclear what type of mobile phone was held by

[11] A malware signature is an algorithm or number that uniquely identifies a specific malware, either by tagging parts of the malware code itself, or by identifying the malware's actions when in the computer.
[12] N=1,647 for mobile phone users, n=658 for smartphone users.

users in this research. This is important as iPhones are protected from malware through Apple's approval process for code to be included in the App Store (which is the only route for installing software on the phone unless it has been jailbroken).[13] This closed approach limits the potential for malware code to get onto the devices.[14] Android platforms, however, require users to download AV to obtain such protection.

Another area for potential risk is public wi-fi use. Just 5 per cent (n=1,458) of internet users in a survey by Ipsos MORI (2013) said that they used a public wi-fi connection for at least an hour a week. However, a greater proportion of public wi-fi users had experienced 1 or more security breaches compared with those using home connections (53% compared with 35%). This raises questions regarding vulnerabilities amongst public wi-fi users (*see Case-study 3*). However the analysis was based on a very small sample of wi-fi users and it is unknown whether the public wi-fi was directly related to the security breaches asked about in the survey. However, use of public wi-fi is growing – ONS (2011b) reported a sevenfold increase in the use of public wi-fi hotspots, from 0.7 million in 2007, to 4.9 million in 2011.

Case-study 3

Mobile threats: Wi-fi hacking

"The hacking tool…was released in late 2010. With (this tool) a person with malicious intent can run the Firefox plug-in and view specific user accounts that can access the wi-fi network simply by clicking the icon presented in the plug-in pane. Rather than steal user credentials, such as username and password, it intercepts the unencrypted cookie. Because access to the cookie enables the hacker to log in as the authenticated user simply by clicking an icon, this type of attack is very powerful. With the tool hackers can easily exploit a user's email account on any Wi-Fi enabled device."

Juniper Networks, 2012

Businesses

According to the 2012 CVS (2013b), there were no clear differences in terms of business size in relation to experiences of online crimes – both large and small businesses reported being victims. The survey showed that 11 per cent of businesses with 50 or more employees had been a victim of one or more online crime incidents, compared to nine per cent with 10–49 employees and 8 per cent with 1–9 employees.

[13] 'Jailbroken' refers to i-phone modifications, which let users install applications that are not officially released through Apple's 'App Store' (wiseGEEK, 2013).

[14] Although this does not necessarily mean that iPhone users are totally immune (as noted by Sophos, 2012) with the rise of iPhone-specific malware appearing within the Apple App store. Moreover, password and encryption attacks can still succeed in some cases.

Table 1.4: Proportion of business premises that experienced online 'crime' in the last 12 months, by size, Commercial Victimisation Survey 2012

	1–9 employees (%)	10–49 employees (%)	50+ employees (%)	All four sectors[1] (%)
Hacking	2%	2%	2%	2%
Phishing	0%	0%	0%	0%
Theft of money (online)	1%	0%	0%	1%
Theft of information (online)	0%	1%	0%	0%
Website vandalism	0%	1%	1%	0%
Computer virus	7%	7%	10%	7%
All online 'crime'	**8%**	**9%**	**11%**	**8%**
Unweighted base	946	559	492	1,997

Source: Home Office (2013b)

Note 1: The four sectors covered in the survey are: wholesale and retail; manufacturing; transportation and storage; and accommodation and food.

Security behaviours amongst businesses

Almost all (97%) businesses from the four sectors surveyed in the CVS adopted one or more forms of security on their computers. The most common measure was AV or anti-spam software, used at 92 per cent of premises (see Table 1.5), followed by firewalls (86%). Around one-half of premises (51%) stated that they had a data security policy, staff code of conduct for computer use or a data security officer responsible for ensuring data security (Home Office, 2013b).

In general, the proportion of premises with security measures on computers increased with business size. For example, 91 per cent of organisations with over 50 employees had a data security policy in place compared with just over 43 per cent of businesses with 1–9 employees. However, both small and large businesses were almost equally likely to have AV/anti-spam software and firewalls (Home Office, 2013b).

