garlik™
powerful stuff

UK Cybercrime report

Author:
Stefan Fafinski
1871 Ltd

Preface

The impact and influence of the Internet over the past ten years has been immense. During that time, access to the Internet has grown enormously. In 1996, 3.4 million UK adults were online; by 2006 this had expanded to 28.5 million. The rise of this networked society has expanded the range of information available to individuals and changed the way in which we relate to one another in the virtual world as well as in the physical world. However, it also has a dark side: the Internet has proven to be an influence on criminal, as well as legitimate, activity.

The potential of the Internet to facilitate crime is increasingly a matter for public concern. This has given rise to a need to understand and measure cybercrime. However, attempting to quantify the amount of cybercrime is not straightforward. In an attempt to shed light on this 'dark figure of cybercrime', Garlik commissioned criminologists from specialist consultancy firm 1871 Ltd to conduct a research project focussing on an estimated quantification of cybercrime.

I.
Defining Cybercrime

Although the term 'cybercrime' is now in everyday use, the first problem encountered in *measuring* cybercrime is that there is no commonly-agreed definition of the term.

Definitions of cybercrime include:

– the use of any computer network for crime (British police)[1]

– any criminal offence committed against or with the help of a computer network (Council of Europe).[2]

These broad definitions offer little insight into the nature of the conduct that falls within the umbrella term. The issue is further complicated by the fact that cybercrime is a social label and not an established term within the criminal law. It seems that a situation has arisen in which everyone knows what cybercrime means but nobody can pinpoint exactly what conduct the term encompasses.

The difficulty in actually defining cybercrime makes measurement of cybercrime problematic. What is it that is actually being counted?

However, this report will focus on the following categories of cybercrime, which predominantly affect individuals:

– Identity theft and identity fraud

– Financial fraud

– Offences against the person

– Computer misuse

– Sexual offences.

The following sections of the report will define and explore each of these categories of cybercrime in more detail.[3]

1 http://news.bbc.co.uk/hi/english/static/in_depth/uk/2001/life_of_crime/cybercrime.stm
2 Definition derived from the provisions of the Council of Europe Convention on Cybercrime (ETS No. 185) 8 November 2001.
3 Fuller discussions of each category can be found in Appendix A to this report.

Identity theft and identity fraud

- Identity theft and identity fraud are not criminal offences in their own right.

- In essence, identity theft is the assumption of the identity of another person, living or dead, irrespective of the motivation underlying this course of action. For example, taking on the identity of a dead person and living life as them, having abandoned one's own identity.

- By contrast, identity fraud is the transient or partial assumption of another' s identity. This involves the fraudster retaining his own identity for most purposes but (mis)using the identity of another for some particular purpose. For example, using another's identity to register a car so that any driving offences are attributed to the victim rather than to the fraudster.

- Identity theft is categorised as a cybercrime within this report (despite not being an offence in itself) on the basis that it is inevitably the first step that is taken towards the commission of a deception (fraudulent use of identity) offence and technology plays such a significant role in the process of locating and acquiring the identity of another.

Financial fraud

- Financial fraud is defined as the use of deception for direct or indirect financial or material gain. Direct financial gain commonly involves the impersonation of the victim (hence the acquisition of his identity – identity theft or identity fraud) in order to obtain money. Indirect financial gain might involve the assumption of identity information that secures the offender access to more lucrative employment opportunities.

- This deception often (but not always) involves a misrepresentation of the identity of the person concerned. For this reason, financial fraud is often viewed as synonymous with identity theft/fraud.

  However, this is a misperception as identity theft/fraud involves the assumption of the identity of another for whatever purpose – this may be financial fraud but need not necessarily be so. For example, a person who assumes the identity of another in order to commit driving offences would fall within the meaning of identity fraud but not financial fraud whereas a person who assumes the identity of another in order to obtain credit in the victim's name would fall within the meaning of both identity fraud and financial fraud.

- This category of conduct was covered by deception offences within the Theft Act 1968 but these were repealed by the Fraud Act 2006 in favour of a new raft of fraud offences. These offences are categorised as cybercrime if they were committed online or involved the use of online resources to facilitate fraud in the physical world.

Offences against the person

– This category of cybercrime involves the use of a computer to cause an individual some form of personal harm such as anxiety, distress or psychological harm.

– It includes abusive or threatening e-mails and the posting of derogatory information online.

– It also includes situations where the offender poses as the victim to engage in offensive behaviour behind the veil of anonymity offered by the Internet.

– It also includes 'hate crimes': the intimidation of a person or group on the basis of their actual or perceived membership of the targeted group; typically defined in terms of religion, political belief, gender, race or sexual orientation. Hate crimes include abuse directed at victims as well as unfair, untrue, unfavourable or otherwise derogatory information disseminated about those viewed as members of the target group.

Computer misuse

This category of cybercrime is reserved for conduct that falls within the Computer Misuse Act 19904 as follows:

– Unauthorised access to a computer system (basic hacking).[5]

– Unauthorised access to a computer system with intent to commit or facilitate the commission of further offences (aggravated hacking).[6]

– Unauthorised modification of computer material (such as that caused by viruses).[7]

Sexual offences

– This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual element[8] including paedophilic activity such as grooming a child for sexual activity which was criminalised by the Sexual Offences Act 2003.[9] The ease of transfer of information offered by the Internet and its largely unregulated nature makes it a useful device for those engaged in these sort of offences.

