Home Office

The future of netcrime now: Part 2 – responses

Sheridan Morris

Home Office Online Report 63/04

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

The future of netcrime now:

Part 2 – responses

Sheridan Morris

Online Report 63/04

Foreword

This report describes the findings from research which asked a panel of experts to suggest responses to a number of criminal threats and technology challenges associated with the Internet and information technology applications in two to five years time. Their suggestions were comprehensive and diverse, encompassing technical, legal, commercial and psychological factors.

The report discusses possible responses to these threats and challenges, drawing upon both the Home Office Police Science and Technology Strategy framework and a revised situational crime prevention model (Newman and Clarke, 2003). The aim is to facilitate consideration and uptake of the research findings by policy, enforcement and research parties, through the adoption of these existing and established frameworks.

The findings conclude that there is no single solution to mitigating such threats, though a number of recommendations are proposed for Government, law enforcement, the information communication industry and individual users; unsurprising all have a role to play in securing both their own transactions and the online experience of others. More broadly, the challenges of netcrime are not transitory, waiting to be 'solved' with the emergence of yet more new technology; they are a permanent, ongoing task, which the report aims to contribute to.

Dr Lawrence Singer
Series Editor
Research, Development and Statistics Directorate
Home Office
December 2004

Acknowledgements

I would like to thank all those who gave freely of their time as participating members of the Delphi panel. Those who were happy to be cited as panel members are listed in the Appendix. Dave Mann and Andrew Silke are also thanked for their time and contributions as members of the project co-ordination committee. Thanks also must be given to the project board members who contributed to the aims and the direction of the project; they were John Crow, Clive Harfield, David Ware, Vina Kapil and Tim Wright. Special thanks are also given to Paul Ekblom who provided valuable comments on earlier drafts of the report. I am especially indebted to Kathryn Hyde-Bales, who undertook the enormous task of administering all elements of the survey, including data collection and panel correspondence.

The author

Sheridan Morris is a Senior Research Officer in the Home Office Crime and Policing Group.

The Crime and Policing Group would like to thank Dr Steven Furnell of the University of Plymouth for acting as independent assessor for this report.

Contents

Tables

Figures

Executive summary

This report describes the results of research seeking to identify emerging criminal and malicious behaviour threats relating to the misuse of computers and the Internet, and is a companion report to *The future of netcrime now: Part 1 – threats and challenges* (Morris, 2004). The research formed part of the Home Office Crime and Policing Group's Organised and Hi-Tech Crime Research programme.

The subject of information and communication technology (ICT) related crime and abuse is increasingly topical, both in the media and government. This research coincides with the publishing of e-crime and information assurance initiatives by the Home Office (to which it has contributed) and the Central Sponsor for Information Assurance. In looking to the future, other relevant programmes include the Department for Trade and Industry's (DTI's) Cyber trust and Crime Prevention Project, which is part of the ongoing Foresight futures research programme. The intention of undertaking this research was to play a part in the strategic development of UK information assurance, through its contribution to informing the Home Office e-crime strategy, and to inform policy makers and practitioners, pulling together diverse information assurance measures into a single, if summary, document.

Definitions

This paper has adopted the term netcrime (Mann and Sutton, 1998), defined here as 'criminal or otherwise malicious activity utilising or directed towards the Internet and/or information technology applications'. This definition extends beyond desktop or laptop computers, embracing all forms of networked device (e.g. hand-held computers of various forms and networked domestic appliances). It is also assumed that most criminal activity will involve such devices being connected to a Local or Wide Area Network, the Internet or a public telecommunications network.

Method

The research involved the creation of a 'Delphi' panel of experts. There are various forms of Delphi panel, but the distinguishing characteristics are the use of structured questioning (e.g. questionnaires) to elicit the judgements of a panel of individuals, identified as experts in their field, on a given topic. As here, the exercise is conducted anonymously so as to encourage individuals to express their opinions, without reservation, alongside their peers. There was a broad range of government, law enforcement and regulatory representation on the panel, joined by experts from industry, academia and the voluntary sector, all of whom brought both a technical and non-technical expertise to the deliberations. Through the use of electronic questions, the members of the panel, whose identities were unknown to each other, were asked nine broad questions, clustered around three themes. First, they were asked to look at criminal threats, identifying what areas of Internet and information technology application they considered would be the possible focus of criminal activity in two to five year's time. Second, a similar set of questions was asked in relation to technology-based challenges which have the potential to be misused by criminals and represent a challenge to law enforcement and/or legitimate users. Through two rounds of questionnaires panel members were able to put forward their views on the questions as well as commenting and rating the comments of the rest of the panel. Thus there was an element of peer review, as well as a ranking of the threats and challenges identified by the panel. The results from the forty-eight experts who contributed to the primary Round 1 questionnaire identified 101 criminal threats and 137 technology challenges for comment and ranking by the panel. Both these areas are discussed in the companion to this report (Morris, 2004). The final part of the survey examined the responses to these threats and challenges from the perspective of UK law enforcement agencies, the UK government and the information and communication technology industries and information technology (IT) users. It is these responses that are the focus of this report.

Twenty-eight out of the 48 (58%) original participants completed the fourth questionnaire, rating and providing additional comments on the 187 proposed netcrime responses. The responses were discussed in one of two frameworks depending upon their perceived relevance to law enforcement issues or broader crime prevention measures. More immediate law enforcement-related measures were incorporated into the Police Science and Technology Strategy that draws upon the Police Performance Assessment Framework. Although this strategy was drawn up to encompass all aspects of policing, not specifically netcrime, it nevertheless, provides a useful, existing frame of reference in which to discuss research panel responses regarding police responses to netcrime. By adopting this framework it was hoped to facilitate the consideration and uptake of the research findings by policy, enforcement and research stakeholders currently engaged in examining current and future technology applications as part of the Police Science and Technology Strategy. Although the framework has a component specifically focused on 'investigating hi-tech crime', it was the author's assertion that an understanding and basic competence in handling netcrime should be placed at the centre of policing to mirror the increasing presence of computing and communication technology in everyday society and hence actual and potential criminal behaviour. For these reasons, the survey responses were discussed under a number of broader policing domains and capabilities. The situational crime prevention framework used the 16 techniques as revised by Newman and Clarke (2003) to discuss criminal threats to e-commerce. This framework is composed of 16 techniques covering four broad objectives: to increase the perceived effort for offenders; to increase the risk to offenders; to reduce the anticipated reward to offenders ; and to removing excuses.

Recommendations

Thirty specific recommendations are made, summarised in Figure 4.1 in the main body of the report. Each recommendation is positioned in regard to its emphasis on the four situational crime prevention categories. Starting with prevention measures, tackling much netcrime involves established concepts: build it secure; educate users to operate it secure; and where appropriate, encourage high risk users to invest in matching preventive measures. This simple message has been applied to many offline crime phenomena with good effect (e.g. vehicle crime). Moving from the target to the offender, measures to remove or restrict the resources at their disposal can be taken. Both sets of intervention will help increase the effort required by the criminals in going about much of their offending.

A large number of law enforcement-oriented measures may be considered to impact both on the effort required from, and the risk of detection to, offenders. Informed investigation management, coupled with improved forensic capability, will require offenders to increase the sophistication of their offending and their forensic awareness to avoid investigation and detection. National and international cross-sector forums will facilitate the sharing of information to assist all parties to harden systems, detect incidents and track offenders. Similarly, private sector law enforcement can assist such efforts by providing specialist knowledge, and often, technical and human resources.

A number of law enforcement measures could improve investigative and intelligence gathering capabilities, increasing the risk to offenders of detection, disruption and arrest. A number of recommendations focus on the continual need for adequate training and resourcing of officers in this area. Such resources and training at the local level need to be provided in a strategic framework to ensure good and consistent operational practice between forces, and as much as possible, other agencies. Such practice, in certain cases, may warrant the use of techniques deployed in serious crime cases, as netcrime investigation moves beyond its niche network investigation and forensic evidence recovery mode, to a more aggressive but also mainstream role. As the final goal of many investigations is a conviction, then, here also, measures such as specialist training and occasionally, the provision of the necessary equipment can increase the chances of a successful prosecution. Other non-law enforcement-oriented measures to increase the risk to offenders include the detailed and long term holding of online transaction records for e-government services (so as to maintain evidence) and increasing the capacity for natural surveillance and incident reporting by users of various online services such as chat rooms. The former will assist post-offence investigations, whilst the latter measure will increase the chances of immediate intervention if criminal or malicious behaviour is occurring. However, such calls for long term record retention must be balanced against the fifth data protection principle that 'personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes'.

Despite all such measures it must be assumed that incidents will continue to succeed and such eventualities should be planned for. Where defensive network hardening measures are overcome, then continuity plans are essential to re-establish online service provision, whatever its role. As well as minimising the impact on service users, the display of such resilience will help reduce the planned benefit or reward to offenders, and may serve to dissuade further attacks once their reduced impact has been demonstrated.

Finally, a number of broad impact measures are proposed that serve also to assist a number of those already cited. Users need to change their behaviour in a number of ways, in regard to the adoption of secure, but also legal, practice. Despite the many calls for service providers and hardware manufacturers to make their services more secure, many security features and practices are not being utilised due to lack of user awareness, and perhaps the complexity of such features. In this respect users must accept responsibility for their own actions following adequate effort to bring such issues to their attention by companies and public sector bodies. Similarly, following private and public sector awareness campaigns, users should increasingly be unable to plead ignorance for criminal acts (e.g. hacking, breaching copyright laws, attempting to purchase from overseas items banned in the UK). Organisations need also to increase their efforts to secure themselves against netcrime in all its forms. The government may contribute to this by promoting the BS7799/ISO 17799 standard to appropriate categories of IT users. For individual home users, the government may directly contribute to hardening the outer perimeter of its own e-government services through the distribution of basic security measures to registered users.

Whilst each of the above recommendations individually contribute to one of the four crime prevention categories, the overlap and synergy between a number of them should not be missed. To increase the security of its e-government online services (increasing the effort through target hardening), government agencies may demand those registered users have minimum safeguards such as up-to-date anti-virus protection and an active firewall (removing excuses through rule setting). However, to ensure such requirements do not become a barrier to the use of online government services, agencies may provide such defensive measures (removing excuses through facilitating compliance). Similarly an increased priority to security measures by an organisation (increasing the effort through target hardening) will require the establishment and implementation of a security policy (removing excuses through rule setting), which should lead to increased organisational user security awareness (increasing the effort through target hardening). Such plans should normally also include a consideration of continuity planning (reducing the reward through denying benefits).

Conclusions

The Delphi research identified a number of threats and challenges and this report has detailed the panel contributions on tackling such issues. However, the development of crime prevention measures and the criminal countermove has been described as a continual ‘arms race’ (Ekblom, 1997) between those charged with securing assets and offenders. Similarly crime prevention or information assurance measures can be seen as a depreciating asset and thus any recommendations in this report must be seen in this context. Law enforcement agencies are familiar with the continual struggle to keep up to date with new technology, as embodied by the Police Science and Technology Strategy.

Most of the recommendations seek to address fundamental issues or approaches to crime problems, hence the report’s call for the tackling of netcrime to be moved from being seen as a specialist capability, to an element of mainstream policing. Discussing the research findings using the whole of the Police Science and Technology Strategy framework has attempted to illustrate this. Similarly, by discussing the findings in established crime prevention terms of the situational model, netcrime seeks to break out from its criminological niche, and be seen as a problem that is permeating mainstream criminal activity. Thus those tackling other offences, through various roles, must accept and indeed explore the implications of netcrime for their own area of accountability, rather than dismiss it as the responsibility of the computer crime or IT security community. Almost all parties involved in tackling crime must recognise that they are now, or will very shortly be, faced with some form of netcrime and it is not going to disappear. Indeed, it is suggested that future efforts in this area should include the development of a ‘future scanning’ capability. Such activity should not be seen as a one-off exercise, but a permanent and ongoing task, affirming that the challenges of netcrime are not transitory, waiting to be ‘solved’ with the emergence of yet more new technology. Rather, the day-to-day criminal challenges facing us all have gained another element.

1. Introduction

The subject of information and communication technology related crime and abuse is increasingly topical, both in the media and government. This research coincides with the publishing of e-crime and information security strategy initiatives by the Home Office and the Central Sponsor for Information Assurance. In looking to the future, other relevant initiatives include the Department for Trade and Industry's Cyber Trust and Crime Prevention Project, which is part of the ongoing Foresight futures research programme. All these initiatives begin to address, from their own perspective, elements of the concerns raised by this research. It is hoped that together all these initiatives may form the beginning of a coherent and comprehensive approach to ensuring a secure future for the UK's e-government and e-commerce success.

Introducing netcrime

Fifty-three per cent (13 million) of UK homes are connected to the Internet, along with 68 per cent of small and medium enterprises[1] (Ofcom, 2004). Offering unprecedented global access to information and individuals, the Internet represents a major societal force in areas as diverse as education, commerce, community formation or freedom of speech. Unfortunately it is equally amenable to misuse. Computer, hi-tech crime, or netcrime (the term adopted by this paper) is becoming an increasing concern to a variety of regulatory and law enforcement sectors. The information technology age in which one live means the scope for information technology-based crime and abuse is extensive and diverse. Those with a role to play in its reduction form an equally diverse group. Any consideration of netcrime will involve an examination of a broad range of technical and commercial sectors, numerous and overlapping government and law enforcement jurisdictions and an increasing number of non-governmental agencies and bodies. All of these must operate in a timely co-ordinated manner across their numerous individual sovereignties in a rapidly changing environment.