Table 1.5: Security measures on computers at premises[1] in the last 12 months, by business size, Commercial Victimisation Survey 2012

	1–9 employees	10–49 employees	50+ employees	All business sizes
	%	%	%	%
Anti-virus/anti-spam software	93	87	92	**92**
A firewall	87	82	92	**86**
A data security policy	43	68	91	**51**
Restrictions on staff internet use	42	64	82	**49**
Encryption software	46	52	70	**48**
Restrictions on mobile data storage devices	28	41	64	**33**
None	3	2	1	**3**
Other	1	1	0	**1**
Unweighted base	*682*	*483*	*459*	***1,624***

Source: Home Office (2013b)
Note: 1 The four sectors covered in the survey are: wholesale and retail; manufacturing; transportation and storage; and accommodation and food.
Note 2: Questions on computer security only asked of those premises with computers. These figures exclude those who answered 'don't know' to these questions on computer security.

Estimating the costs of cyber crime

Estimating the costs for all types of cyber crime (not just cyber-dependent crime) is challenging. The first main attempt to do so was conducted by Detica (2011), which estimated overall costs of £27 billion to the UK. As outlined by the Home Affairs Select Committee (2013) report on e-crime, the precision of this estimate has subsequently been questioned (for example, Anderson *et al.*, 2012) due to the lack of robust and transparent data upon which their estimates were based. The UK cyber security strategy (Cabinet Office, 2011) recognised the challenges in this area and noted that: *"a truly robust estimate will probably never be established, but it is clear the costs are high and rising"*.

Some progress in this complex area has been made with work conducted by Anderson *et al.* (2012) who sought to estimate separate costs for different cyber crimes (including cyber-dependent crimes), and opted not to produce one total estimate given the paucity and level of reliability of the data available. Anderson *et al*. drew largely upon data from global case-studies and excluded costs for particular crime types where there were insufficient data. Estimates for the UK were partly based on scaled down global estimates, based on the UK being five per cent of the world in terms of gross domestic product (GDP). For example:

- revenue obtained by criminal gangs from fake anti-virus was estimated at $5m for the UK. This was based on an estimated $97 million in terms of global revenue using evidence found on internal databases of sales and prices run by three criminal gangs during 2008–10.
- annual botnet herder income was estimated to be in the single millions per year,[15] assuming: there are approximately 50 million bots worldwide with a

[15] Based on research by Florencio and Herley (2011).

> herder income of 50 cents per machine per week, meaning that a 20,000-machine botnet earns a herder $190 a week.

Anderson *et al*.'s approach provided a step forward in this area, although there are limitations to their method. Depending heavily on a GDP-based share of total crime costs to calculate UK estimates relies both on the accuracy of the global estimates used and the assumption that the relative proportion of an offending category in the UK is always equal in cost to its proportionate GDP. Based on the limited research available (i.e. Anderson *et al*.'s work), the costs of cyber crime could reasonably be assessed to equate to several billion pounds per year. To develop a more precise assessment of the cost of cyber crime our understanding of the prevalence of different types of cyber crime must be markedly improved (see Chapter 4: 'Improving measurement of cyber crime').

The available literature in this area also focuses on impacts from cyber crimes in monetary terms. However, there may be a range of non-financial impacts as well. The BSC (House of Commons Science and Technology Committee, 2012) specifically mentions the possibility of:

- criminal charges to be brought against owners who unknowingly were in possession of a bot-infected machine, or machines being used to host illegal content, such as child pornography;
- loss of sensitive or personal data impacting on personal relationships; and
- irreplaceable loss of some items stored on computers.

Further work looking at wider impacts in this area and how these could be incorporated into assessments of cost and harm would be beneficial.

Characteristics of offenders

There is limited published UK evidence available regarding the characteristics of cyber-dependent offenders*.* Published evidence is generally reliant upon small numbers of offender case-studies or interviews and tends to focus on their methods and motivations (as discussed on p 6). The main exception is the Offending, Crime and Justice Survey. There is little published evidence around offender characteristics, their backgrounds, career pathways, the links between online and offline offending and progression into different criminal roles and interventions to prevent (re-)offending.