4 Note that amendments to these offences were made by the Police and Justice Act 2006, although the relevant provisions of that Act are not currently in force.
5 Computer Misuse Act 1990, s.1
6 Computer Misuse Act 1990, s.2
7 Computer Misuse Act 1990, s.3
8 That is, it would be considered by the objective observer to involve sexual wrongdoing irrespective of the subjective views of the parties themselves
9 Meeting a child following sexual grooming, Sexual Offences Act 2003, s.15

II.
Counting Cybercrime

It is not easy to count any sort of crime. Cybercrime is no exception.

In general terms, there is a three-stage process involved in quantifying crime:

– The conduct needs to be observed

– The conduct needs to be categorised as criminal

– The conduct needs to be brought to the attention of the authorities in order to be recorded.

Therefore, if any of these three stages fails, then a particular crime will not be recorded in official statistics. In relation to cybercrimes, there are certain factors which are relevant to each of the stages:

– The criminal conduct may not be noticed. For instance, if an online banking fraud comprises multiple low-value transactions across a bulk body of victims, the victims may not spot the minor discrepancy in their accounts.

– The victim might not know that the observed conduct is criminal. For instance, in relation to virus attacks, there is a general public and industry perception that no-one has broken the law.[10]

– The victim may choose not to report the crime to the authorities.

There are a number of reasons why a cybercrime victim may not report the crime to the authorities:

– A feeling that nothing can be done because it is too late to rectify the harm caused

– A feeling that there is little chance that the police will identify, detain and prosecute the offender:

  • because the Internet offers relative anonymity and an easy way to shield identity

  • the police have limited resources and expertise to tackle cybercrime so may discourage the victim from pursuing a formal complaint as investigation would be too difficult

  • victims report that the police emphasise the futility of making an official report or state (wrongly) that the reported conduct is not a criminal offence in an attempt to dissuade the victim from pursuing the matter

  • if the offence has been committed outside the UK, not only is it likely to be harder to identify the offender, but there would also be complications introduced by the collaboration necessary between the police forces of different nations and by the discrepancies between the laws of the respective jurisdictions[11]

Given these issues, it is hardly surprising that official crime statistics are regarded as representing only the tip of the iceberg of the totality of criminal behaviour and that cybercrime, in particular, is massively under-reported.

10 DTI Information Security Breaches Survey 2004 at www.pwc.com/images/gx/eng/about/svcs/grms/2004Technical_Report.pdf
11 Since something which is a crime in the UK may not be a crime in the nation where it was committed.

III.
Outline research methodoloy

As cybercrime suffers from under-reporting, it follows that in order to appreciate the extent of cybercrime fully, recourse has to be made to sources of information other than official recorded crime statistics.

Although illuminating the dark figure of unrecorded cybercrime is an inherently imprecise activity, this report has drawn on a range of different sources of information in order to extrapolate the relevant information such as Hansard (the official edited verbatim report of proceedings in Parliament) and other official sources, specialist organisations and industry analyses, newspaper archives and the findings from earlier research projects carried out by the principal researchers. A list of sources is provided in Appendix G.

Where possible, statistics were derived from surveys which are based on interviews. For the crime types such surveys cover, this can provide a better reflection of the true extent of crime because it includes crimes that are not reported to the police. The British Crime Survey in particular gives a better indication of trends in crime over time because it is unaffected by changes in levels of reporting to the police, and in police recording practices.

References are therefore made within this report to quantitative research conducted by other organisations and to official statistics. While these are reproduced from authoritative sources, neither Garlik nor 1871 Ltd can take any responsibility for their integrity either in terms of their accuracy or in the method used to gather the data.

IV.
Identity theft and identity fraud

Identity theft is the assumption of the identity of another person, living or dead, irrespective of the motivation underlying this course of action. For example, taking on the identity of a dead person and living life as them, having abandoned one's own identity. By contrast, identity fraud is the transient or partial assumption of another's identity. Sources for this section can be found in Appendix B.

- It is estimated that there were 92,000 cases of online identity fraud during 2006
- Around 40% of all identity frauds are facilitated online
- The top three false or stolen documents used by fraudsters to attempt identity fraud in 2006 were utility bills, passports and bank statements
- Current address fraud (where the victim lives at the same address as the 'current address' given on the fraudulent application) is on the increase (from 25% to 35% of all identity fraud cases).

Commentary

- Although it is anticipated that overall levels of identity theft/fraud will remain relatively stable in 2007, the means of facilitating the identity theft/fraud will change such that an increasing number of offences are committed online.
- The increased level of current address fraud demonstrates that fraudsters are increasingly acquiring a very thorough knowledge of the victim's details. They will therefore supplement basic information with that available online in order to quickly build up a comprehensive portfolio of identity information relating to the victim.
- Therefore, the proportion of identity theft/fraud facilitated online is expected to increase throughout 2007 as a result of the increasing technical sophistication and organisation of fraudsters and the increasing amount of identity information that may be gathered from online sources.
- Possession of a piece of key identity information (such as driving licence or passport) can render the victim more vulnerable to online identity theft/fraud as this gives the fraudster a solid foundation for adding more peripheral personal detail in order to commit more sophisticated identity fraud.

garlik™
powerful stuff

The proportion of identity theft/ fraud facilitated online is expected to increase throughout 2007 as a result of the increasing technical sophistication and organisation of fraudsters and the increasing amount of identity information that may be gathered from online sources.