Definition

This report has adopted the term netcrime (Mann and Sutton, 1998), defined here as 'criminal or otherwise malicious activity utilising or directed towards the Internet and/or information technology applications'. This definition extends beyond desktop or laptop computers, embracing all forms of networked device (e.g. hand-held computers of various forms and networked domestic appliances). It is also assumed that most criminal activity will involve such devices being networked in some form, to a Local or Wide Area Network, the Internet and/or a public telecommunications network.[2] The terms computer, network and system will be used interchangeably throughout the report. The word 'application' has been used to suggest that the concern is not just with developments in hardware and software, but changes in the societal applications of current and future technology. Such changes may be driven by political, economic or cultural reasons. The term *hi-tech* crime has been rejected as this could include technology developments outside the scope of networked information technology such as nanotechnology or bioengineering.

Before discussing various forms of netcrime (fraud, extortion, espionage, paedophilia) the role of computers clearly varies and it is around this role that most high-level definitions revolve. The author puts forward the following three categories – a computer network[3] can be the *target* of criminal activity or it can function as an intermediary for crime, either as a *medium* or *facilitator*. The phrase '*criminal activity*' is taken to include not only the activity of criminals (those operating for personal financial gain) but also others with different motivations such as threats to national security or the national interest from politically motivated groups.

[1] Businesses that employ up to 250 employees and a minimum annual turnover of £50,000.

[2] Direct data transmission using technology such as GPRS or GSM.

[3] No explicit distinction will be made between 'computers' (e.g. desktop or centralised sitemaps) and the network which connects them, as networks are themselves made up of computers (e.g. routers) and all 'computers' require network connectivity to operate, so they should be seen as an integrated system (albeit one which may be separated into elements such as network for certain administrative or operating reasons).

Computer as target of crime

Hardware theft

The most obvious form of a computer as the target of crime is the physical theft of computers themselves. Although this does occur (e.g. theft of individual laptops), the bulk theft of computer components, such as memory or processor chips also occurs. Such theft is undertaken either by hijacking the components in transit or the removal of the chips from operating computers during the burglary of commercial premises. Looking forward, significant hardware theft may return as new powerful personal organiser or personal digital assistant (PDA) devices such as the Palm Pilot become more popular and valuable. Their size will make them as easy to steal as mobile phones (this concern is discussed in Chapter 2).

Data: confidentiality, integrity and availability

Other than the physical protection of computers from theft, most information technology security has traditionally been concerned with three key principles; maintaining the *confidentiality*, *integrity* and *availability* of system data.

Confidentiality is the simple concept that data must not be disclosed to those who are not authorised to receive it (e.g. its theft, copying or interception). The unauthorised disclosure of information may be motivated by many things other than criminal personal gain including personal malice, economic or political espionage and a variety of political motivations. The theft, copying or interception of data, may be an offender's prime, convertible or transitional target (Newman and Clarke, 2003). The copying of trade secrets may be considered the prime or final target for an offender motivated by commercial espionage. In contrast, network intruders (e.g. hackers) may seek network or user information as part of an ongoing process to gain greater access to a system and ultimately a database. Whilst such hacking is an offence in its own right, it is but a transitional target to database access and credit card details it may contain. Finally, the copied credit card details may be later used in the committal of online frauds and thus categorised as convertible targets (e.g. the credit card information is converted to a means of purchasing online goods and services). Although most information security may focus on online system (e.g. preventing hacking), information confidentiality can be breached physically. Often overlooked is the low-tech physical copying and removing of information, installed on a CD or a keyring-sized storage device. Malicious but inadvertent forms of unauthorised disclosure can also occur if a virus or worm infects a system and then randomly emails stored documents to addresses held in a contacts list; increasingly however virus-type infections intentionally seek out sensitive data and return it to a third party email address at the behest of the virus writer.

Data integrity is an issue if there is evidence or even suspicion that unauthorised system access and data modification has occurred through changes in file details such as size or when last accessed (a new file access date may also indicate a data confidentiality breach). If, for example, the accuracy of stored information in a banking system was questioned the consequences would be immense; if they were incorrect in a medical system they could be fatal. The threat of such corruption can form the basis of extortion threats against organisations. Viruses and other malicious software can also cause data to be destroyed or partially corrupted.

Data availability is a product of computer or network availability, a concept best illustrated by the inconvenience experienced by users when an office system or Internet website becomes unavailable or 'goes down'. Malicious attacks against websites are generally referred to as a 'denial of service' attack. A denial of service (DoS) attack can be defined as 'actions that prevent any part of a system from functioning in accordance with its intended purpose' (Power, 2000:330). Most attacks are in fact 'distributed denial of service' (DDoS) incidents, the impact of the attack being magnified by hitting the target from multiple computers.

The availability of systems is attacked in numerous ways including hacking, malicious software and denial of service attacks. What are often overlooked, however, are low tech, physical attacks on computer facilities or network cabling. Whilst most major computer facilities such as webhosting centres have high physical security, private power supplies and sophisticated fire controls, network cabling between sites is more vulnerable.[4] Such incidents are of particular relevance to those concerned with the integrity of the telecommunication elements of the critical national infrastructure. The critical national infrastructure can be defined as 'those parts of the United Kingdom's infrastructure for which continuity is so important to national life that loss, significant interruption, or degradation of service would have life-threatening, serious economic, or other grave social consequences for the community, or any substantial portion of the community, or would otherwise be of immediate concern to the government'.

[4] An example of such attacks can be found at http://news.zdnet.co.uk/story/0,,t269-s2124353,00.html

Computer as intermediary of crime

As computers have become increasingly widespread in modern society so their use in criminal activity has increased, reflecting a recurring pattern in the use and misuse of technology. As an intermediary, computer systems are viewed as acting as a buffer between offenders and their victims, affecting how an offence is undertaken or executed (*medium*) – the criminal *modus operandi* . Similarly computers can enable communications between offenders in a global, near real-time and relatively secure manner (*facilitator*). The Internet can also facilitate offending through its ability to provide resources such as intelligence, and in many contexts, direct tools for offending (e.g. hacking tools). Computer as an offending medium considers the offender-victim/conspirator contact, whereas computer as offending facilitator considers the offender-offender contact. The difference between these categories is often a matter of emphasis. It is possible for computers to play both roles in a single offence such as an Internet e-commerce-based fraud (medium) which may also involve significant online communication between offenders (facilitator).

Computer as medium

Much crime encountered through the Internet may be considered as 'old crimes, new medium'. An example of this is 419 fraud.[5] This fraud involves the victim receiving an unsolicited request from an overseas individual requesting assistance in transferring large amounts of money out of his/her country due to unfortunate circumstances. In return for the victim's assistance by providing bank details to receive the money, he/she will receive a percentage of the transfer. At the last minute the victim is asked to forward a cash advance to pay 'banking fees' which will be repaid along with his/her commission for helping the funds transfer. After the cash is advanced the transfer does not take place and the overseas individual disappears. This established scam has kept its essential confidence trick element whilst moving from unsolicited postal mail, then faxes and now email as the offenders seek to con the gullible and the greedy. However the offender contacts the victim, the objective is fraud, something recognised in UK legislation which does not explicitly take into account how the offence is committed. Similarly, the Internet can act as merely another distribution channel for offenders (e.g. the online selling of obscene material). In contrast to 'old crimes, new medium' is what may be considered 'new crimes for a new medium' (e.g. the Internet). Examples would be computer as target category offences such as hacking, virus writing and denial of service attacks.

Computer as facilitator

Organised offenders, be they criminals or terrorists, often require a command, control, communication and intelligence gathering capability to operate effectively, particularly if they are insulated from each other by geography, anonymity or surveillance threats (i.e. offenders may be in close proximity to each other but wary of contacting each other due to concerns that they are under surveillance). The dramatic growth of the Internet and its underlying technology, accessible encryption capabilities, and a more recent growth in mobile telephony and now wireless communications, has reduced the efficacy of traditional telephone surveillance techniques. Previously communications surveillance had to contend with monitoring perhaps a small number of fixed lines at static addresses and registered mobile phones. Computer and communication services are now widespread, with the miniaturisation and increasing sophistication of affordable devices. Conversations, along with email and data files can now be sent and received on the move from unregistered mobile phones and other portable computing communication devices using non-registered Internet access (discussed in Chapter 2 under the technology challenges of portable computing and communication devices).[6] Powerful and secure communications can be utilised via personal computers using Internet-based services such as newsgroups, mail lists, chat rooms, peer-to-peer services (discussed in Chapter 2) and, of course, websites.

Other definitions regarding netcrime include the early work by Carter (1995, cited in Casey, 2000) who proposed the following computer crime categories.

1. Computer as target (e.g. computer intrusion, data theft, techno-vandalism, techno-trespass).
2. Computer as the instrumentality of the crime (e.g. credit card fraud, telecommunications fraud, theft or fraud).
3. Computer as incidental to other crimes (e.g. drug trafficking, money laundering, child pornography).
4. Crime associated with the prevalence of computers (e.g. copyright violation, software piracy, component theft).

[5] Named after the relevant section of the Nigerian criminal code that criminalises the offence.

[6] Such devices include both wireless enabled Personal Digital Assistants such as a Palm Pilot, as well as mobile phone based devices which now include keyboards such as the Blackberry or xda.

The first three categories resemble those proposed by the author, whilst it could be said that all incidents covered in category four can be accommodated by one of the previous three (e.g. contemporary copyright violation in the form of downloading music files is copyright crime using the medium of the computer and the Internet. Casey (2000) makes the point, however, that such categories omit the role of computers as a source of evidence for investigations, whatever the crime or the role of the computer. Whilst it might be assumed that computers may be such a source of evidence whatever their role, this is perhaps a function worth noting.

Whatever the device or medium, offenders can now communicate with each other irrespective of physical location using numerous and ever evolving channels. The 'death of distance' was the first barrier to go for internationally mobile offenders with the development of the Internet and basic services such as email. For instance, dispersed and anonymous paedophiles found each other, forming self-supporting communities, strengthening and feeding their desires via bulletin boards, websites and newsgroups. Such activity is now facilitated by the next generation of communication platforms, chat rooms and peer-to-peer tools. Similarly international organised criminals and terrorists may now communicate using old techniques in a new medium such as cryptographic and steganographic[7] communications, or covert messages in public spaces (e.g. chat rooms, personal ads, auction sites etc).

Aims and objectives of the research

This research formed part of the Crime and Policing Group's Organised and Hi-Tech Crime Research programme. The aim of the research was to identify emerging criminal and malicious behaviour threats relating to the misuse of computers and the Internet, along with insight into corresponding responses and counter-measures. Such threats include ever evolving old offences committed in the new online medium and new offences that may brought about by technological or societal change. The study had three key objectives:

- to identify what areas of Internet and information technology application will be the possible focus of criminal activity in three to five year's time;
- to examine what areas of Internet and information technology possess the potential to be misused by criminals and represent a challenge to law enforcement;
- to explore how various sectors can prepare for such threats and challenges.

This report is concerned with the third objective, *The future of netcrime now: Part 1 – threats and challenges* (Morris, 2004) reporting the findings in regard to the first two objectives. In attempting to generate insight into the future, one of four different methodologies tends to be employed: forms of consensus; extrapolating on trends; historical analysis and analogy; and the systematic generation of alternative future paths such as scenario analysis (Lang, 1995). The offences and behaviours this study sought to consider are highly diverse but are linked by a common absence of recorded offence data. This is because most legislation is technology or *modus operandi* neutral and makes no specific reference to the role of computers or the Internet in its committal (the Computer Misuse Act 1990 being the main exception in covering unauthorised system access such as hacking and the dissemination of viruses). Though there is little or no official offence data (other than that generated by commercial surveys and data sets) with which to undertake quantitative trend analysis (Hyde-Bales, Morris, Charlton, 2004). Also, as this study sought to identify the new and unexpected, it was clear that the output would be qualitative in nature and hence the Delphi was selected. In undertaking such a forward-looking exercise it was hoped the findings would contribute to strategic threat assessments and broader futures work undertaken by other governmental and law enforcement organisations, as well as pulling together numerous and diverse concerns into a single, if summary, briefing document for policy makers or practitioners with an interest in this area. At the time of writing, this research (and the companion report) have contributed to the formulation of the Home Office e-crime strategy and ongoing work in this area.

[7] Cryptographic information is in plain view but encrypted to remain secure. Steganographic information, in contrast, is concealed or embedded in another object, which itself may remain in plain view. A current example would be the hiding of secret bank account details in an innocent photograph which is publicly posted on the Internet or distributed by email.

Methodology

The Delphi method

The Delphi method is a form of futures research that seeks to inform perceptions, alternatives and choices about the future. The technique was developed during the early 1950s by the RAND Corporation for military applications and has developed into three key formats (Woudenberg, 1991).

- The Conventional Delphi, as loosely used here, has two common applications, forecasting and estimating unknown parameters. The technique is often, except here, used to facilitate consensus on an issue amongst a number of individuals or groups.

- The Policy Delphi does not aim for consensus but seeks to generate the strongest possible opposing views on the resolution of an issue and to table as many opinions as possible.

- The Decision Delphi is used to reach decisions amongst a diverse group of people with different investments in the solution (Lang, 1995).