The Home Office Offending, Crime and Justice Survey (OCJS) provides some insight into the characteristics of cyber-dependent and cyber-enabled offenders. The survey was the first and only nationally representative survey of self-reported offending carried out every year between 2003–06 and includes questions on self-reported technology offending (Allen *et al*., 2005). Despite the survey now being quite dated it can help to fill some knowledge gaps in this area. Not all of the offending behaviours included in the survey necessarily relate to criminal activity, nor would they all be classed as a crime within Home Office Counting Rules.

The most common technology-related activity amongst young people was illegal downloading. In the 2004 OCJS around one in four (26%) of 10- to 25-year-old internet users reported that they had illegally downloaded software, music or files in the 12 months prior to the survey (Wilson *et al.*, 2006).

In relation to cyber-dependent offending, 1 per cent of internet users aged 10 to 25 years had sent a computer virus in the 12 months prior to the survey and the same proportion reported using a computer to access another person's computer files without permission. Males were more likely than females to report both sending viruses (2% compared with 1%) and gaining unauthorised access (2% compared with 1%). Age differences are also evident, with 10- to 17-year-olds more likely than 18- to 25-year-olds to participate in both activities (2% versus 1% for both viruses and hacking).

Cyber-enabled offending was rare. The number of young people who reported obtaining someone else's card details over the internet was very low (0.1% of all 12- to 25-year-olds), and the same proportion reported buying goods or services over the internet using someone else's card details without the card owner's permission (0.1% of 12- to 25-year-olds).

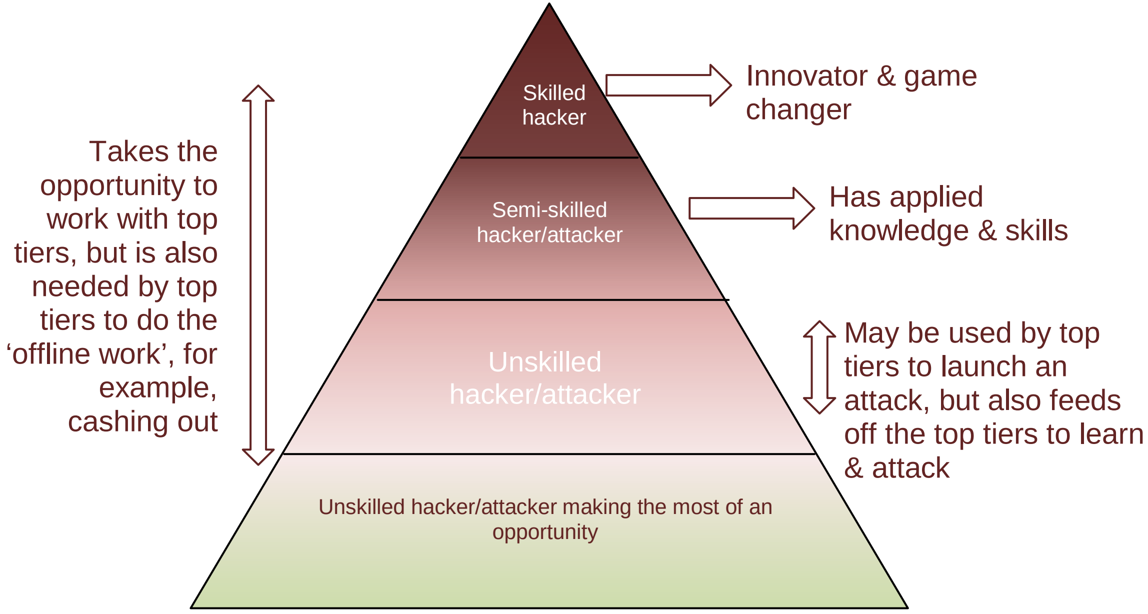
The survey also found that 3 per cent of 10- to 25-year-olds reported visiting a website which gave details on how to commit a crime, while 1 per cent of 18- to 25-year-olds said that they had visited a racist website (this question was not asked to those aged under 18). Similarly, 1 per cent of OCJS internet-users (aged 10 to 25 years) reported sending an email message intended to harass, scare or threaten.