V.
Financial fraud

Financial fraud is very closely linked to identity theft. An instance of identity theft can give rise to an instance of financial fraud if the stolen identity is misused for financial gain. However, there are also instances where an identity is stolen and not used for financial gain or, more commonly, where an online financial fraud takes place by using card details but not necessarily involving the use of a complete set of identity information. Sources for this section can be found in Appendix C.

– It is estimated that there were 207,000 cases of online financial fraud during 2006 (up 32% from 2005)

– Card-not-present (CNP) fraud is increasing (49% of all losses in 2006; 41% of all losses in 2005). The total value of CNP fraud also rose by 16% from £183.2M to £212.6M. Given a relatively consistent average value of loss, the total number of individual occurrences rose by a similar amount.

– The proportion of CNP fraud taking place online is also increasing (73% of all CNP in 2006; 65% of all CNP in 2005).

– Although police recorded card fraud has fallen by 33% from 2005/06 to 2006/07, this is largely due to the requirement that the financial institutions now act as gatekeepers to police reporting. Following the introduction of the Fraud Act 2006, banks and financial institutions became the first point of contact for card and online fraud offences; it is the decision of the institution and not the account holder, to pass details of the crime to the police. Therefore in straightforward low-value cases, the financial institution will generally make good the financial loss without the involvement of the 'traditional' law enforcement agencies.

Commentary

Although the total value of card fraud has declined overall, the number of card users affected is relatively constant. This suggests that fraudsters are adopting strategies of adaptation and diversification in order to find innovative ways of committing card fraud in response to prevention measures such as chip and PIN.

This is reflected in the increase in CNP fraud.

CNP fraud is attractive to fraudsters since businesses cannot physically check the card; there is no signature or PIN and there is no guarantee that the information provided to authenticate the transaction has been given by the legitimate cardholder.

The numbers of retailers offering online purchasing is increasing. Therefore opportunities for CNP fraud will also increase and it would be unsurprising if the extent of CNP fraud increases while counter-measures are introduced to deal with the problem.

garlik™
powerful stuff

‘Cyber crimes are just as prevalent as traditional crimes. In 2006 the incidents of online financial fraud doubled the number of robberies taking place.’

VI.
Offences against the person

This category of cybercrime involves online harassment: the use of a computer to cause personal harm such as anxiety, distress or psychological harm, including abusive, threatening or hateful e-mails and messages and the posting of derogatory information online. Sources for this section can be found in Appendix D.

– It is estimated that there were 1,944,000 cases of online harassment during 2006.

– In the same period, a total of 218,817 incidents of physical harassment were recorded.

– At least 90% of online harassment goes largely unreported.

Commentary

– The relative anonymity provided by the online environment lends itself to harassment.

– Perpetrators take advantage of the dissociative effect of the Internet to behave in malicious or threatening ways that they would consider unthinkable in the physical world.

– Online harassment can take many forms such as:

  • unsolicited e-mail (often hateful obscene, or threatening)
  • live chat abuse
  • online defamation.

VII.
Computer misuse

This category of cybercrime is reserved for conduct that falls within the Computer Misuse Act 1990. It encompasses both basic and aggravated hacking (where a system is accessed without authorisation with the intent to commit further offences) and the unauthorised modification of computer material, such as might happen as a result of a virus attack. Sources for this section can be found in Appendix E.

– It is estimated that there were 144,500 cases of computer misuse (excluding viruses) during 2006.

– In the same period approximately 6,000,000 virus incidents took place.

– Despite this, prosecution levels are extremely low (around 100).

Commentary

– Despite their criminalisation the threat from computer viruses and hacking remains real.

– Reporting and prosecution levels are extremely low.

  • Corporate victims often rely on internal disciplinary measures rather than bringing a prosecution.

  • There is a general perception that virus writers have not broken the law.

  • Most users view computer security as a private matter (taking their own responsibility for anti-virus software and firewalls) and therefore fail to appreciate that breaches are a matter for the criminal law.

  • There is no prospect of damages or compensation for loss in a criminal prosecution.

  • The prospect of adverse publicity resulting from a security breach often outweighs the benefits of prosecution.

VIII.
Sexual Offences

This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual element. It includes paedophilic activity such as grooming a child for sexual activity. Sources for this section can be found in Appendix F.

– It is estimated that there were 850,000 cases of unwanted online sexual approaches, primarily messages of a sexual nature within Internet chat rooms, during 2006.

– During the same period 238 offences of meeting a child following sexual grooming were recorded.

Commentary

– Although the number of unwanted sexual approaches is high, it does not necessarily follow that all sexual approaches are a precursor to grooming the recipient for a (physical) meeting or physical sexual activity.

– As with online harassment, perpetrators take advantage of the dissociative effect of the Internet to behave in ways that they would consider unthinkable in the physical world.

– The veil of anonymity offered by the Internet does however enable perpetrators to masquerade as children, often gaining the confidence of their victims over a period of time before introducing a sexual element into the online interaction.

IX.
Conclusions and wider social implications

It is clear that cybercrime is a pressing and prevalent social problem. As access to the Internet has grown then the opportunities for the commission of cyber-crimes have increased. As more individuals access the Internet, the cyber criminal has a broader range of potential victims within reach. Moreover, the increased availability of personal information online provides the identity thief with a useful portfolio of identity information as a 'starter kit' for the misuse of that identity. That is not to say that the Internet has spawned a whole new set of crimes. For instance, 'identity theft' is not a criminal offence in itself, but could give rise to liability under the Fraud Act 2006, the Theft Act 1968 and the Computer Misuse Act 1990.