Furthermore, a Delphi approach may also be combined with other futures techniques such as the use of scenarios. The Delphi technique may be found in areas where there is an absence of sufficient data and/or an incomplete theory on cause and effect in regard to the phenomena under study. Sitting between knowledge and speculation, the informed deliberations of the panel may best be considered informed judgement. Given the diverse, interrelated and fragmented knowledge sets under examination it was deemed a suitable method for examining this area and indeed follows in the footsteps of similar research (Coutorie, 1995; Tafoya, 1986).

A conventional Delphi study (hereafter referred to simply as the Delphi) was adopted for this research and involved convening a panel of relevant 'experts' regarding netcrime and associated issues. Such a Delphi has four basic features (Lang, 1995; Woudenberg, 1991).

- *Structured questioning* is achieved through the use of questionnaires. This aims to keep participants' responses focused and enables the channelling of many inputs into a compact output.

- *Controlled feedback* is achieved by feeding back to the panel members the responses of the group, as well as their own response, for their reconsideration. This means that all the responses of the panel are taken into account.

- *Iterations* is the process by which the questionnaire is presented over at least two rounds to enable participants to reconsider their responses.

- *Anonymity of response* is achieved through the questionnaires, ideally giving group members the freedom to express their opinions without feeling pressured by the wider group.

The Delphi panel is an attempt to 'generate the positive interaction of views of a group but avoid the negative group dynamics that may emerge, such as domination by key individuals, falling into a rut of pursuing a single train of thought, pressures to conform and becoming burdened with periphery information' (Preble, 1983). It is acknowledged that such a written interactive process may lack some of the potential brainstorming stimulation that can emerge in the best group situation but it is felt that the benefits and the opportunity for considered answers outweigh these potential negative factors.

The expert panel

The composition of the expert panel is the cornerstone of the Delphi method as rigorous method and analysis cannot compensate for weak input. As the scope of the criminal and technological threats that may emerge are broad, it was essential to gather a broad church of knowledge and opinion from differing sectors. For every criminal threat it is likely that there may be both a law enforcement and technological perspective (e.g. breaking into a computer network presents technical, prevention and investigative detection issues). Such a dual approach is further complicated by the organisational and technical complexity of much Internet activity where examining one particular concern might involve numerous parties. Finally, in examining any single issue different perspectives were sought. Thus security concerns regarding a singular technology might be addressed by those who built it (a vendor); those who deploy it (information technology security); those who use it (government or consultants); and, those who may study it for weaknesses (academic researchers). The dominant theme of this study was concern over criminal and malicious behaviour hence there was a broad range of government, law enforcement and regulatory representation. Technical complexity was a significant but not sole focus of this study and the panel composition. Furthermore, some topics were given explicit recognition by the inclusion of participants with specific knowledge and experience in dealing with online paedophilia, fraud and piracy. In attempting to seek out as diverse an opinion as possible, consideration was given to seeking the participation of members of the hacker and warez community regarding hacking and piracy respectively. This approach, as adopted by Coutorie (1995), was abandoned as it was considered too problematic to validate the experience and competence of such participants, along with concerns over the confidentiality of the study.

Potential panel members were identified from numerous sources including published literature, conference presentations or were otherwise known from their participation in certain forums. In some cases relevant organisations (e.g. significant information and communication technology businesses) were approached and they in turn proposed a representative. Similarly, specialist law enforcement, government and not-for-profit organisations were approached and a suitable representative requested. The need for informed, rather than senior, representation was emphasised.

Table 1.1 summarises the sectors from which participants were drawn. Academic researchers were largely from computing and engineering disciplines but did include those from a criminal justice perspective. Government representatives covered a variety of broad issues from a regulatory and policy making perspective. Law enforcement included individuals from diverse police- and security-oriented agencies, representing experience in a broad range of criminal offences. Fraud takes many forms on the Internet and was addressed by a number of practitioners from legal and financial perspectives.

Information technology security is a very broad field and this was reflected in the differing perspectives participants brought. Some respondents could be considered ‘users’ in that they managed security for commercial organisations, whilst others represented service providers such as telecommunications, Internet Service Providers (ISPs) and webhosting companies. Others involved in broader information technology risk management consultancy also made up this group. A number of individuals specifically involved in tackling piracy (software and entertainment content) and online paedophilia in different capacities boosted input on these areas.

Table 1.1: Panel sector composition

Sector	N=	Percentage
Information technology security	7	25
Law enforcement	6	21.4
Academic research	6	21.4
Fraud	3	10.7
Government	1	3.6
Piracy	3	10.7
Online paedophilia	2	7.2
Total	28	100%

Seventy-three individuals were invited to participate in the study, of which fifty-three agreed to do so. Forty-nine actually participated in the first survey round which produced the initial round of proposed responses. Twenty-eight respondents completed the final questionnaire which examined these initial responses in detail, providing additional comments and rating the suggested responses. All of these 28 provided academic and experience details. More than half of these were graduates (54%), a quarter (29%) postgraduates (e.g. masters degrees or postgraduate certificate) and a more than a quarter (29%) either held doctorates or were undertaking doctoral studies. Twelve of the 28 (43%) possessed industrial or professional qualifications and certifications.

As well as their formal qualifications, respondents were asked to indicate on what topics they felt confident to comment based on the number of years’ experience they had in an area. Table 1.2 details the number of respondents and the accumulative years of experience represented by the panel in a number of particular topics. For individuals with broad roles their experience may contribute consecutively to many categories. That is, an experienced systems security specialist, for example, may have 20 years’ experience in each of the following: system security, computer crime investigation and digital forensics (having been the victim of hack attacks) and malicious software (patching and repairing the system after major virus outbreaks). Respondents may also have experience in the same category but from differing perspectives. A forensic accountant and a police officer may be brought in to investigate a company fraud; the system administrator may be required to search for evidence on the computer; and, a specialist lawyer may prosecute, or defend, the case.

Table 1.2: Panel experience composition

Topic experience	N=	Cumulative experience (years)
Fraud	13	151
System security management	14	133
Computer crime investigation	18	113
Information assurance	9	94
Malicious software	13	93
Encryption	11	78
Online privacy, anonymity issues	10	68
Counter espionage	6	62
Digital forensics	8	63
Digital piracy and counterfeiting	7	36
Online activism and protest	5	29
Online harassment	6	17
Social service issues (e.g. child protection)	7	31

The panel members were recruited during September 2002 and the survey conducted between October 2002 and February 2003.

The survey

The research employed four questionnaires over two rounds. Questionnaires took the form of electronic spreadsheets, distributed largely by email. Written guidance accompanied each questionnaire and respondents were able to email or telephone with any queries (though very few were received).

Round 1: Questionnaire 1

An initial short netcrime questionnaire was circulated to panel members. These questions were intentionally loose and open-ended to allow participants free rein in their responses. Questionnaire 1 contained five primary and four supplementary questions, allocated into two sections. Section one contained two primary questions (question 1 and 4), each with two identical supplementary questions (questions 2 and 3; 5 and 6), and considered future criminal threats and challenges to law enforcement.

> Question 1: What areas of Internet and information technology application do you consider the possible focus of criminal activity in two to five years time?
>
> Question 2: What form do you think these activities will take?
>
> Question 3: What are your reasons for this expectation?

Question 1 asked respondents to identify a high-level threat (e.g. online fraud), whilst question 2 asked them to illustrate what form the threat may take (e.g. online transaction websites being defrauded by the use of stolen credit cards for online goods or services). A question 1 response was often accompanied by two or more responses to question 2. Question 3 asked respondents to provide some indication of the rationale for their responses to questions 1 and 2, so that other respondents might better understand and consider their responses. The co-ordination committee did not assess the validity of the panel responses for accuracy as it was felt that any such inaccuracies would be picked up the panel peer review phase in Round 2.

Round 2: Questionnaires 2 and 3

Questions 4, 5 and 6 in questionnaire 2, regarding technology challenges, took a similar format.

> Question 4: What areas of Internet and information technology do you consider possess the potential to be misused by criminals and represent a challenge to law enforcement and/or

legitimate users?

Question 5: What form do you think these activities will take?

Question 6: What are your reasons for this expectation?

Whilst question 1 was interested in behaviour that was explicitly criminal or malicious, questions 4, 5 and 6 were concerned with technology that possessed a potential for criminal or malicious use. For example, whilst network monitoring tools are developed for legitimate purposes, a number can be used for malicious purposes (e.g. hacking).

Questions 7, 8 and 9 in questionnaire 3 were concerned with respondents' opinions on what needs to be done to prevent or mitigate the threats and challenges outlined in questions 1 to 6.

Question 7: How should UK law enforcement agencies prepare for such threats?

Question 8: How should the UK government prepare for such threats?

Question 9: Globally, how should the information and communication technology industries and IT users prepare for such threats and challenges?

As with questions 1 to 6, panel responses were not assessed in terms of accuracy or suitability by the co-ordinating committee. In a number of instances where suggestions were made for initiatives that already existed, other panellists recognised such inaccuracies and these have been cited in the relevant discussion. The responses to these questions, seven to nine, form the basis of this report.

Round 2 responses

There was substantial response overlap as respondents identified many commonly perceived criminal threats and technology challenges. Examples included threats from fraud and online paedophilia, and technology challenges presented by mobile computing and communications devices. Where such duplication existed responses were aggregated into a reworded single response (e.g. ten entries for more police training were combined into a single entry on this point). Once responses to all nine questions from questionnaire 1 had been aggregated they were fed back to the panel over three second round questionnaires covering criminal threats, technology challenges and preventive responses (the focus of this report). Each questionnaire contained the items (threats, challenges or responses) identified in Round 1, clustered around key themes. Respondents were presented with a number of forms the item might take, along with some explanation for its inclusion by members of the panel. They were then invited to comment on each item and rate it. This second phase comment and rating process served as the group feedback function, as each panel member was able to anonymously feedback on the comments of all others. Figure 1.1 provides an example of a questionnaire 4 item respondents commented on.

Figure 1.1: Example of Questionnaire 4 item

Q8. UK government response
Continual efforts to raise awareness amongst users and gatekeepers (e.g. parents, teachers, librarians) about safety and new technologies. Companies need to look to their own individual strategies but also fund charitable and joint efforts.

With questionnaire 4, respondents were asked to rate each proposed netcrime response in terms of its perceived importance, '1' representing the highest importance, '5' representing the lowest importance. Other options available to respondents were 'unwilling to comment' and 'no knowledge'. As the panel had a broad and diverse knowledge base it was to be expected that there would be response suggestions that individuals were not able to comment on. The two categories 'unwilling to comment' and 'no knowledge' enabled the survey to differentiate between respondents who were knowledgeable in an area but were unwilling to make an educated rating on an item, from those who were simply inexperienced or unaware of a certain topic. Average rating scores were calculated for each suggested response, based on the number of respondents who rated the item. The number of respondents who rated each item (excluding those who indicated they were either unable or unwilling to rate the item) is indicated alongside each item (N=) in the following tables. Because the use of average rating scores alone may be misleading (e.g. with a number of high and low scores producing a figure in the middle which does not accurately reflect panel opinions), the standard deviation score for each item is also given. The standard deviation number is a measure of the average amount user ratings on an item varied from the average rating score for that item. The more widely respondent ratings varied from each other, the larger the standard deviation. A standard deviation of zero would indicate total agreement on rating an item (highly unlikely), whilst a deviation of two would indicate the panel members were polarised (equally split between ratings of one and five).

The co-ordinating committee

Co-ordinating committees, or monitoring teams, are often found in the administration of Delphi projects. Administering Delphi research often involves subjective decisions when processing respondent contributions. In this research this subject processing focused around aggregating the respondent results as previously discussed. To avoid or minimise individual biases, the primary researcher was joined by two other researchers to form a project co-ordinating committee. Whilst these individuals were from the same organisation as the primary researcher, they were both experienced researchers with differing academic backgrounds. Furthermore, a taxonomy was used to provide a structured means of aggregating respondent contributions, where differences in language and phrasing could obscure similarities and subtle differences in proposed threats and challenges.

Summary findings of the study

Round 1: Questionnaire 1

Of the 53 questionnaires issued in Round 1, forty-eight (91%) were returned. The panel submitted a total of approximately 2,500 comments. These were aggregated down to 425 items, allocated across the three questionnaires: criminal threats (101), technology challenges (137) and netcrime responses (187).

Round 2

Round 2: Questionnaire 2 (criminal threats)

One hundred and one criminal threats were put forward for comment and rating in questionnaire 2. The threats were clustered around 13 high-level categories that emerged from a review of the responses:

- critical national infrastructure/infowar;
- denial of service attacks;
- espionage;
- extortion;
- fraud;
- hacktivism;
- hardware theft;
- malicious software;
- market abuse;
- money laundering;
- online paedophilia;
- piracy;
- non-categorised.

A non-categorised section was used for all other items that did not fit into the 12 other categories. This included items relating to topics such as spamming (the sending of unsolicited emails) and online gambling. Thirty-eight out of the 48 (80%) Round 1 participants completed the second questionnaire and rating, providing 947 additional comments on the 101 identified criminal threats.

Round 2: Questionnaire 3 (technology challenges)

One hundred and thirty-seven technology challenges were put forward for comment and rating in questionnaire 3. The threats were clustered around nine high-level categories that emerged from a review of the responses:

- anonymisation;
- broadband;
- email;
- encryption;
- mobile communications;
- peer-to-peer;
- wireless;
- webhosting; and
- non-categorised.