Case-study research has attempted to categorise particular types of cyber offenders. Hackers are often presented on a continuum – at the one-end are 'white-hat' or 'ethical' hackers, infiltrating systems to help to find vulnerabilities and at the other are 'black-hat' hackers or 'crackers', intent on malicious criminal damage. A number of hacker classifications exist, for example, Rodgers (2000) suggests that there are seven subtypes of hackers:

- newbies (who have limited skills and experience, and are reliant on tools developed by others, also known as 'script-kiddies');
- cyberpunks (who deliberately attack and vandalise);
- internals (who are insiders with privileged access and who are often disgruntled employees);
- coders (who have high skill levels);
- old guard hackers (who have no criminal intent and high skill levels, so would most likely equate to white-hat hackers);
- professional criminals; and
- cyberterrorists.

Cyber-dependent offenders have also been categorised in terms of skill level. Holt and Kilger (2012) outline the skills distribution of hackers in terms of a pyramid (see Figure 1.7). A small but elite group of skilled hackers sits at the top of the pyramid – the only group with sufficient knowledge to engage in truly sophisticated attacks on their own. They are responsible for identifying new vulnerabilities and creating the required tools and techniques to undertake cyber attacks. Beneath this group are a larger group of semi-skilled hackers who can use the tools of the high-skilled group but lack the skill and innovation to create their own tools. The lowest and largest group of hackers are the low or unskilled group (which includes 'script-kiddies'). These individuals have little real understanding of the tools and techniques behind cyber attacks, but can still be a nuisance to security professionals.

Figure 1.7: Skills pyramid for the cyber attacker


Skilled hacker
Semi-skilled hacker/attacker
Unskilled hacker/attacker
Unskilled hacker/attacker making the most of an opportunity
Innovator & game changer
Has applied knowledge & skills
May be used by top tiers to launch an attack, but also feeds off the top tiers to learn & attack
Takes the opportunity to work with top tiers, but is also needed by top tiers to do the 'offline work', for example, cashing out

Source: Holt (2013)

In terms of geographic location, Holt (2013, p166) states *"many of these attacks stem from computer hackers living in China, Russia, and Eastern Europe"*. The online marketplaces for selling malware, hacking tools and personal data have generally been found to operate in channels located in Russia and Eastern Europe (Holt, 2013).

Methods

The technical skills and methods central to cyber-dependent crimes such as hacking are comprehensively outlined in other literature. Furnell (2010), for example, describes different tools available to hackers such as *"packet-sniffers"* used to capture network traffic and potentially intercept unencrypted data; and *"vulnerability scanners"*, which are used to test for security holes and identify vulnerabilities. However, cyber-dependent offenders cannot be identified solely through their use of these tools as many of the same tools that can be used to attack a system, can also be used to defend it (Furnell, 2010). Scanning facilities, for example, should be used by security staff to identify vulnerabilities in order to fix them and keep attackers out.

It is not necessary though for offenders to always have in-depth technical skills to commit these crimes. The emergence of sophisticated and automated 'do-it-yourself' malware kits and hacking tools available to purchase in online web forums means that opportunities for complex forms of offending are now opened up to a much wider range of lower-skilled individuals (Holt, 2013; and see Figure 1.7). In the online global marketplace hackers sell a variety of products and services, including: malware kits; spam and phishing services (including bulk email lists); DDoS attacks and web-hosting on compromised servers. The growth of botnet malware means that skilled attackers can now lease out their large attack infrastructure to semi-skilled hackers for a fee. Also available for purchase in online forums are personal data, such as credit card and PIN numbers (Holt, 2013).

Case-study 4

Mixing methods: Blending social engineering with technical sophistication

"A UK university student [pleaded guilty to] a malware-based scam that allowed him to break into the personal computers and webmail accounts of an estimated 100 victims. [He] tricked victims into downloading password-stealing software, called Istealer, which he had disguised as a code-generation key for online games. Istealer is designed to capture the login credentials of webmail and other online accounts (email, Instant Messaging, online gaming) before uploading them to a remote server, where they can be retrieved by a hacker controlling the program."