The Internet has, however, made the commission of what might be termed 'traditional' crimes easier – or more widespread. A further example relates to child pornography. Distribution of child pornography is a criminal offence which was relatively well-contained prior to the Internet: it is now a widespread social harm.

Moreover, the nature of the Internet, and its relative anonymity enables individuals to behave in ways that they would consider to be unthinkable in the physical world. It has been suggested that the moral boundaries relating to technology are at odds with the moral standards of the physical world. In essence, the lack of tangibility in the technological realm suggests that the ethical considerations relating to personal property and privacy in the physical world do not apply in the electronic world. This allows people to engage in deviant behaviour involving computer misuse whereas they would be less likely to engage in the analogous physical world mischief.

Moreover, computer misusers tend not to consider their actions as immoral. This lack of virtual moral consensus has been referred to as 'toxic disinhibition': arising from the very nature of the interaction of the individual with the technology. Individuals are led into a relationship with technology within which conventional moral rules and norms do not apply.

garlik™
powerful stuff

The nature of the Internet, and its relative anonymity enables individuals to behave in ways that they would consider to be unthinkable in the physical world.

Computer technology has become more widespread. Thirty years ago, computers were still largely in the realm of the 'expert' – used in specialist scientific and technical applications or as expert systems within large corporations. It follows that the computer users were also generally highly skilled and knowledgeable about the technology environment.

However, the commoditisation of technology and the efforts put in to accessibility and ease of use have led to the situation where many individuals are perfectly competent in using their systems for whatever purpose they require, but lack the detailed knowledge to understand the potential threat to them as individuals. This collective diminution in general computing skill levels gave rise to a knowledge gap between the expert and non-expert user. The exploitation of this knowledge gap is a potential driver of cybercrime.

Of course, technology is able to include safeguards as well as introduce vulnerabilities. However, there is generally a low level of understanding of both the threats posed to users by the Internet as well as the tools that are available to end-users for protection from those threats. This is supported by the House of Lords Science and Technology Committee who consider that the 'dangers of the Internet are poorly appreciated by the general public'.

This lack of appreciation of the Internet's dangers is coupled with a number of factors which hinder the reporting and investigation of cybercrime. Firstly, there is often a misconception that the behaviour which has been experienced is not criminal. Therefore, not only is there some public ignorance of the dangers, there is also public misconception about what manifestations of online activity could be potentially criminal. This is also a product of the relative unfamiliarity of the Internet: most people readily understand that burglary is a crime, but may not appreciate that, for example, computer viruses also give rise to criminal liability.

Moreover there is a commonly held belief that the police will be unable or unwilling to investigate cybercrime. This perception has not been helped by the subsuming of the UK's National High Tech Crime Unit (NHTCU) which had the sole job of investigating crimes relating to Internet security into the Serious Organised Crime Agency (SOCA) which has a much broader remit of tacking organised crime, not just that committed or facilitated by the Internet. Bodies such as the Society for Computers and Law fear that the expertise formerly concentrated within the NHTCU will become diluted as SOCA's emphasis on organised crime takes precedence. The NHTCU also provided useful public information on cybercrime issues.

Furthermore, the changes introduced as a result of the Fraud Act 2006, mean that from 1 April 2007, victims of bank fraud must notify the financial institution directly rather than the police. The institution will then decide whether to report the details on to the police. There is criticism that this reporting regime will give financial institutions too much discretion over what types of fraud are reported and investigated by the police. Since it is unlikely that banks will report low value card fraud to the police, this is likely to result in a decrease in reported crime figures even though the scale of the problem may increase in terms of the absolute number of instances of fraud occurring. Indeed, the Commissioner of the City of London Police has stated that 'fraud is in danger of becoming the forgotten crime of British policing'.

Finally, there is also the issue of jurisdiction which is also a confounding factor upon the police. While the rise in international terrorism has provided more legislative means of expediting and facilitating international law enforcement, such as the European arrest warrant system under the Extradition Act 2003, it remains the case that this is not widely used in practice. In 2005, there were 6,900 warrants across Europe of which 1,770 resulted in an arrest.

Therefore, given the global nature of the Internet and the fact that over 95% of malicious activity originates outside the UK, it follows that the international nature of computer misuse renders the use of the criminal law cumbersome and unattractive as a means of control. The exception here is that extra-territorial criminal law will only tend to be employed where there is a threat to national security.

There is also no consistent mechanism for reporting or measuring cybercrime, nor a commonly-agreed set of definitions as to what constitutes cybercrime. This is again recognised by the House of Lords who criticise the Government for failing in their responsibility 'to show leadership in pulling together the data that are available, interpreting them for the public and setting them in context, balancing risks and benefits. Instead of doing this, the Government have not even agreed definitions of key concepts such as "e-crime"'.

In relation to identity fraud, this view is echoed by the Home Office who admit that there is 'no comprehensive measure of the extent of identity fraud since different sources measure it in different ways'. Official crime statistics subsume cybercrimes into more 'familiar' categories. This is partly due to the reluctance of the Crown Prosecution Service to pursue criminal charges where the only basis for liability falls within the Computer Misuse Act 1990 or the Data Protection Act 1998 and partly that where charges are brought under those Acts, other 'traditional' offences will be charged at the sametime.