Twenty-nine out of the 48 (61%) Round 1 participants completed the third questionnaire and rating, providing 1,152 additional comments on the 137 identified technology challenges.

Round 2: Questionnaire 4 (netcrime responses)

Twenty-eight out of the 48 (58%) Round 1 participants completed the fourth questionnaire, rating and providing 1,493 additional comments on the 187 proposed netcrime responses. Responses were clustered around eight categories that emerged from the panel results:

- strategy and research;
- legislation, prosecution and standards;
- awareness and alerts;
- prevention and security;
- reporting and recording;
- communication and co-operation;
- policing;
- resources, tools and training.

The data produced in this study was inherently qualitative. The purpose of the rating exercise was merely to serve as a notional indicator of potential priority areas for research, policy and law enforcement stakeholders when they were faced with almost two hundred suggested responses to tackling the previously identified netcrime threats and challenges. The average importance rating for responses was 2.3, with ratings ranging from 1.36 to 3.06. Thirty per cent of the proposals had an average score of between one and two (1 being the highest importance rating), with only just under five per cent of items obtaining an average rating of below 3.5 (5 being the lowest importance rating). Broadly, therefore, one can see that respondents were uniformly disposed to positively rate netcrime response items as to their importance.

Structure of the report

The remainder of this report is broken down into three chapters. The proposed responses to netcrime have been discussed in one of two frameworks depending upon their perceived relevance to law enforcement issues or broader crime prevention measures. Such a distinction is subjective and not all items are mutually exclusive to one framework or the other. Chapter 2 will discuss a number of panel suggestions to tackle netcrime in the law enforcement context, whilst Chapter 3 will take a broader approach, considering responses in a situational crime prevention context. Each chapter contains a number of sections, each of which will conclude with report recommendations. These recommendations are the author's considered aggregations of the many points made by the panel, reflecting also knowledge of other initiatives and related issues. Finally, Chapter 4 will summarise and conclude with a discussion and the recommendations.

2. Implications for law enforcement

Home Office Police Science and Technology Strategy

The Home Office National Policing Plan seeks to outline a rounded picture of police performance by the use of the Police Performance Assessment Framework[8], which is based on six domains: reducing crime; investigating crime; promoting public safety; citizen focus; helping the public; and resource usage. The Home Office Police Science and Technology Strategy[9] seeks to identify how science and technology will have a positive impact across these domains. Its purpose is 'to ensure the police service is equipped to exploit the opportunities in science and technology to deliver effective policing as part of a modern and respected criminal justice system'. The strategy has three key aims:

- to establish priorities for current and future science and technology applications and research;
- to co-ordinate the development and implementation of technology between users and suppliers to ensure a coherent and effective process; and
- to implement processes for future scanning to ensure the police service can exploit new technology at the earliest opportunity and is prepared for new technology-based threats.

The strategy identifies 28 *capabilities* across the six Police Performance Assessment Framework domains. Each law enforcement capability is further divided into a number of *components*. Although this strategy was drawn up to encompass all aspects of policing, not specifically netcrime, it nevertheless, provides a useful, existing frame of reference in which to discuss research panel responses regarding police responses to netcrime. Figure 2.1 details the Police Science and Technology Strategy capabilities (e.g. reducing crime) and components (detailed in parenthesis e.g. 1c) drawn upon in discussing the panel responses. By adopting the Strategic Framework it is hoped to facilitate the consideration and uptake of the research findings by policy, enforcement and research stakeholders currently engaged in examining current and future technology applications as part of the Police Science and Technology Strategy. It is these issues that are largely the focus for this section of the report.

Figure 2.1: Adopted Police Science and Technology Strategy domains and components

1. Reducing crime	2. Investigating crime	4. Citizen focus	6. Resource usage
• Authenticate identity (1c) • Identify and eliminate threats to public safety (1e) • Monitor offenders that pose a threat (1f)	• Effective mgt of investigations (2a) • Effectively use intelligence gathering technology (2b) • To be able to locate and recover evidence effectively (2c) • Present evidence in court (2g) • Investigating hi-tech crime (2h)	• Communicate with the public/ external groups (4a)	• Support to different models and styles of policing (6b) • Secure exchange of electronic data between forces and other agencies (6c)

In assigning Delphi response items to the Police Science and Technology Strategy framework it should be noted that Capability 2h (Investigating Crime domain) is specifically focused on 'investigating hi-tech crime'. It has two sub-components: (i) 'local and national capability to tackle Internet based crime', and (ii) 'ability to investigate crime with Internet, email or computer storage elements'. However, allocating all policing related netcrime survey items to either of these two elements would not do justice to the many and varied actions and comments proposed by the panel. Such an approach would also continue to portray hi-tech or netcrime policing as a marginal function. In contrast, it is the author's opinion that an understanding and basic competence in handling netcrime should be placed at the centre of policing to mirror the increasing presence of computing and communication technology in everyday society and hence actual and potential criminal behaviour. For these reasons, the survey responses will be discussed under a number of broader policing domains and capabilities.

[8] http://www.policereform.gov.uk/psu/ppaf.html

[9] http://www.policereform.gov.uk/implementation/scienceandtech.html

Reducing crime (Police Performance Assessment Framework Domain 1)

Seven panel responses are considered against three reducing crime components: (i) authenticate identity (component 1c), (ii) identify and eliminate threats to public safety (component 1e), (ii) monitor offenders that pose a threat (component 1f).

Table 2.1: Reducing crime responses (Domain 1)

Response item	Rating*	SD	N=
Authenticate identity			
Paedophilia – work with industry to eliminate anonymous network activity.	1.89	1.20	19
Identify and eliminate threats to public safety			
Digital piracy manufacture/ distribution networks and criminals need to be understood.	2.86	1.25	22
A fraud / criminal IT "Tracking" system should be implemented, i.e. rogue users can be followed online at any location.	2.72	1.49	18
Industry to develop methods for identifying individuals using systems to distribute pornography or disrupt legitimate use. This has been done to combat fraud by understanding unusual behaviour patterns, and the same techniques may well be able to be adapted.	2.42	1.50	24
Ensure sufficient enforcement tools available to close down criminal web sites, web addresses etc. Interim preventative orders to order ISPs to close down sites or email accounts, to counter the speed that a site can be transferred to an alternative ISP or host. Magistrate courts to have ability to grant such orders in camera.	2.07	1.07	27
Gather intelligence on capability, targets and *modus operandi* of organised crime.	1.61	0.78	18
Monitor offenders that pose a threat			
Need to establish a group to develop creative ways of managing paedophiles in the community.	2.00	0.88	14

*1=highest importance, 5=lowest importance

As new areas of criminal or potentially challenging activity emerge, such behaviour has to be understood before it can be tackled. With netcrime this will often involve both a technical understanding (e.g. how are system vulnerabilities being exploited) and criminal network understanding (who is involved, what is their role, what is their motivation etc.). With such knowledge a combination of technical surveillance and law enforcement investigation expertise can be combined to attempt to identify and potentially track offenders, who may be operating alone or as part of a wider network. Respondents flagged these concerns in regard to copyright pirates, distributors of pornography, hackers and fraudsters, though such responses could be applicable to any criminal or malicious activity. Some respondents, however, were concerned that suggestions to track users were currently not feasible and unrealistic.[10] They also felt that law enforcement should perhaps lead such initiatives, rather than 'industry' alone. This issue of authentication of identity, confirming that someone is who they claim to be was raised by the panel as an issue in regard to tackling online paedophiles (an issue in preventing online grooming through false online personas), but the problem is fundamental in online transactions of any sort, be it for e-commerce or sending emails. However, as with proposals to 'track' certain online users, some respondents believed eliminating anonymous online activity was too difficult to realistically achieve.

There is much talk of organised crime involvement in online offending but evidence is limited. The National Criminal Intelligence Service (NCIS) 2003 *UK Threat Assessment* identifies hi-tech crime as a threat to the UK but is unable to identify what proportion of hi-tech crime is attributable to serious and organised criminals. This is largely due to the fact that crime recording does not differentiate between those with a hi-tech or organised crime component, just the crime type. It does, however note, that organised crime groups are

[10] This issue is complicated because at the simplest consideration one has to decide what shall be used to define the identity of a 'user'. First, individuals may have different identities in the form of different user names established as part of the registration process for gaining Internet access via an ISP. Second, they may again be required to adopt another user name when registering for a specific service or website. Third, some services such as chat rooms specifically allow you to change your persona online. So far one at least have three 'administrative' identities to potentially track. A fourth more 'technical' means of potentially identifying users is by the unique number (IP address) assigned to their computer when they connect to the Internet. However such addresses can be faked to various degrees and in truth indicates only the identity of the computer connected to the Internet or service, not the individual using the keyboard.

likely to be attracted to hi-tech crime due to potential financial gains and their willingness and ability to ‘buy in skills and expertise, or subcontract to specialists’ (NCIS, 2003). This lack of clear evidence on the role of organised crime activity in this area needs remedying through a concerted intelligence gathering exercise be it in specific areas of netcrime (e.g. production and distribution of illegal content) or against known criminal networks.

Criminal threats and other challenges can stem directly from the activity of offenders or from the availability of resources to potential offenders. As the largest and most accessible repository of information the world has ever seen, the World Wide Web offers many means of facilitating offenders in terms of their communications, distribution channels or making available expertise and tools they may currently lack (Ekblom and Tilley, 2000). Facilitating platforms include websites, bulletin boards, ftp servers, chatrooms and numerous peer-to-peer applications. When such facilitators of criminal behaviour are identified, respondents highlighted the need for legal powers to rapidly disrupt them through their seizure or termination. Whilst agreeing with the need for such powers, some respondents highlighted that unless such powers were effective globally, then local initiatives would have little impact against overseas-based platforms (e.g. foreign websites).

In discussing netcrime the focus is often with online activity and measures, but offline problem behaviour may also exist, particularly if online activity merely facilitates offline offending. Respondents were concerned with the offline monitoring and management of paedophiles as their online content consumption activity cannot be divorced from their potential to commit offline contact offences. Again, the potential and need for such offline activity to disrupt online offending can be applied to offenders other than paedophiles.

Reducing crime recommendations

1. Netcrime investigative techniques need to be developed that integrate technical knowledge with established criminal investigation practice.
2. A concerted intelligence gathering exercise should be undertaken to assess the role of organised crime groups in netcrime.
3. Serious consideration should be given to attempts to disrupt or remove platforms that significantly facilitate criminal or malicious online activity (e.g. the closure of websites that distribute tools or information amenable to harmful use).

Investigating crime (Police Performance Assessment Framework Domain 2)

Forty-nine research responses are considered against five investigating crime components: (i) effective management of investigations (component 2a); (ii) effectively use intelligence gathering technology (component 2b); (iii) to be able to locate and recover evidence effectively (component 2c); (iv) present evidence in court (component 2g); and (v) investigating hi-tech crime (component 2h). The investigating hi-tech crime component will be discussed separately due to the number of items attributed to it.

There were numerous calls in this report for law enforcement training in the area of netcrime from the panel which are discussed later. However skilled staff are not best used if senior managers are not themselves suitably conversant with the issues and able to effectively initiate and direct netcrime-oriented investigations. Respondents also noted the need for senior law enforcement managers to have a basic grasp of netcrime investigations so as to understand resource allocation issues in this area.

As with any crime, intelligence gathering has a potentially significant role in tackling much netcrime. Respondents had views on who, how and what should be targeted in such gathering operations. Who should be targeted was previously highlighted when discussing the need to identify and eliminate threats to public safety (component 1i); the how and what is the focus of intelligence operations. Here respondents flagged the use of established offline policing operations in tackling online offenders. When planting probes (i.e. the authorised ‘bugging’ of premises) the suspect’s hard disk could be imaged (i.e. copied). Also, the use of human intelligence sources such as undercover officers and informants could potentially be used. Respondents did note, however, that the probable lack of experienced officers in this area would be problematic, as would be the assessment and management of informants, particularly if supervised purely in an online environment. In the context of netcrime there is potential for such individuals to operate both offline and online. The US practice of police officers posing as minors in chatrooms to identify paedophiles could be considered an example of online undercover operations. In looking at *what* to target in intelligence gathering, some respondents proposed the need for law enforcement to be able to intercept the content of online communications, in addition to current ‘traffic analysis’ (e.g. X sent an email to Y). Concerns were expressed over who would best suited to issue such interception warrants, as well as the cost implications for companies tasked with storing such information.