Leyden (2011) from *The Register*

Cyber-dependent and cyber-enabled 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). An internet user might unknowingly download a virus in an attachment if they are led to believe that the email is from someone they know or a respected organisation. Some malicious files or programs can be made to look similar to known products, tricking users into opening them up. Sometimes offenders may call internet users pretending to be from IT support in order to obtain details of passwords and so on (Furnell, 2010; Rusch, 2002). Offenders may use a variety of hooks or bait to ensure that individuals continue to be deceived, even if they are aware of a particular trick or scam. Some threats have remained active for months using these methods (for example, the storm worm, which appeared in January 1997).

Organised cyber criminals

There is limited published evidence available regarding organised cyber crime. The survey evidence available reveals that approximately 25 per cent of respondents to the 2012 CVS thought that their most recent online 'crime' incidents were committed by an organised group of criminals[16] rather than someone working alone (Home Office, 2013b). However, these reports cannot be independently verified.[17] AV providers have also observed increases in targeted attacks, which they suggest are indicative of increasing levels of organised attacks, attempting to phish users for credentials and push malware, rather than more 'random', non-targeted attacks (Symantec, 2012).

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, extortion, fraud, distribution of illegal materials) and money laundering (for example, using Ebay or online games such as Second Life) (Choo and Smith, 2008). Global organised crime groups such as the Asian triads and the Japanese Yakuza have been linked directly with cyber-enabled crimes such as computer software piracy, and credit card forgery and fraud (Choo and Smith, 2008). Whilst these types of groups may not be working online themselves, evidence

[16] 'Organised criminals' were defined in the CVS as crimes involving individuals, normally working with others, committing serious crime on a continuing basis. This usually includes elements of planning, control and coordination, and benefits those involved.
[17] 2012 CVS (Home Office, 2013a). Four main sectors surveyed were: accommodation and food; transportation and storage; wholesale and retail; and manufacturing.

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, it has also been suggested that 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, 2013). 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). *Case Study Five* outlines further findings from U.S. research in this area.

Case Study 5

Organisational structure of carding forums:

Recent US research by Holt (2013) examined the organisational structure[18] *of a small number of English-speaking and Russian-speaking online carding forums by analysing their conversation threads. Holt found that most sellers appeared to operate as loners or in small teams rather than as sophisticated organisations. They tended to use the online environment to build short-term partnerships when necessary.*

Depending on the products and services, there was also a substantive division of labour between individuals. This involved forum administrators acting as regulators, but also individuals offering particular specialist skills such as drop services (to remove funds from stolen accounts) or particular types of data (e.g. CCVs vs PayPal accounts). In the observed forums, the buying and selling process was peer-driven as individuals influenced each others behaviour by providing feedback about each other (similar to e-bay style feedback). In some respects the online markets therefore seemed relatively formal and organised.

Other research by Holt (2013) has also explored the structure and operations in forums selling malware and other cyber crime services (such as DDoS attacks)

A variety of criminal roles and specialisations can make up these types of online organised groups. For example Moore *et al.*, (2009) point to crime group members who design malware, others who use it perpetrate frauds and the ‘mules’ who launder the profits (amongst others). Chabinsky (2010) identified 10 key specialists who make up typical organised online fraud groups, this includes: malware coders; distributors/vendors trading in stolen data; techies maintaining the site; hackers; fraudsters/social engineers; hosters; cashers; money movers; digital launderers; and personnel.

Cyber offenders have specifically been identified as trading online in personal details (such as passports, driving licenses, credit card details), via online marketplaces and carding forums. Such items can then be used for fraudulent purposes. Holt (2013) explored the costs of personal and financial data sold and bought from different countries on carding markets, using a qualitative analysis of a sample of posts from

[18] Holt examined whether individuals worked as ‘loners, colleagues, peers, teams or as formal organisations’ (in accordance with organisational structure outlined by Best and Luckenbill, 1994).

four web forums. The costs of personal information were found to vary depending on the type of information for sale and the country of origin. US sourced credit card details were typically more expensive than those from other countries, although this varied between forums and sellers.