The range of sources that this report has considered as a means of estimating the prevalence of cyber-crime has demonstrated that the sources of data are fragmented and inconsistent. While there is no co-ordinated approach to data collection relating to cybercrime it will be difficult to assess the true extent of the problem and the most effective means of its control. While there is a key role for the greater education of users about the threats posed by the Internet, there is also a danger that consumers will not always understand the threats or possess the technical competence to implement technology based protection in response to those problems.

There may also be a role for ISPs to play in the protection of individuals by taking measures to include personal security measures within the services that they provide.

Therefore, the problems inherent in measuring cybercrime could be addressed, at least in part, by increasing individual awareness of the nature of cybercrime so that more reporting takes place. This must be supplemented by clear and consistent reporting mechanisms with a commonly agreed definition of what constitutes a cybercrime.

These reporting mechanisms do not necessarily have to be involve the police as the first port of call – for example, the way that financial institutions now act as gatekeepers to reporting card fraud. However, it is crucial that even where private or industry bodies have devolved responsibility for recording instances of cybercrime, they are doing it in such a way that their individuals statistics can be rolled up to provide a national indicator of the problem: the total number of recorded cybercrimes as distinct from the total number of police recorded cybercrimes (which will be lower, since not all 'privately' recorded cybercrimes will attract the attention of the police).

Moreover, where a 'traditional' offence is recorded it should be 'tagged' in some way where the offence has been facilitated online even if any associated technology offence is not charged. This will give an insight into the proportion of online crime.

The first basis for dealing with any problem is to gain as thorough an understanding of the problem as possible. The recommendations of the House of Lords in relation to co-ordinated data collection and standardisation of definitions are to be welcomed. However, these recommendations may present practical difficulties in relation to both definition and reporting. A greater Government focus on reliability of data and public education and protection is essential. This will require co-operation from private data collection institutions such as the banks to ensure consistency and transparency in reporting.

Appendix A – Definitions

Identity theft and identity fraud

Identity theft and identity fraud are not offences in their own right. They are terms that have passed into common parlance to describe the appropriation of some or all of another's identity information, generally with the aim of using the victim's identity as a mask for their own wrongdoing or to evade responsibility for some action or event although there are situations in which another's identity is assumed for innocuous, or at least non-criminal, reasons.

In essence, identity theft is the assumption of another's identity irrespective of the motivation for which this course of action is undertaken. It is categorised as a cybercrime despite not being an offence per se on the basis that it is frequently the first step that is taken towards the commission of an offence.

This first step may be taken because with chosen offence cannot be committed without impersonation of the victim, i.e. financial fraud in which the offender passes himself off as the victim, or because the offender is using the victim's identity to shield himself from the consequences of his criminal behaviour, i.e. he commits an offence whilst posing as the victim. Irrespective of which of these motivations is operative, the initial first step – the assumption of another's identity – is integral to the commission of the criminal offence that is planned hence the inclusion of identity theft/fraud as a cybercrime is justified as it is a way of facilitating the commission of an offence.

Financial fraud

This category of offences can be defined as the use of deception for direct or indirect financial or material gain. The deception often involves a misrepresentation of the identity of the person concerned, i.e. the offender impersonates the victim in order to gain access to things to which the victim is entitled or to incur financial liability in the victim's name.

Direct financial gain commonly involves the impersonation of the victim in order to obtain his money, obtain credit in his name or abuse credit facilities that have been granted to him whereas indirect financial gain might involve the assumption of identity information that secures the offender access to more lucrative employment opportunities.

This category of conduct was covered by the deception offences enshrined in the Theft Act 1968 but these were repealed by the Fraud Act 2006 in favour of a new raft of fraud offences. The categorisation of these offences as a cybercrime rests on either the commission of the offences online, i.e. an online loan application or online shopping, or the use of online resources to facilitate fraud in the physical realm, i.e. the acquisition of identity information to make the impersonation of the victim possible and convincing or the creation of a sham online website that purports to offer goods for sale.

Offences against the person

The common theme to this category of offences is that the computer is used as a means by which an individual is caused some form of personal harm. Obviously, the remote nature of computer communications precludes any possibility of direct physical harm but there is potential to cause anxiety, distress and psychological harm by indirect means. This may include adverse communications aimed at the victim, i.e. abusive or threatening emails, or it may involve communications with a third party – either targeted individuals or the world at large – that are intended to disseminate derogatory or unfavourable information about the victim, i.e. false accusations are posted on a website. Alternatively, the offender may use the anonymity offered by the Internet to engage in offensive behaviour whilst posing as the victim thus incurring the wrath of others that will spill into the victim's physical world. The opportunity offered by the Internet to distance oneself from one's words is seem by some as an invitation to bully, harass and threaten others with impunity as one's true identity is shielded. This type of behaviour could give rise to liability for harassment, blackmail, common assault or defamation.

This umbrella category of offences also includes 'hate crimes': the intimidation of a person or group on the basis of their actual or perceived membership of the targeted group. This commonly involves groups associated with particular religious or political beliefs as well as those concerned with sex, race or sexual orientation. It would include abuse directed at victims as well as unfair, untrue, unfavourable or otherwise derogatory information disseminated about those viewed as members of the target group.