Table 2.2: Investigating crime responses (Domain 2)

Response item	Rating*	SD	N=
Effective management of investigations (2a)			
Need to develop hi-tech skill sets in law enforcement senior management.	2.24	1.30	21
Effectively use intelligence gathering technology (2b)			
Change data interception regime to make content as well as communications data admissible. Probably requires changes to the warranting regime, giving judges primacy over politicians and senior law enforcement officials.	2.65	1.39	20
Informants need to be recruited with technical knowledge and access to services utilised by criminals.	2.37	1.34	19
When planting probes, UK law enforcement agencies should always consider taking a covert image of the suspect’s computer at the same time.	2.12	0.78	17
Use hi-tech undercover officers to infiltrate organised crime groups considering hi-tech attacks.	2.05	1.23	20
To be able to locate and recover evidence effectively (2c)			
Police need to use a wider range of log analysis to identify incidents.	2.36	0.93	14
Increase law enforcement capacity to examine the volume of computer material being seized.	1.94	1.00	18
Recognise when a mobile phone, cellular base station or test equipment has been used in a crime and how to get maximum information out of captured equipment, data and the networks.	1.50	0.52	16
Present evidence in court (2g)			
Crown Prosecution Service (CPS) and the judiciary should be educated, quickly, to understand the implications of online actions.	1.68	0.75	25
Crown Courts need to be able to view computer and DVD output to improve efficiency and increase clarity of case presentation.	1.59	0.73	22

*1=highest importance, 5=lowest importance

Whilst adequate intelligence is required to focus law enforcement and other investigative or preventive measures, evidence is finally required. Such evidence needs to be identified, recovered and presented in such as way so as to maximise the chances of legal proceedings, criminal or civil. Respondents encouraged law enforcement to make greater use of computer log analysis, as well as flagging new areas of evidence such as those involving mobile communications equipment. Identifying sources of what to examine for evidence is of little use if investigators do not have the capacity to process or examine such sources, a point raised by respondents. The inability of many police forces to examine seized computer hard disks in a timely manner due to limited resources is demonstrated by the delay investigating officers face and the use of external parties to provide such forensic support. This issue, however, is one of capacity rather than ability, a situation that may change if agencies are faced with less common software or hardware such as mobile phone base stations. Similar problems, although not raised by the panel, will exist as investigators are faced with an increasing array of smartphones and similar converged computing/communication devices, along with emerging forms of wireless networks. Respondents questioned whether undertaking forensic recovery was the best use of trained law enforcement officers and that such activity could be outsourced to specialist companies. Such outsourcing is already used to varying degrees by UK police forces, along with the use of civilian forensic personnel. Respondents recognised that once evidence is gathered its significance has to be understood by the legal authorities, something achieved through adequate education. Such understanding, by jurors as well as legal representatives, needs to be facilitated by clear and creative communication of evidential issues. This communication may require increasingly sophisticated equipment in courtrooms and other legal settings, currently provided on an *ad hoc* basis by commercial third parties.

Responses categorised under component 2h, investigating hi-tech crime, are detailed in Table 2.3 and are organised around key themes that are not part of the Police Science and Technology Strategy framework. Calls were made for netcrime policing to be given a greater priority in force strategic policing plans. In addition a far reaching, possibly independent, review of policing needs in this area, at a local, national and international level was suggested. Specific priority was given to fraud, particularly against the public sector, and child protection issues in government and police plans respectively. However, it was recognised such concerns should not be over hyped and that the public are generally more concerned with offline offences such as robbery and burglary. Also, despite the high media attention, online paedophile activity is believed to represent a far lesser threat to children than offline contact offences against children.

Table 2.3: Investigating hi-tech crime (component 2h)

Response item	Rating*	SD	N=
Strategy, priorities and organisations			
The current structure is about right, but it will take time to produce results, particularly if financial support is not increased to allow further development.	2.67	1.45	15
The creation of a dedicated tracking team (almost like a digital Interpol) would be beneficial.	2.63	1.12	19
Extend the role of National Infrastructure Security Co-ordination Centre (NISCC).	2.55	1.21	11
Move ‘hi-tech’ investigations into mainstream CID work. Almost all frauds, many murders, rapes and all paedophile cases involve a computer.	2.53	1.70	17
UK law enforcement cannot afford hi-tech resources to be in every authority.	2.40	1.30	15
Establishment of a central body/agency as a 'centre of excellence' that will be responsible for the development of standards, research & development, new forensic methods and national/international co-operation.	2.37	1.39	27
The existing hi-tech crime unit is not the right mechanism to fight tomorrow’s crimes – they are under funded and unable to attract or retain the right level of individual.	2.31	1.35	16
Internet crime does not easily fit into the National Intelligence Model. The local teacher who has downloaded images & networked, is he level 1 or 3?	2.29	0.76	7
Development of regional expert investigative support units, due to the number of paedophiles & local, national and international context.	2.18	0.88	17
Need suitable encryption legislation. Current RIPA legislation may be ineffective. Other proposals may be better – e.g. [France] treat failure to disclose password in criminal investigation as an aggravation to the offence, and incur double the penalty if convicted.	2.16	1.34	25
Research into computer forensics and development of techniques to prevent, detect and investigate e-crime. The market may never develop all the technical solutions that law enforcement needs. Academics and independent technical consultants could be briefed	2.15	1.05	26
Undertake an evidence led (independent?) assessment as to what the policing needs are at local, national and international levels.	2.13	0.95	24
Government to give higher profile to fraud prevention and investigation, in particular fraud against the public purse.	2.08	0.88	24
Ensure Human Rights and Data Protection legislation does not prevent UK PLC from conducting own incident investigation.	1.92	1.09	26
Ensure police resources are placed where we can effectively deal with the important issues. In the case of Internet paedophilia, the issue is child protection, not focusing on those who have good computer skills.	1.89	1.05	19
Higher priority must be given to e-crime initiatives in strategic police planning process, because of the projected high growth.	1.79	1.13	19
Regional law enforcement and other agencies need to drop parochial ideas concerning activities within their own boundaries, and recognise the scale and scope of Internet activity. There needs to be a better link between regional forces and the national squad	1.68	0.69	25
Put child protection & the proactive/ reactive detection of suspects in police business plans.	1.65	0.79	17
Training			
Copyright enforcement – maintain awareness of developments and investigation techniques.	2.76	1.18	21
Increase basic and refresher training for Internet specialists.	2.52	0.98	21
Introduce regular hi-tech police personnel knowledge reviews.	2.50	0.99	18
Develop a school of accreditation to identify qualified officers to deal with hi-tech crime enquiries.	2.47	1.28	17

Need a national experts group to review use of most up-to-date technology & training implications.	2.36	1.26	22
Privacy techniques – maintain awareness of developments.	2.27	0.98	22
Develop an investigations toolkit for investigators, providing up-to-date practices and protocols.	2.19	1.21	21
Evidence eliminators – maintain product awareness.	2.11	1.02	18
Incorporate IT security/ investigation principles into law enforcement training for existing & new officers.	2.09	1.19	22
Develop a forensics toolkit for investigators, providing up-to-date practices and protocols.	2.00	1.18	21
Police need to fully understand the potential intelligence available in digital technologies. Integrate this with that obtained from traditional sources.	1.92	0.86	25
Identity theft – maintain awareness of developments and investigation techniques.	1.82	0.91	22
Develop a hi-tech crime National Training Strategy, along with an ACPO best practice guide.	1.55	0.76	20
Resources and tools			
Recruit and retain more Interne- and computer-savvy police personnel and support staff by paying better wages.	1.84	0.90	19
Significant investment and training is required to build IT forensics and IT investigation capabilities. Law enforcement often seem to lack the proper equipment and facilities.	1.53	0.70	19

*1=highest importance, 5=lowest importance

The need to continually develop forensic and investigatory good practice and guidance was raised by the research. A national centre of excellence was proposed by some respondents as an option in the light of possible market failure to develop such services. Other respondents, however, believed that this was the current, or potential, role of the National Hi-Tech Crime Unit (NHTCU). Although the NHTCU's tasking does include offering 'best advice' to law enforcement and business, its primary focus is leading and supporting law enforcement investigations. Along with issuing strategic assessments and other intelligence products, the unit does undertake a limited amount of outreach and crime prevention activity but does not have the resource to develop advanced forensic practice. Other respondents cited current government promotion of relevant research, such as that commissioned by the Department for Trade and Industry (e.g. the Management of Information Programme[11]).

In regard to the organisation of present law enforcement there were very mixed views. Some respondents thought the present structure 'about right'; others believed there should be more national centralisation of expertise ('a Digital Interpol'), whilst some favoured regional units supporting local forces. This latter suggestion mirrors the previous role of the Regional Crime Squads who tackled serious crime, but were then reorganised into the National Crime Squad (of which the National Hi-Tech Crime Unit is a part). Another suggestion was that hi-tech crime investigations should not be seen as a distinct area of investigation but incorporated into 'mainstream CID', reflecting the societal incorporation of computers in everyday life, and hence, everyday offending. One suggestion for expanding the role of the National Infrastructure Security Co-ordination Centre[12], was that it should take responsibility for protecting the increasing roll-out of government online services. Whatever the organisational structure of those tackling netcrime, the highest priority from respondents was that all law enforcement bodies should drop parochial attitudes and practices so as to facilitate co-operation.

The importance of law enforcement training clearly emerged. Fourteen respondent contributions identified numerous areas of training (network investigations, forensic recovery, fraud, piracy and privacy), as well as a general desire to increase training regimes for general and specialist officers. All such training initiatives should sit within the context of a coherent national training strategy, possible with an accreditation structure. It was suggested that the National Specialist Law Enforcement Centre currently undertakes such a role in delivering a training strategy, whilst an accreditation scheme could mirror that which exists for forensic practitioners. Although there was broad support for increased technical training of law enforcement officers, it was submitted that final forensic or network investigation analysis should be undertaken by civilian

[11] For further information http://www.dti-mi.org.uk.

[12] NISCC (http://www.niscc.gov.uk/) is an interdepartmental organisation set up to co-ordinate and develop existing work within Government departments, agencies and private sector organisations, to defend the critical national infrastructure against electronic attack.

technicians who may be more removed from a criminal case and thus remain more impartial. An example of this would be the development of the forensic science service that supports, but is distinct from, the agencies it serves.

Trained individuals still require resources in the form of equipment and software tools, and some responses expressed concern at the apparent lack of such facilities. In specific regard to the development of forensic toolkits it was suggested that these are already commercially available, whilst the development of tools to tackle copyright piracy was best left to relevant industry groups created to tackle such activity.

Investigating crime recommendations

4. A national netcrime training and delivery strategy should be developed, providing basic netcrime competence training for all police officers.
5. Senior law enforcement managers need training in netcrime fundamentals so as to make more informed decisions in investigation and resource management decisions.
6. When suitable, serious crime investigative techniques should be applied to netcrime investigations (e.g. the covert imaging of hard disks, the online use of undercover officers, the identification and recruitment of online informants).
7. The existing and future urgency to increase forensic examination capability (volume and complexity) by law enforcement must be addressed. Possible solutions include the outsourcing of such examination to a suitable third party and the use of police staff specialists rather than officers to undertake such forensic recovery.
8. Those involved in prosecuting and hearing netcrime cases need specialist training in technology and netcrime fundamentals.
9. Courtrooms and similar facilities need to be adequately equipped to present technical evidential issues.
10. A national review of the existing policing organisational and resource response to netcrime should be undertaken to examine good practice and areas for development.
11. Forces must allocate resources to ensure specialist officers receive relevant netcrime training.
12. Law enforcement and other agencies must be creative in identifying additional skilled individuals to support netcrime investigations.
13. Forces and agencies must be adequately resourced to maintain their technical investigative capabilities as workloads increase and technology develops.

Citizen focus (Police Performance Assessment Framework Domain 4)

As with all forms of tackling most forms of criminal and malicious behaviour, communication and co-operation between all relevant parties, particularly victims, is important. In an area as complex as netcrime, respondents clearly confirmed the need for significant co-operation between law enforcement agencies and government departments with the information and communication technology industry as well as academic researchers. Instruments proposed to underpin closer working relationships included memorandums of understanding (e.g. with banks) and multi-stakeholder forums. An example of the latter would include the Internet Crime Forum[13], nominally hosted by the Home Office but with a broad commercial, government and public sector membership.

[13] The objective of the Internet Crime Forum (http://www.Internetcrimeforum.org.uk) is "*To promote, maintain and enhance an effective working relationship between industry and law enforcement to tackle crime and foster business and public confidence in the use of the Internet in ways that respect human rights and are sympathetic to the needs of industry*."