Holt (2013) suggests research such as this presents opportunities to better understand how online organised groups operating in such forums may be disrupted. For example, by identifying individuals who may hold stolen data and using slander attacks to disrupt the relationships and trust held between buyers and sellers. Some successful operations have already been conducted against these online forums and carding groups. For example, the closure of the ‘Darkmarket’ forum in 2008 – a carding group based in north London which had over 2,500 affiliates (see Glenny, 2011). In a 2010 international operation, the FBI arrested 11 US citizens and passed on information which led to the arrests of 13 further individuals in Canada, India and five other jurisdictions (Federal Bureau of Investigation, 2012). In 2012, the UK Serious Organised Crime Agency (SOCA) and the FBI worked together to take down 36 websites involved in the criminal sale of stolen credit card details and online bank accounts, estimating disruption to organised criminal groups of over £500million (Serious Organised Crime Agency, 2012)

References

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

Alhomoud, A., Awan, I., Disso, J. P., and Younas, M. (2013) ‘Cyber security next generation toolkit against botnets’, *Computer* , 46(4), pp 62-66.

Allen, J., Forrest, S., Levi, M., Roy, H., and Sutton, M. (2005) *Fraud and Technology Crimes: Findings from the 2002/3 British Crime Survey and 2003 Offending, Crime and Justice Survey.* Online Report 34/05. London: Home Office.

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>.

APWG (2012a) *Phishing Activity Trends Report (1st Quarter 2012).* Retrieved September 2013. Available at: <http://www.apwg.org/reports/apwg_trends_report_q1_2012.pdf>.

APWG (2012b) *Phishing Activity Trends Report (2nd Quarter 2012).* Retrieved September 2013. Available at: <http://docs.apwg.org/reports/apwg_trends_report_q2_2012.pdf>.

APWG (2012c) *Phishing Activity Trends Report (3rd Quarter).* Retrieved September 2013. Available at: <http://docs.apwg.org/reports/apwg_trends_report_q3_2012.pdf>.

APWG (2013) *Phishing Activity Trends Report (4th Quarter).* Retrieved September 2013. Available at: <http://docs.apwg.org/reports/apwg_trends_report_q4_2012.pdf>.

Beal, V. (2011) *The difference between a computer virus, worm, and trojan horse.* . Retrieved June 2013. Available at: <http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp>.

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>.

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

Chabinsky, S. (2010) *The Cyber Threat: Who's Doing What to Whom?* Retrieved September 2013. Available at: <http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom>.

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

CISCO. (2013) *CISCO Annual Security Report.* Retrieved September 2013. Available at: <https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf>.

Computer Misuse Act 1990.

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>.

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

Federal Bureau of Investigation. (2012) *Manhattan U.S. Attorney and FBI Assistant Director in Charge Announce Additional Arrests as Part of International Cyber Crime Takedown.* Retrieved August 2013. Available at: <http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-additional-arrests-as-part-of-international-cyber-crime-takedown/>.

Florencio, D., and Herley, C. (2011) ‘Sex, lies and cyber crime surveys’, *Economics of Information Security and Privacy III*, pp 35-53.

Fraud Act 2006.

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

Glenny, M. (2011) *Darkmarket: Cyberthieves, cybercops and you*. UK: Bodley Head.

Holt, T. J. (2013) '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: <www.gov.uk: https://www.gov.uk/government/publications/the-national-crime-recording-standard-ncrs-what-you-need-to-know>.

Home Office (2012) *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 (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.

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

Juniper Networks (2012) *Malicious Mobile Threats Report 2010/2011.* Retrieved June 2013. Available at: < http://www.juniper.net/us/en/local/pdf/whitepapers/2000415-en.pdf>.

Kaspersky (2011) *DDoS Attacks in H2 2011*. Retrieved July 2013. Available at: <http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011>.

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

Leyden, J. (2011) 'UK student hacker sentenced over gaming Trojan', *The Register,* May 18 2011. Retrieved June 2013. Available at: <http://www.theregister.co.uk/2011/05/18/gaming_trojan_conviction/>.

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

McAfee. (2012) *McAfee Threats Report: First Quarter 2012.* Retrieved August 2013. Available at: <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2012.pdf>.

McAfee-NCSA. (2007) *Cyber Security Survey: Newsworthy Analysis* . Retrieved September 2013. Available at: < http://download.mcafee.com/products/manuals/en-us/McAfeeNCSA_Analysis09-25-07.pdf>.