Computer misuse

This category of offences is reserved for conduct that falls within the parameters of the Computer Misuse Act 1990 and covers situations such as hacking, the spread of computer viruses, and unauthorised access with ulterior intent.

Sexual offences

This category covers a range of conduct that has an objectively ascertainable sexual element, i.e. it would be considered by the objective observer to involve sexual wrongdoing irrespective of the subjective views of the parties themselves. This covers paedophilic activity such as grooming a child for sexual activity which was criminalised by the Sexual Offences Act 2003. The ease of transfer of information offered by the Internet and its largely unregulated nature makes it a useful device for those engaged in these sort of offences.

Appendix B – Identity theft and identity fraud

According to CIFAS,[12] the UK's fraud prevention service,[13] the 2006 figures relating to fraud break down as follows:

Identity fraud14	80,377
Application fraud[15]	63,860
Impersonation[16]	67,406
Total	**211,643**

This represents an increase from 2005 of 16.7%.[17] The top three false or stolen documents used by fraudsters to attempt identity fraud in 2006 were utility bills, passports and bank statements. It is noteworthy that 1% of all passports and 2% of all driving licences were lost or stolen in the year.[18]

In the same period, according to the British Crime Survey[19] around 250,000 adults[20] had their identity misused for credit card applications, mobile telephone applications, benefit fraud or in order to open a bank/building society account.[21] This is not inconsistent with the figures from CIFAS.

Not all this fraud is facilitated online. 28% of victims identified the root cause of their victimisation as theft of physical documents/identity details or mail.[22] This leaves 72% of victims potentially suffering from online victimisation. Based on interviews with both convicted and unconvicted fraudsters it is estimated that around 40% of identity frauds are facilitated online.[23]

Given this it is estimated that there were approximately 92,000 cases of online identity fraud in 2006. [24]

According to CIFAS[25] Current Address Identity fraud[26] represents 35% of identity fraud cases in 2007 (from 25% in the same period of 2006).

12 CIFAS '2006 Fraud Trends' at www.cifas.org.uk/default.asp?edit_id=624-57
13 Credit Industry Fraud Avoidance Scheme
14 Includes cases of false identity, identity theft, account takeover
15 Applications with material falsehoods
16 Fraudulent operation of victim's account or facility as the offender's own; asset conversion
17 2005 total figure 181,357. See CIFAS '2006 Fraud Trends' at www.cifas.org.uk/default.asp?edit_id=624-57
18 British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)
19 BCS respondents were asked whether they had experienced having their personal detailsused in any of the following activities: to apply for and obtain a credit card, to open a bank or building society account, use credit or debit card to make a purchase, to obtain a loan, mortgage or credit agreement, to apply for state benefits, to apply for a drivers' licence, to register a vehicle, to apply for a passport, or to apply for a mobile phone contract.
20 British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)
21 There is some overlap here with financial fraud: since identity theft is commonly used to facilitate financial fraud a single criminal course of action can lead to an instance of both identity theft and financial fraud.
22 CIFAS 'Identity Fraud – What about the victim?' (March 2006) www.cifas.org.uk/default.asp?edit_id=577-73
23 1871 Ltd (2003-6) based on interviews with 117 convicted and unconvicted fraudsters
24 Using a midpoint between CIFAS and BCS figures for the total figure and 1871 Ltd data for the proportion of online activity
25 CIFAS 'Worrying Fraud Trends - the rise continues' at www.cifas.org.uk/default.asp?edit_id=715-57
26 Current Address Fraud is a type of identity fraud where the victim lives at the same address as the 'current address' given on the fraudulent application. The fraudster is often resident at the same property as the victim. In such cases, the fraudster applies for, and uses, products in the name of the victim whose property they share. The fraudster will generally have access to, or can intercept, the victim's post (e.g. in flats where individuals share a communal mailbox with shared access). Other contributory factors to current address fraud can include abuse of Companies House data, data breaches, fraudulent mailredirections and bin raiding.

Appendix C – Financial fraud

In 2006, in relation to all crime

- 83% of adults used a plastic card (35.15 million)[27] 4% of card users had been a victim of card fraud (1.41 million)
- Approximately 1% of the adult population (351,500 adults) had at least one of their plastic cards used without permission
- There were only 87,860 police recorded incidents of cheque and credit card fraud[28] – therefore only 6.5% of card fraud victims were recorded by the police.
- The average loss was £740.[29]

The Fraud Act 2006, introduced in January 2007, altered the definition, coverage and some counting rules for fraud offences. From 1 April 2007, following an annual upgrade to systems, new offences were recorded under the most appropriate specific classification. In addition, from 1 April 2007, there was a change in reporting procedures so that an account holder who suspects fraud on their account is required to report the matter to their financial institution, who will then determine whether to report the crime to the police.

The new system was introduced to reduce considerable bureaucracy surrounding the reporting of fraud, where a report of crime made by a member of the public would also then normally require the police to contact the financial institution to determine whether a fraud had actually occurred. This accounts for the corresponding drop in police recorded card fraud of 33% from 2005/06 to 2006/07 of 33% (from 87,860 to 59,035).[30]

The number of card users who had been an actual victim of credit or debit card fraud[31] were relatively constant from the previous year. This suggests that the scale of the problem is static and that fraudsters are adopting strategies of adaptation and diversification in order to find innovative ways to commit card fraud in response to prevention measures.