Table 2.4: Communicate with the external groups/public (component 4a)

Response item	Rating*	SD	N=
Put more police effort into the collection of reliable statistics, help justify and focus activities.	2.80	1.26	25
Mandate reporting of computer crime to law enforcement officials or a neutral party like UNIRAS, so at least incident statistics can be compiled.	2.63	1.50	24
Develop a working forum consisting of law enforcement and technologists to include ISP/telecom providers.	2.41	1.15	27
Police should meet regularly with other law enforcement agencies and digital rights protection groups to exchange trends and develop strategies to address piracy issues.	2.36	1.05	22
Create a 'one-stop' shop for society to report their concerns, including child abuse. Evidence has shown that the educational programmes have not been as successful as they might have been.	2.31	1.23	26
Accessibility: need to ensure that incident reports don't get stuck with the desk sergeant. Equally, need to give the impression that there's some likelihood of investigation.	2.17	1.05	24
Police need to work with e-tailers/banks to establish effective code of conduct for investigating all levels of card crime over the Internet. Put memorandums of understanding in place with banks.	2.11	0.88	19
Increase access to academic and industry knowledge and skills.	2.09	0.85	23
Police need regular meetings with governmental and policy agencies to discuss issues and identify methods of addressing them.	2.08	0.81	25
Cyberwarfare: all incidents reported to central authority. Work with industry to validate identification and location of originators. Co-ordinated intelligence gathering from critical infrastructure areas.	2.05	1.00	22
Businesses are wary of damaging their reputation if a case goes to court. Law enforcement agencies should offer 'off the record' support for business.	2.00	1.08	25
Develop information sharing between law enforcement IT industry, UK local authorities and wider UK private and non-governmental sectors e.g. the Fraud Advisory Panel. This is a big topic and needs an understanding of the US ISACS.	2.00	1.07	22
Without incident disclosure by the private sector, UK law enforcement will not be able to counter the threat and develop intelligence and threat profiles.	1.96	0.84	25
Police need to work with National and International CERTs and CIP teams to combat cybercrime.	1.78	0.80	23
Police need good working relationships with ISPs as they are often the link that stores information required in criminal cases.	1.77	0.76	26
Government needs to work with law enforcement agencies, UK IT industry, UK local authorities, the wider UK private and non-governmental sectors to develop information sharing. This is a big topic and needs an understanding of the US ISACS. Consultation should be detailed and not confined just to issues of principle.	1.73	0.78	26
The Reporting Economic Crime Online (RECOL) initiative tested by the RCMP and FBI could be utilised in the UK. At the moment the UK does not have a body that acts as a clearing house for details of possible frauds.	1.89	0.88	19

*1=highest importance, 5=lowest importance

In discussing the need for interested parties to work closely together it must not be forgotten that a large part of the information and communication technology community already has many such forums. One of the most significant in regard to tackling hackers and other forms of malicious behaviour that involves exploiting system vulnerabilities is the CERT/FIRST[14] community. This extensive and well-established global community serves as a bridge between individual users, frontline system administrators, industry and academic researchers and numerous law enforcement/regulatory agencies. Although such formal forums were generally deemed as very important by respondents, some expressed concern that there should not be unnecessary growth in bureaucracy with such contacts. They highlighted the value in existing informal

[14] This coalition, the Forum of Incident Response and Security Teams, FIRST, (http://www.first.org), brings together a variety of computer security incident response teams from government, commercial, and academic organisations. FIRST aims to foster co-operation and co-ordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large. Currently FIRST has more than 100 members.

relationships that had developed with contacts. In regard to the relationships with the Internet Service Providers who are a major source of information to law enforcement, there was concern that current positive law enforcement relationships might be undermined if new less experienced agencies sought similar information in a heavy-handed or less informed manner (e.g. all such agencies should follow the single point of contact (SPOC) process[15]).

As well as sharing information to identify issues and how to solve them, the need for victim reporting of incidents was flagged as a significant concern. Items called for both voluntary and mandatory incident reporting, noting the need for an effective mechanism to facilitate such reporting. The need for adequate training of all police personnel who may be the first point of contact for such victim reporting was stressed. As with general crime handling, if victims overcome a resistance to report an incident and then feel poorly treated they may not report subsequent incidents as well informing their peers of their poor experience. Although respondents overwhelmingly agreed with the need for increased incident reporting there were concerns over the need for adequate definition of 'incidents' so as not to swamp any reporting mechanism, particularly in regard to system penetration[16] activity. Also, the idea of 'criminalising' non-reporting victims was deemed unhelpful and disproportionate in light of the absence of mandatory reporting for other more serious crime offences. A number of comments made the point that the case for the benefits of coming forward still needed to be made as many victims are sensitive to adverse publicity, something that would be assisted by the assurances of confidentiality. Such a scheme has been formally launched by the National Hi-Tech Crime Unit. Once victims were willing and able to record incidents, then it was noted that there was a need to analyse the ensuing data to focus and help justify preventive and investigative efforts, albeit with a precautionary note that such statistics could be considered as under reporting for some time to come and not a true reflection of the state of the problem.

Citizen focus recommendations

14. National forums to ensure multi-sector communication on risks, threats and co-operative measures are essential between law enforcement, government departments, industry and research.
15. Where applicable more formal communication agreements, such as memoranda of understanding, need to be put in place to ensure reliable and confidential information sharing.
16. Netcrime victim reporting needs to be encouraged and facilitated. Key issues here are confidentiality, sensitivity and appropriateness of law enforcement response to reports when received. Accruing incident data should be analysed to identify trends, hotspots, intelligence and so forth, as is usual in crime analysis.

Resource usage (Police Performance Assessment Framework Domain 6)

The need for increased forms of communication and co-operation amongst parties is continued when considering varying forms of policing. These issues are examined by respondent views outlined in Table 2.5. The global nature of the Internet clearly requires extensive international co-operation amongst law enforcement agencies and a number of respondent items developed this point. Some respondents cited the distinction between joint working on technical issues and standards, where progress was seen to be made, and collaboration on actual operations; it was suggested that outside issues such as paedophilia and counter-terrorism, co-operation was less forthcoming. The need to develop a legal footing for global co-operation through the use of individual memorandums of understanding between agencies, to supplement existing multilateral agreements such as the Council of Europe (CoE) Cybercrime Convention and the G8 high tech crime agreements, was flagged. Until further such agreements are in place it was considered easy for offenders to locate outside the scope of such conventions.

[15] The SPOC process is a model of inter-organisation communication, found in various contexts, that dictates that for each organisation there is a single agreed point of contact between them. In the netcrime context this means that Internet Service Providers will normally only respond to police enquiries if channelled through a named and specially trained police contact officer (e.g. 'the force SPOC') normally found in the force intelligence bureau.

[16] The most basic of network security devices such as a firewall will detect hacker reconnaissance activity such as port scans and probes. If these were defined as reportable incidents then recorded figures would be in the millions.

Table 2.5: Support to different models and styles of policing (component 6b)

Response item	Rating*	SD	N=
Provide digital right holders with ability to enforce their rights.	2.89	1.15	19
Encourage a more open policy towards security for government infrastructure, weighing up risks versus economic advantage, particularly for unclassified and restricted data.	2.83	1.47	18
Extend statutory powers to private prosecuting bodies (lessening burden on police) e.g. search warrants for commercial property and access to stored data e.g. risk assessment for safety of officers, providing with information on offender (dangerous and armed).	2.82	1.59	22
There should be economic crime units regionally to partner commercial companies.	2.75	1.29	16
Police should give greater support to other enforcement agencies and encouragement for industry to protect itself, with law enforcement providing powers to enforce in management capacity.	2.62	1.24	26
Accept that the police are too few and there needs to be a manager of anti-counterfeiting activity by industry.	2.59	0.87	17
Centralise fraud prevention activity.	2.53	1.30	15
Need to consider attacks on information infrastructure security systems as a national security rather than criminal issue.	2.50	1.14	24
Share specialised police training with private prosecution bodies (who relieve the pressure on general policing), thus ensuring a level platform of investigation across public/private agencies.	2.50	1.46	16
Interchange of personnel – law enforcement staff secondments to ICT industries.	2.50	0.91	22
Police should look to overseas law enforcement in dealing with online criminals. Countries with the most successful arrest and conviction rate use proactive techniques.	2.50	1.22	24
Need to help a large number of other police forces, especially in developing countries, to get up to speed and stay there.	2.46	1.10	26
Thought should be given to some sort of Global Internet Police or co-ordinators of law enforcement efforts.	2.41	1.31	27
Audit of every government department's interest in online matters. Strategic research undertaken by all agencies to assess priorities and direction, to identify national priorities.	2.40	1.04	25
Greater thought to civil remedies as well as criminal prosecutions.	2.28	1.02	25
Recruit industry specialists as Special Constables to hi-tech crime units. Would help industry liaison and access to expensive skill sets.	2.14	1.11	21
Government should recognise that IT and law enforcement innovation comes from practitioners rather than a central directing agency.	2.08	0.95	25
Need full UK participation in CoE Cybercrime Convention activity.	2.00	0.92	20
Develop high-technology crime expertise that genuinely examines business issues to encourage industry support and commitment.	1.95	0.91	19
Bring in industry technology specialists on loan or secondment to help train.	1.91	0.75	22
Ensure mutual international recognition for enforcement orders against ISPs or webtraders. Facilitate international partnerships and Memorandums of Understanding.	1.88	0.93	25
UK Government must bring together public bodies in this space (e.g. OeE, NISCC, NHTCU, CCS, Home Office, DTI to name the most obvious). Currently work overlaps (duplicating expenditure) and makes UK government incapable of interfacing effectively with private sector, non-governmental bodies and international bodies.	1.83	0.72	23
Create a list of people with key IT skills that government/ police can call upon at time of crisis.	1.57	0.90	23
The security services, GCHQ and law enforcement should work more closely together.	1.57	1.03	21
Secure exchange of electronic data between forces and other agencies (component 6c)			
Police need bilateral or multilateral intelligence sharing agreements with other countries. Ensure mutual assistance measures for international co-operation. This just does not exist in any effective form at present.	1.36	0.49	25

*1=highest importance, 5=lowest importance

Such legal instruments need to be underpinned by an effective communications medium to enable the secure exchange of information between agencies, a response item that relates to Police Science and

Technology Strategy component 6c (secure exchange of electronic data between forces and other agencies). Occasionally, international co-operation amongst law enforcement agencies may require the exchange of expertise and even physical resources, particularly in developing countries with more pressing policing priorities. Such an outreach scheme is currently undertaken by the NHTCU in partnership with the Foreign & Commonwealth Office. A final point regarding increased co-operation is the suggestion of an international enforcement agency, with a global policing remit, the potential of Interpol and Europol to assist in this respect being cited. In the European Union context such a body has been announced. The European Network and Information Security Agency[17] (ENISA) was due to commence operations in 2004. ENISA's role is to ensure co-operation between national European high-tech crime units rather than tackling crime itself, as well as to act as a central knowledge and research resource.

Respondent calls for increased co-operation did not relate purely to the international arena. Domestically, it was suggested that attacks on the critical national infrastructure should be considered as a national security rather than criminal issue, though concern was expressed that adding another legal complexity to what is already a criminally prosecutable act was unnecessary. Aligned to a concern over attacks on the critical national infrastructure, was a call for UK law enforcement to work closer with elements of the security and intelligence community. A similar call for tighter working relationships included other non-law enforcement-based public bodies such as the Office of the e-Envoy and the Department for Trade and Industry who both play a significant role in Government online policy from differing perspectives.

Other suggestions in which the fight against criminal and malicious behaviour could be shared involved a greater role for industry and other non-law enforcement bodies. Ideas included the extension to private organisations of selected powers allowing investigatory actions such as search and seizure warrants, along with suitable police training in their use and execution. Such proposals echo suggestions for the greater use of civil rather than criminal instruments in tackling offenders.[18] Whilst there was support for such measures, concerns included the disclosure of potentially sensitive law enforcement investigative techniques, the need for high standards of training and integrity in performing such tasks and the need for law enforcement to maintain primacy in all serious cases. There is a fine line between public and private collaboration and most respondents felt there should be limits on the scope of commercial investigations and prosecutions. The use of civil courts for suitable actions was supported with mention that certain of these courts have more experience in some netcrime areas than criminal courts.

Other forms of public/private collaboration could be extended via skills exchange through the secondment of law enforcement officers to various information and communication technology companies, though concern was expressed that this could in fact increase the loss of suitably trained law enforcement personnel to the private sector. An alternative suggestion was the appointment of private sector IT specialists as Special Constables, though some doubt was expressed as to whether specialist IT individuals had the time for such activity. Such individuals would also have to be extensively vetted prior to assisting in sensitive operations.

Another route to obtaining additional personnel was proposed involving the pre-registration of volunteer experts. In discussing the role of volunteers, respondents noted the need for confidentiality of such arrangements.

Resource usage recommendations

17. International and national mediums need to exist to ensure rapid and effective communication between law enforcement agencies and government departments with a role in preventing, investigating and disrupting global netcrime offending. An efficient and secure communications medium is required to facilitate such co-operation. International forums or a single agency may be serve as such a medium.
18. There needs to be greater public and private sector collaboration in investigating and disrupting much netcrime with non-law enforcement bodies undertaking their own criminal investigations.

[17] For further information regarding ENISA http://europa.eu.int/agencies/enisa/index_en.htm .

[18] The use of law enforcement techniques, such as surveillance leading to civil prosecutions, has become increasingly common in recent years in regard to local authorities tackling anti-social behaviour (Morris, 1994).

3. Situational crime prevention: implications for government, users and the information and communication technology industry

Situational crime prevention

The diversity of criminal and malicious behaviours identified by the panel reflects the scope for computer and communications technology misuse. In trying to untangle the technological and criminal complexity involved in many such crimes, it became clear that one has to separate out often numerous stages and parties involved in their committal, each of which may represent an offence in its own right. Similarly, some offences are targeted against specific individuals or organisations, whilst others are unfocused in their attack. Newman and Clarke's (2003) seven target types provide a useful framework to deconstruct the complexity of much netcrime. As previously discussed *prime* targets represent the object to be stolen and can be thought of as either information to be seized (e.g. sensitive intellectual property) or manipulated (e.g. moving electronic funds between accounts). In contrast *transitional* targets are again information or elements of an information system that have to be overcome in obtaining the prime target (e.g. overcoming log-in or other secure access measures). Similarly, *convertible* targets may also be transitional in that they facilitate the committal of an offence (e.g. the theft of credit card details for the fraudulent purchase of goods and services). An offender, such as a hacker, may have a specific computer target (e.g. the website of a particular bank) with a specific criminal objective in mind (e.g. gaining access to and the theft of account details). Such a focused attack would be considered as against an *attractive* target in that it may represent significant financial or high profile gain. In contrast many hackers, particularly the less skilled (i.e. script kiddies), may not have a specific target. Such offenders often use automated tools that simply scan large areas of the Internet looking for an open door into a computer system.[19] Such potential victims may be considered *proximate* targets as such attacks are specific only to a virtual locale (i.e. a block of computer IP addresses), rather than a specific computer address. Finally, some netcrime victims may be considered *undifferentiated* targets of an offender who has little or no focus as to who is to be affected by his or her actions (e.g. the mass victims of a virus released by its creator).