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

Metropolitan Police (2010) 'Computer hacker who posed as student sentenced'. November 25, 2010. Retrieved May 2013. Available at: <http://content.met.police.uk/News/Computer-hacker-who-posed-as-student-sentenced/1260267431754/1257246842383>.

Microsoft (2011a) *Microsoft Security Intelligence Report,* vol. 10. Retrieved August 2013. Available at: <http://www.microsoft.com/en-us/download/details.aspx?id=17030>.

Microsoft (2011b) *Microsoft Security Intelligence Report,* vol. 11, first half 2011. Retrieved September 2013. Available at: <http://www.microsoft.com/en-us/download/details.aspx?id=27605>.

Microsoft (2011c) *Microsoft Security Intelligence Report,* vol. 12, second half 2011. Retrieved September 2013. Available at: <http://www.microsoft.com/en-us/download/details.aspx?id=29569>.

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 (2013) Unpublished data. London: Ministry of Justice.

Moir, R. (2008) *Defining Malware: FAQ.* Microsoft WindowsServer 2003. Retrieved September 2013. Available at: < http://technet.microsoft.com/en-us/library/dd632948.aspx>.

Moore, T., Clayton, R., and Anderson, R. (2009) 'The Economics of Online Crime', *Journal of Economic Perspectives* , 23(3), 3–20.

NCC (2012) *Origin of Hacks, quarter 3.* Retrieved September 2013. Available at: <http://www.nccgroup.com/media/169256/origin_of_hacks_q3_2012.pdf>.

Neustar. (2012) *DDoS Attacks in the United Kingdom. Annual Trends and Impact Survey.* London: Neustar.

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>.

ONS (2003) *Crime Survey for England and Wales* (formerly known as the British Crime Survey, 2002-2003 [computer file]). Data set available at UK Data Service [distributor]. Retrieved September 2013. Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=5059&type=Data%20catalogue>.

ONS (2004) *Crime Survey for England and Wales* (formerly known as the British Crime Survey, 2003-2004 [computer file]). Data set available at UK Data Service [distributor]. Retrieved September 2013. Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=5324&type=Data%20catalogue>.

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 (2011a) *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. (2011b) *Internet Access - Households and individuals 2011.* UK: Office for National Statistics. Retrieved September 2013. Available at: <http://www.ons.gov.uk/ons/dcp171778_227158.pdf>.

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>.

PwC (2013) *2013 Information Security Breaches Survey.* Retrieved September 2013. Available at <http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf>.

Rodgers, M. (2000) *A new hacker taxonomy.* Retrieved July 2013. Available at: <http://homes.cerias.purdue.edu/~mkr/hacker.doc>.

Rusch, J. J. (2002) *The Social Psychology of Computer Viruses and Worms.* Retrieved June 2013. Available at: <http://www.thehackademy.net/madchat/vxdevl/papers/avers/g10-c.pdf>.

Serious Organised Crime Agency (2012) *Web domains seized in international operation to target online fraudsters.* Retrieved September 2013. Available at: <http://www.soca.gov.uk/news/446-web-domains-seized-in-international-operation-to-target-online-fraudsters>

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 (2012) *Security Threat Report 2012.* Retrieved September 2013. Available at: <http://www.sophos.com/en-us/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf>.

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.

Szor, P. (2005) *The art of computer virus research and defense.* Addison-Wesley Professional.

Wilson, D., Patterson, A., Powell, G., and Hembury, R. (2006) *Fraud and technology crimes: Findings from the 2003/04 British Crime Survey, the 2004 Offending, Crime and Justice Survey and administrative sources.* Retrieved September 2013. Available at:

<http://webarchive.nationalarchives.gov.uk/20110220105210/rds.homeoffice.gov.uk/rds/pdfs06/rdsolr0906.pdf>.

wiseGEEK (2013) *What is a jailbroken phone?* Retrieved August 2013. Available at: <http://www.wisegeek.com/what-is-a-jailbroken-phone.htm>.

YouGov (2012) *Social Media Tracker*. Retrieved September 2013. Available at: <http://research.yougov.co.uk/services/social-media-tracker/>.

ISBN: 978-1-78246-245-3