In 2006, card-not-present fraud accounted for 49% of all card fraud losses in the UK – an increase of 16% on 2005.[32] Internet fraud on cards is part of the card-not-present fraud total of £212.6 million. In 2006 the amount of card-not-present fraud that took place over the Internet is estimated at £154.5 million – 73% of total card-not-present fraud losses. This figure has gone up by 32% from 2005, when the Internet losses were £117.0 million and accounted for 65% of card-not-present fraud losses.[33]

On this basis, there were an estimated 207,000 cases of online financial fraud in 2006.[34]

27 UK adult population 2006 (aged 16-84) 42,344,600 (National Statistics at www.statistics.gov.uk/populationestimates/svg_pyramid/ew/index.html
28 Home Office Statistical Bulletin Crime in England and Wales 2005/06
29 Averaging figures from Fraud Advisory Panel; Get Safe Online (£875) and APACS (£608)
30 Home Office Statistical Bulletin Crime in England and Wales 2006/07
31 Defined as having a credit or debit card (or cards) or card details used to buy goods or withdraw cash without the cardholder's permission
32 APACS (1.127M fraudulent CNP transactions out of a total 2.260M UK fraudulent transactions) a www.apacs.org.uk/media_centre/press/07_14_03.html
33 APACS 'Fraud: The Facts 2007' at www.apacs.org.uk/resources_publications/documents/FraudtheFacts2007.pdf
34 Extrapolating total number of CNP internet cases from total sum and average losses (£154.5M/£740)

Appendix D
Offences against the person

– 57% of adults[35] personally use the Internet[36] (24.13 million)[37]
– 8% of adults using the Internet were victims of online (e-mail) harassment[38] (1.93 million)[39]

It is estimated that around 0.75%[40] of adults were victims of racially or religiously aggravated online harassment (14,475)

On this basis, there were an estimated **1,944,000** cases of online harassment in 2006.

Comparators

Over the same period there were 218,817 recorded incidents[41] of harassment: only 11.2% of the figure reported by adults suffering harassment online. This suggests that online harassment goes largely unreported or, even if reported, is unrecorded by the police. For 2006/07 there were 228,842 recorded incidents of harassment (an increase of 4.6%).[42]

35 Over 16s
36 British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)
37 UK adult population 2006 (aged 16-84) 42,344,600 (National Statistics at www.statistics.gov.uk/populationestimates/svg_pyramid/ew/index.html
38 Receipt of an e-mail which was considered by the recipient to amount to a course of harassment or to be personally offensive
39 British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)
40 Derived from the relative proportions of all racially-aggravated harassment incidents to all harassment incidents
41 Home Office Statistical Bulletin (Crime in England and Wales 2005/06)
42 Home Office Statistical Bulletin (Crime in England and Wales 2006/07)

Appendix E – Computer misuse

– 52% of UK businesses had a malicious security incident[43] (850,000 businesses)[44]
– 21% involved staff misuse (178,000 incidents)
17% involved unauthorised access by an outsider (144,500 incidents)
– Of the staff misuse, 4% involved unauthorised access to another's data (7,000 incidents)
– 3% were impersonated online (93% of these were financial services businesses) (25,000 incidents)
12% suffered significant attempts to break into their network
– 2% suffered actual penetration into the network (17,000 incidents)

Therefore, it can be estimated that there were **144,500 hacking offences** committed in 2006.

A virus which modifies the content of a computer without authorisation also falls within the definition of cybercrime.[45] Given that around 25% of users report having suffered a virus in 2006 – this equates to approximately **6,030,000 incidents.**[46]

Computer misuse is categorised under the same 'Other frauds' heading for police recorded crime as the much more commonly recorded offence of making off without payment.[47] 128,182 reported crimes fell into this category in 2005/06 and 127,949 in 2006/07.

There are, however, only around 20 prosecutions per year under the Computer Misuse Act 1990.[48] This suggests that the proportion of this 128,000 reported crimes which relate to computer misuse is very small indeed. Many incidents which relate to computer misuse are often recorded under 'traditional' offences since these are more readily familiar to the typical police officer.

When considering hacking and viruses together, it is estimated that there were **6,174,000** cases of computer misuse in 2006.

However, the inclusion of the virus data distorts this figure. Therefore it is estimated that there were **144,500 cases** of computer misuse (excluding viruses) in 2006.

Comparators

Over the same period, approximately 337,000 burglaries from non-dwellings were recorded.[49]

43 DTI Information Breaches Security Survey 2006
44 Assuming 1.64 million businesses in the UK (from VAT registered businesses – National Statistics)
45 Computer Misuse Act 1990, s.3
46 20% of the 57% of adults who personally use the internet (24.13 million)
47 Theft Act 1978, s.3
48 From House of Commons Official Report Written Answers 'Computer Misuse Act Prosecutions' 26 March 2002, c.WA35 and House of Commons Official Report Written Answers 'Computer Misuse Act: Prosecutions' 7 January 2003 in Akdeniz, Y 'CyberCrime' in Stokes, S and Carolina, R (eds.) (2003) E-Commerce Law and Regulation Encyclopedia, London: Sweet & Maxwell, 15-18 (revised April 2005)
49 Home Office Statistical Bulletin (Crime in England and Wales 2005/06) – 344,551; Home Office Statistical Bulletin (Crime in England and Wales 2006/07) – 329,759

garlik™
powerful stuff

Appendix F – Sexual offences

Although there were 62,080 recorded sexual offences in 2005/06[50] and 57,542 in 2006/07,[51] it is self-evident that many of these cannot be committed online since they require physical sexual contact between perpetrator and victim.