If the discussion of policing implications largely focused on means of increasing the ability of law enforcement to better detect, investigate and prosecute netcrime, then the focus of this section is prevention and impact reduction. To this end, respondent response items will be discussed largely in terms of the situational crime prevention model. Figure 3.1 details the 16 techniques of situational crime prevention as revised (Newman and Clarke, 2003) to discuss criminal threats to e-commerce.[20] This framework is composed of 16 elements covering four broad objectives: (i) to increase the perceived effort for offenders; to increase the risk to offenders; to reduce the anticipated reward to offenders [if successful]; and to remove excuses. There is often a dynamic link between these issues in that an offender may increase his offending effort or choose to forgo some of the potential reward in response to a perceived increase in risk.

Figure 3.1: Sixteen techniques of situational crime prevention

Increasing the perceived effort	Increasing the perceived risks	Reducing anticipated rewards	Removing excuses
1. Target hardening	5. Detection intrusions	9. Target removal	13. Rule setting
2. Access control	6. Formal surveillance	10. Identify property	14. Alerting conscience & controlling disinhibitors
3. Safeguarding data integrity	7. Employee surveillance	11. Reducing temptation	15. Assigning responsibility
4. Authenticating identity	8. Natural surveillance	12. Denying benefits	16. Facilitating compliance

In discussing the application of such techniques to tackling online crime (specifically in regard to e-commerce crime), Newman and Clarke (2003) argue that any attempts to increase the risk to offenders will be

[19] This is known as 'port scanning'. Port scanning has legitimate uses in managing networks, but can also be malicious if looking for a weakened point of access.

[20] The most recent adaptation of the situational crime prevention classification by Cornish and Clarke (2003) features 25 techniques across five categories.

undermined by the perceived general lack of legislation – and hence sanction – in large swathes of the Internet, both by offence and geographically. In examining panel responses to netcrime and other problematic behaviours, it can be seen that potential measures lie both online and offline. Also, a number are not 'confined by elements of time' (Newman and Clarke, 2003: 111), meaning that despite the real-time nature of much online activity, such activity does leave residual traces that can be recovered to provide useful evidence at a later date.

Increasing the perceived effort

Four broad techniques are identified in increasing the effort to offenders in the committal of their crime: target hardening; access control; safeguarding data integrity; and authenticating identity.

Target hardening

Target hardening is traditionally one of the more straightforward concepts to apply to offline situational crime prevention (e.g. improved locks on cars to prevent their theft). In regard to netcrime its use is still straightforward, although one should think somewhat laterally as to what the 'target' may be. A number of proposals put forward by the expert panel echo those suggested by Newman and Clarke (2003).

Table 3.1: Panel responses: target hardening techniques

Response item	Rating*	SD	N=
Industry should provide automated firewall protection for home users.	2.88	1.42	25
Consider encouraging ISPs to provide a first line of defence against viruses. This would not obviate end users responsibility but might slow down dissemination.	2.79	1.59	24
Industry should try harder to inform users of software vulnerabilities and security loopholes and make patches available as a matter of routine.	2.56	1.28	27
In consultation with child welfare specialists, industry should ensure that there are safeguards and safety messages when introducing new technologies, and that they are reviewed regularly.	2.36	1.15	25
Organisations should pay urgent attention to system vulnerability testing.	2.36	1.15	25
Industry should develop and promote greater use of deterrents to make abuse harder e.g. firewalls, intrusion detection systems, biometrics, encryption.	2.22	1.19	27
Design and build systems for a hostile Internet, not a trusted one.	2.13	1.25	23
Government action should be informed by risk analysis and the differential ability of organisations to manage it. Large professional firms may be able to secure themselves. Initiatives need to focus on smaller firms and individuals, with less access to IT security expertise.	2.12	1.03	26
Build security requirements into the design of IT systems and outsourcing arrangements.	1.96	0.90	27
Companies should use a best practice patching and security configuration checking policy.	1.96	0.82	23
More focus on e-crime prevention rather than response. ICT industries must be encouraged to 'design in security' and 'design out crime'. Developers should follow best secure coding practice and have a flaw reporting and remedial system in place.	1.63	0.84	27

*1=highest importance, 5=lowest importance

A number of panel suggestions related to the 'designing out crime' perspective, namely building products from a security perspective at the outset rather than considering security concerns as an afterthought. Such product hardening would include the numerous components that make up modern feature-rich computer operating systems, as well as specific software applications (McGraw, 2002). The need for an increased security emphasis relates to off-the-shelf packages, as well as bespoke products and services, including the defining of security requirements when existing systems are outsourced. The overall ethos for all parties should be, as one item put it, to assume that the Internet is a hostile environment, in strict contrast to an earlier ethos facilitating the sharing of information, rather than securing it. In discussing these points respondents pointed out that many applications can currently be secured against offenders but require the user to configure them appropriately; hence whilst more education may be required, users also have to take responsibility in hardening existing products. An essential feature of security features is that they are easy to use so as to facilitate user adoption (Johnston *et al.*, 2003). More broadly, some comments suggested that vendors should be held more responsible for issuing products with security vulnerabilities (i.e. product liability).

Other forms of improving security related to elements of the Internet infrastructure, as well as individual desktop computers. Starting with the Internet Service Providers, through which all residential and many businesses connect to the Internet, one suggestion was that they act as an upstream anti-virus filter. Respondents indicated that such services already exist, provided by both Internet Service Providers and certain email services. Concern was expressed, however, that individual users might get complacent and fail to practise basic user security measures (e.g. do not open emails from unknown sources, particularly with attachments). The suggestion that software suppliers increase their efforts to inform system administrators and home users of patches to reduce vulnerabilities that hackers or virus writers might exploit was largely met with comments that this does already occur but that again, users, for various reasons, are failing or delaying the installation of such patches. It was also pointed out that at least one major operating system can now automate this process but again users have to enable this feature, requiring attention to user education. Similarly, it was suggested that 'industry' should provide firewall capability to users by default, rather than an additional purchase option. Again, respondents pointed out that at least one major operating system had already taken this approach, but again, users were currently required to activate it themselves. Other panel members felt that such security measures would add to the cost of computing products and services and should not be imposed on users but remain optional.

Where users may have security measures in place one suggestion related to testing such measures, often by a retained third party. Some respondents felt such measures, and expenditure, were only required where a thorough risk assessment indicated such testing was warranted. In general it was felt, as with offline security management, that security measures should be commensurate with the perceived threat level, which should be inferred by careful consideration of a risk management strategy.

Access control

Access control is a familiar term in a network or computer security context. In regard to the physical environment it has associations with the concept of 'defensible space' and historical measures such as moats and drawbridges (Newman and Clarke, 2003). There is the potential of overlap with the target hardening category, as some such techniques may provide a form of access control (e.g. a firewall). In looking at access control techniques one needs to consider access to what, how and by whom. Access may be physical access to computer workstations by an offender. Alternatively, it could refer to access to information by an offender (online by hacking or offline through the use of social engineering techniques) or by a piece of software acting on behalf of an offender (e.g. spyware or some form of blended virus). User-sensitive information may also be disclosed to an offender by the use of fake websites (also known as 'phishing') which tricks a user into providing credit card or other confidential information.

Table 3.2: Panel responses: access controls techniques

Response item	Rating*	SD	N=
Organisations need to vet IT staff.	2.71	1.23	24
Users should be provided with personal safety tools e.g. able to block certain callers on mobiles (as is currently possible on Instant Messenger). Users should also be educated about these tools.	2.69	1.35	26
Industry should introduce means to authenticate and independently validate nodes on wireless networks.	2.42	1.35	19

*1=highest importance, 5=lowest importance

Offenders need to connect to a network if attempting to remotely access resources on the system. The particular current vulnerability of wireless networks to such remote access was touched upon in this report's companion (Morris, 2004), and respondents therefore flagged the need to identify and control such connections. Panel respondent views were that such features were the responsibility of both vendors and users of such networks. Suppliers should decide whether to introduce such features whilst users could influence such decisions by deciding whether or not to use such services (e.g. market forces). Also, one of the purposes of such networks is to facilitate *ad hoc* connections, a feature stronger access measures could disrupt. As in other forms of criminality (e.g. fraud and theft) staff represent a potentially significant threat to controlled information. Another source of unauthorised access to information access is from internal staff who may not have to overcome such outward-facing control measures. Suggested, but already well established, was the need to thoroughly vet IT staff (respondents cited IT staff in their response but all users with a certain level of access to sensitive information should be included in such measures) joining the organisations. Such vetting could include a criminal records check and following up employer references. It was pointed out that employees who may have been dismissed but not convicted for offences may seek to omit such employment periods from their employment history. To overcome this it was pointed out that some retail business communities maintain their own list of dismissed staff for this very reason. Other forms of access control, at the user level, were promoted to deter malicious behaviour such as harassment or stalking by email or other communication devices. A number of panel members suggested that such features did in fact already exist on many products and services and that users need to be made aware of such features and also make the effort themselves to become acquainted with them.

Safeguarding data integrity

Although no panel responses neatly fit into this category it is worth outlining the issues it encompasses as they are established computer security measures. Safeguarding data integrity is a central tenet of computer security and in this context would include measures such as the use of checksum verification measures which indicate if a file has been altered or even accessed in any way. The use of powerful cryptography could also serve to prevent data manipulation if accessed and indeed Newman and Clarke (2003: 120) call for allowing the commercial use of the highest level of cryptography available, something restricted by law in the US.

Authenticating identity[21]

Authenticating identity is another core computer term, but in this context is discussed by Newman and Clarke (2003) to include online measures such as public key infrastructure, digital signatures and certificates. Offline measures would include the use of credit or smart cards to pay for services which, whilst not perfect, do offer less anonymity than cash or other payment systems.

Table 3.3: Panel responses: authenticating identity techniques

Response item	Rating*	SD	N=
Wireless technology – work with industry to have a unique identity associated with every wireless product.	2.75	1.60	12
ISPs and CSPs should be more accountable for who uses their services. Although privacy is relevant, anonymous use of ISP/CSP services, primarily for illegal activity, must be tackled.	2.50	1.23	26
Insist on greater proof of identity of Internet account holders. Require cybercafe and public access terminal users to provide identification to remove anonymity.	2.30	1.35	27

*1=highest importance, 5=lowest importance

The issue of authentication partially overlaps with measures proposed elsewhere, such as greater control of wireless network nodes. The comments here invoke largely offline measures to tackle online anonymity to varying degrees. Some measures seek to require physical identity authentication by demanding proof of identity to open an Internet account (e.g. an ISP connection) or even users of public Internet terminals where such user account status is frequently not required. Panel concerns were that such requirements might hinder government efforts to get more people online, as well as breaching a right to privacy. Again there were also fears that such measures would represent another cost to the running of such services. Other respondents supported such measures, believing that the ability to operate relatively anonymously was a major aid to offenders. It was pointed out that responsibility for tackling anonymity was quite distinct from making ISPs and others also accountable for the actions of such users. Moving from identifying users to individual computing devices (though this will not tell you who is operating the device), again concern was raised over the perceived lack of identification of hardware connected to wireless networks. It was pointed out that this would be a global issue, due to the international nature of manufacturing and engineering standards, and would again represent a potential privacy issue.

[21] This technique replaces the ‘controlling facilitators’ technique from earlier situational crime prevention models.

Increasing the effort recommendations

19. Hardware, software and service providers need to be encouraged to design and deliver goods and services for a hostile environment, incorporating easy-to-use security and crime prevention measures at conception rather than post-design stage.
20. The message that IT-dependent organisations need to secure their IT infrastructure from internal and external threats and abuse must be constantly promoted.
21. Individual users need to become aware of existing security measures on personal computing and communication devices.

Increasing the perceived risks

Increasing the risk to offenders comprises four techniques: intrusion detection; formal surveillance; employee surveillance; and natural surveillance.

Intrusion detection

For intrusion detection[22] Newman and Clarke (2003) suggest measures which monitor and analyse network and user activity. Such measures can operate in real time (i.e. live network monitoring) or in retrospect (the historical review of computer log records). Measures put forward include server log and user keystroke analysis. Such activity is similar to crime pattern analysis of recorded crime or incident data to identify areas of concern, patterns or trends. In contrast, Newman and Clarke suggest searching out signs of unauthorised network monitoring in the form of locating unauthorised packet sniffer software. To this one could add unauthorised keystroke loggers. The presence of either application would indicate unauthorised system access through some means. Not cited by Newman and Clarke, but an obvious candidate for this category, would be the use of intrusion detection systems.

This technique category has some overlap with other categories, mostly target hardening and access control. For example, whilst a firewall may be considered a means of target hardening a network, its specific function is to control who *accesses* a network[23] and in doing this it will detect and record attempted and actual intrusions to the network. Firewalls commonly integrate with network intrusion detection systems applications where deployed.

A number of panel responses related to the identification and recording of network activity, unauthorised or otherwise. As government services are rolled out online, the need to monitor and record all such transactions for later possible investigation was flagged. Panel respondents pointed out that such data may be of limited use however, if not accompanied by strong authentication techniques (i.e. transaction details are of no use if one cannot guarantee the identity of the user to which they allegedly relate). This need for authentication and transaction details is clearly not new or limited to government, being a major issue for the current multitude of online services that involve sensitive activity (e.g. online banking).