The most relevant sexual offence in terms of online behaviour is that of 'meeting a child following sexual grooming'[52] which is defined as intentionally meeting[53] a person under 16,[54] having met or communicated on at least two earlier occasions, with the intention to commit a 'relevant offence'.[55]

The extent of children being targeted online for sexual purposes is difficult to evaluate. However, there have been some surveys of children's experience online. A draft report from the Internet Crime Forum reports that 20% of Internet children using chatrooms have been approached by paedophiles and other undesirables while online.[56]

Approximately 80% of adults with children between five and 15 stated that at least one child in the household had accessed the Internet at some time.[57] 95% of young adults between 16 and 24 access the Internet.[58] It is therefore reasonable to assume, as a conservative estimate, that 60% of children between five and 15 access the Internet.

Given a population of 7,137,700 children between five and 15[59] it follows that 4,282,000 access the Internet and that there were therefore an estimated 850,000 cases of unwanted sexual approaches in 2006.

Comparators

For 2005/06 only 238 offences of sexual grooming were recorded.[60] For 2006/07 the recorded figure was 322.[61]

50 Home Office Statistical Bulletin (Crime in England and Wales 2005/06)
51 Home Office Statistical Bulletin (Crime in England and Wales 2005/07)
52 Sexual Offences Act 2003, s.15
53 Or travelling with intention to meet
54 Without reasonable belief that the person is 16 or over
55 Broadly speaking, a range of child sex offences
56 The 2001 Internet Crime Forum (ICF) report revealed that one in five of the 4.8 million children online in the UK have been approached by paedophiles in Internet chatrooms (see http://news.zdnet.co.uk/itmanagement/0,1000000308,2085206,00.htm)
57 British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)
58 British Crime Survey additional report: Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2 to Crime in England and Wales 2005/06) (15 May 2007)
59 UK population 2006 (aged 5-15) 7,137,700 (National Statistics at www.statistics.gov.uk/populationestimates/svg_pyramid/ew/index.html
60 Home Office Statistical Bulletin (Crime in England and Wales 2005/07)
61 Home Office Statistical Bulletin (Crime in England and Wales 2006/07)

garlik™
powerful stuff

Appendix G – References

APACS (2006) 'Fraud: The Facts 2006'
APACS (2007) 'Fraud: The Facts 2007'
APACS (2007) 'Press release: card fraud losses continue to fall'
CIFAS (2006) 'Identity Fraud – What about the victim?'
CIFAS (2007) '2006 Fraud Trends'
CIFAS (2007) 'Worrying Fraud Trends - the rise continues'
Denning, D (1998) Information Warfare and Security Reading, Pennsylvania: Addison-Wesley.
Flatley, J (ed.) (2007) 'Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey' Home Office Statistical Bulletin 10/07 (Supplementary Volume 2 to Crime in England and Wales 2005/06)
House of Commons Official Report Written Answers 'Computer Misuse Act Prosecutions' 26 March 2002, c.WA35 and House of Commons Official Report Written Answers 'Computer Misuse Act: Prosecutions' 7 January 2003 in Akdeniz, Y 'CyberCrime' in Stokes, S and Carolina, R (eds.) (2003) E-Commerce Law and Regulation Encyclopedia, London: Sweet & Maxwell, 15-18 (revised April 2005)
House of Lords Science and Technology Committee (2007) 'Personal Internet Security'HL 165-I
House of Lords Science and Technology Committee (2007) 'Personal Internet Security: Evidence' HL 165-II
Internet Crime Forum (2001) Report on paedophile activity in Internet chat-rooms.
Lovbakke, J, Taylor, P and Budd, S (2007) 'Crime in England and Wales: Quarterly Update to December 2006' Home Office Statistical Bulletin
McAfee (2006) 'McAfee Virtual Criminology Report: Organised Crime and the Internet'
National Statistics (2006) 'Crime in England and Wales 2005-6: A summary of the main statistics'
Nicholas, S, Kershaw, C and Walker, A (2007) 'Crime in England and Wales 2005/06' (2nd edition) Home Office Statistical Bulletin
Parliamentary Office of Science and Technology (2006) 'Postnote: Computer crime'
Price Waterhouse Coopers (2007) 'DTI Information Security Breaches Survey 2006: Technical Report'
Registrars General for England and Wales, Northern Ireland and Scotland (2006) 'Disclosure of death registration information: Consultation paper'
Report from the Commission on the implementation since 2005 of the Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States COM(2007) 407 (Brussels, 11 July 2007)
Rogers, MK, Siegfried, K and Tidke, K 'Self-reported computer criminal behavior: A psychological analysis' [2006] Digital Investigation 116
Spafford, E (1997) 'Are hacker break-ins ethical?' in Ermann, M, Williams, M & Shauf, M. (eds) (1997) Computers, ethics, and society New York, New York: Oxford University Press 77
Suler, J The Psychology of Cyberspace http://www.rider.edu/~suler/psycyber/psycyber.html>
Symantec (2007) 'Symantec Internet Security Threat Report: Trends for July-December 06'
Walker, A, Kershaw, C and Nicholas, S (2006) 'Crime in England and Wales 2005/06' Home Office Statistical Bulletin 12/06
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' Home Office Online Report 09/06