Table 3.4: Panel responses: detecting intrusions techniques

Response item	Rating*	SD	N=
Work with IT industry to develop quarantine feature/ applications that can reduce impacts of attacks – develop the 'honey trap' idea. Will have to consider data, privacy and human rights legislation.	2.69	1.01	16
Ensure online government transactions can be evidential and are archived in a way that will remain admissible in court. Automatically capture IP address, date and time on all declarations submitted online to government agencies.	2.28	1.21	25

*1=highest importance, 5=lowest importance

In tackling network intrusions, much can be learnt by the opportunity to observe offenders in action. Whilst not new, honeynets (or honeypots) are increasingly being deployed so as to enable security specialists the opportunity to monitor offenders tackling a variety of network configurations and security measures. Honeynets are computers that mimic a computer network, whilst in fact normally being a single computer

[22] This technique replaces the ‘entry/exit screening’ technique from earlier situational crime prevention models.
[23] Firewalls can actually generally monitor both incoming and outgoing activity.

connected to no network other than the Internet. The goal of one of the most established such projects is to ' learn the tools, tactics, and motives of the blackhat community [hackers] and share these lessons learned'.[24] Thus they identify and disseminate the observed *modus operandi* of offenders. A number of such projects exist but are operated by either private security companies or research organisations.

Surveillance

Surveillance can be formal, employee- or natural-based. Although the panel generated two items that fit neatly within this category, all three categories will be discussed as they are applicable to the online environment.

Formal surveillance

In an offline context formal surveillance would include monitoring by security staff, contrasting with the additional surveillance undertaken by non-security employees in many workplaces (e.g. shop sales assistants). In the online environment a localised example of formal surveillance would be the monitoring of chatrooms by human moderators, or to a lesser extent the automated filtering of online chat by software (e.g. block the use of obscene language). Such measures can generally only apply to commercial services, in contrast to open *ad hoc* non-commercial IRC based chat rooms.

Table 3.5: Panel responses: formal and employee surveillance techniques

Response item	Rating*	SD	N=
Government should support national/ international early warning detection systems for viruses and hacking attacks.	2.19	1.30	26
Develop better chat room monitoring and authentication methods, particularly those that expose child pornography.	1.83	1.17	24
Organisations should properly monitor staff and support the information security function as part of the corporate ethos. Have a CSO/CISO is a good start.	1.74	0.75	23

*1=highest importance, 5=lowest importance

Larger formal surveillance systems would include network protection applications that aim to identify, prevent and notify users of viruses, spam and spyware applications. Other more complex forms of monitoring, often undertaken by commercial or government information security organisations, involve watching out for the dissemination of software code (i.e. exploits) that can be used by hackers to penetrate insecure (i.e. unpatched) networks.

One of the key deliverables of any monitoring is to warn users so they may take appropriate preventive action (e.g. patching their systems and updating anti-virus software). A panel suggestion that this be undertaken by the government sector in some form was largely met with respondent comments that many publicly accessible warning systems are currently provided by the private (anti-virus and security vendors, as well as software manufacturers) and research sectors (e.g. CERT/CC). The UK does already have such a government agency in the form of UNIRAS[25] (Unified Incident Reporting and Alert Scheme). UNIRAS was established in 1992 with the role of gathering information on IT security incidents in government departments and agencies, producing periodic analysis and assessment of incidents and trends, and issuing alerts and briefings on matters of IT security concern. Although aimed primarily at UK government departments and agencies, its alerts are publicly accessible from its website. Panel respondents pointed out that such an alert scheme should not distract from efforts to ensure users secure their networks or computers in a proactive manner rather than in response to notifications from a central source.

Employee surveillance

Although most transactions in online services are by definition automated, there are always elements with human intervention, particularly customer service or ordering lines. As in any retail or service industry, such telephone-based employees can be trained in identifying suspicious behaviour when handling queries or transactions. Such training could also include briefing staff in what information not to disclose to phone enquiries, be they internal or external. Although this action could be considered under access control, organisations should be aware that hackers may attempt to obtain sensitive information to aid their unauthorised online access by obtaining information from an organisation by phoning employees and

[24] The Honeynet Project http://project.honeynet.org/misc/project.html.

[25] For further information visit the UNIRAS website http://www.uniras.gov.uk/index.html.

masquerading as customers or internal staff. This deception technique is called ‘social engineering’ and was used to great effect by a number of early infamous hackers such as Kevin Mitnick.

Natural surveillance

Natural surveillance in an offline context is taken to include members of the public observing and reporting any crime or malicious behaviour they may encounter in the normal course of events. Online chat users can provide a form of natural surveillance by reporting malicious or questionable behaviour by other users to service providers as they participate in the online environment.[26]

Increasing perceived risks recommendations

22. Online services need to retain detailed transaction records for an extensive period to facilitate later possible investigation or query.
23. Organisations should think broadly in developing surveillance capabilities to detect online and offline system or service abuse.

Reducing the anticipated rewards

If an offender is successful in the initial stage of his/her offence a number of measures are proposed to remove or reduce the pay-off. Reducing the anticipated rewards to offenders comprises four techniques: target removal; identifying property; reducing temptation; and denying benefits. Although respondent responses occupy only one of these categories all four shall be outlined, as they are all potentially useful.

Target removal

Offline examples of target removal include disrupting the robbing of payphones and gas meters by switching from cash to non-cash payment methods(e.g. token or card credits) thus removing the cash target. In an online environment auctions are currently a major vehicle for fraud. One common method is for victims to pay for items with cash or some online cash substitute (excluding credit cards) but the goods fail to materialise. Increasingly, however, the target of the crime, the victim’s payment, is held in a third party escrow until the purchaser verifies receipt of the correct goods. Thus the business process is changed to remove the primary criminal target. The use of third party verification services can be used for many online transactions other than the auction example given here.

Identifying property

Identifying property to facilitate its recovery or disrupt its later use or sale is an old technique and strongly used in the tracking of stolen vehicles. In the online context, Newman and Clarke (2003: 129) suggest the theft or undermining of intellectual property, often in the form of piracy, be countered by the prominent display of copyright information on websites, software and other electronic products. However, for many offenders this may function only as a potential ‘alerting conscience’ technique (discussed below) if it does not actually disrupt the use of the product. In the physical but networked environment, radio frequency identification (RFID) tags are an emerging property-marking technology.

Reducing temptation

In dealing with online offenders, particularly hackers, reducing temptation is a challenging task. Newman and Clarke (2003) suggest that organisations, primarily through their websites, have to demonstrate to customers and potential offenders that their networks are secure (e.g. ‘protected by’ logos and security statements), whilst not seeming to throw down a challenge to potential offenders (e.g. ‘we believe our network is impregnable’). Unfortunately many organisations may be targeted due to the nature of the data they possess (e.g. credit card issuers or processors) or their status to elements of the hacking community (e.g. major

[26] The Home Office *Good practice models and guidance for the Internet industry* includes a recommendation that server providers prominently deploy user reporting mechanisms http://uk.sitestat.com/homeoffice/homeoffice/s?docs.ho_model&ns_type=pdf&ns_url=%5Bhttp://www.homeoffice.gov.uk/docs/ho_model.pdf%5D

online security providers or software providers). This is a fine line to walk and explicit guidelines are probably not possible.

Denying benefits

Looking beyond deterrence, prevention and detection, measures can be put in place to disrupt an offender even if initially successful in the committal of an offence. Offline examples would include products that require a separate secondary item to operate (e.g. car radios or credit cards requiring a PIN code). Online examples include the product key that is increasingly required to activate many software products. Alternatively, data files can be encrypted such that even if accessed and copied they are unreadable (unless a secondary process is able to decrypt them). With the move to online content for consumer items such as music, games and video, new technologies are constantly emerging to control the use of digital media. The expert panel flagged the development of such measures but did not rate them particularly highly and considered them the responsibility of the content publishers.

Much criminal online behaviour involves the disruption or termination of online services (i.e. hacking or denial of service attacks), be they by large e-commerce operators, communication service providers or government departments. Countering such attacks may be considered the responsibility of various measures discussed under target hardening and access control techniques. However, if such measures are overcome and an attack is successful in taking a service offline, then the ability of the target organisation to resume service may still deny the offender the benefits they seek. The benefits denied depend upon the motivation of the offender(s). If the attackers are hackers motivated purely by ‘bragging rights’, then these are somewhat curtailed, albeit probably still quite significant, if the impact of their actions lasts a number of hours rather than days. In contrast, if the attackers are criminals out for personal financial gain, then their ability to extort money from the victim organisation is significantly undermined if the loss of business extends to hours rather than days. Similarly, if critical government or other critical national infrastructure systems are able to re-commence in a short period following a politically motivated infowar attack by terrorists or a hostile nation state, then less of a vulnerability window is presented.

Table 3.6: Panel responses: denying benefits

Response item	Rating*	SD	N=
Industry to increase anti-piracy mechanisms on files.	3.04	1.30	23
Organisations need to develop risk assessments and continuity action plans in case of network attack.	1.92	0.89	26
Contingency arrangements and risk assessments for any major hi-tech crime disruption or infowar should be part of government online systems.	1.92	1.13	26

*1=highest importance, 5=lowest importance

Reducing anticipated rewards recommendations

24. Risk assessments need to consider and take account of the nature of the perceived reward to the offender.
25. Both governmental and non-governmental organisations with significant IT and communication operations need to ensure risk-based continuity plans are in place.

Removing excuses

Removing excuses for offending comprises four techniques: rule setting; alerting conscience and controlling inhibitors; assigning responsibility; and facilitating compliance. All these techniques will be discussed alongside panel responses.

Rule setting

Newman and Clarke believe that ‘if rules are unclear or not visibly enforced, individuals will take advantage of the ambiguities’, (2003: 132). Standards, rules and procedures are the basis for rule setting, negating ambiguity at the individual user and organisational level. Legal ambiguity regarding much potentially criminal behaviour is a product of the global nature of the Internet and the lack of common laws and enforcement agencies for activity such as computer misuse (e.g. hacking, virus writing, denial of service attacks) and pornographic material and intellectual property. A second potential driver of such ambiguity may be the basic ignorance of users of the legal status of many online transactions. In the offline world one assumes that the majority of the retail environment is legal because one is aware to varying degrees of the regulatory activity of bodies such as trading standards officers and the police. Online, one may again assume that the availability of a product or service must be legal if it is 'publicly available', assuming the existence of some local (wherever local is in regard to the website) regulatory body. The ambiguities such global variations can produce is illustrated by the emergence of 'grey markets' in products as diverse as pharmaceuticals to branded clothing. The Internet facilitates such cross-regulatory transactions as never before. In the absence of any kind of kite mark for an organisation's website, users may take their cues from the professionalism of the website's appearance, but this is a product of design capability rather than legal authenticity. When users use peer-to-peer applications such as KaZaA to download music files, it may be assumed that a number of them are unaware of the illegal nature of what they are doing due to its near commonplace usage and highly professional appearance.

As well as the legal ambiguity of much behaviour, a greater problem may be the naivety of users in regard to secure behaviour. The panel put forward a number of suggestions involving the broad education of users. Compliance in this case may not be in regard to just legal behaviour but also in regard to secure or 'safe surfing' behaviour. Issues would include how to 'harden' their computers with firewalls and anti-virus applications, as well as securing access to sensitive information such as credit card details. One panel suggestion was that online banking providers educate their customers to such issues; such education could be provided by any confidential service provider. Although not cited by the panel, one obstacle to such initiatives is that such online service providers are reluctant to highlight the potential dangers as they may deter individuals from using their service in the first place. Another means of assisting unsophisticated users to assess the vulnerability of their computers is through the use of simple software tools. Such an approach was not cited by the panel but such tools or services are freely available and their use should be promoted.[27] Despite the numerous calls for users to be educated, a number of respondents commented that domestic users should still be considered a low grade primary target (although they are equally vulnerable as undifferentiated virus victims) compared to larger organisational targets. An alternative view is that domestic users may be viewed as high convertible targets, as unprotected home PCs may be unwittingly used as intermediaries through which offenders attack other systems, as currently seen with commercial systems.

The panel had a number of suggestions in regard to formal legislation as a means of setting rules for Internet behaviour. Specifically there was a call to revise the existing Computer Misuse Act 1990 in regard to concerns over its ability to effectively prosecute offenders for denial of service attacks or 'unauthorised activities by authorised persons'. Similar concern was expressed over the perceived lack of enforcement of the Data Protection Act. Progress in this area was acknowledged with the drafting of online grooming legislation for paedophilia, but broadly there was a concern that any new legislation must keep up with technological developments. The development of 3G smartphones was cited as an example of new computing devices that need to be captured in any legislation. However, such concerns must be set alongside the need for legislation to be functionally generic or broadly worded, so as to ensure it is flexible in its application and does not quickly become out of date as technology changes.

Adoption of existing IT security standards (e.g. the international information security best practice standard ISO 17799) was a key theme. Although adoption of this standard was generally encouraged it was pointed out that many organisations might comply with it whilst not actually achieving certification for a variety of reasons. It was suggested that government could encourage take up of the standard by requiring that its contractors comply with it, whilst also promoting the standard through various mediums. Other suggested means of enforcing minimum security standards were to make such standards explicit in relevant sector legislation. An example of this would be those standards required by the Financial Services Authority (FSA) as part of their authorisation requirements.

[27] An example is the online Symantec Security Check http://www.symantec.com/homecomputing/?sfgdata=4 .

__Table 3.7: Panel responses: rule setting techniques__

Response item	Rating*	SD	N=
Consumers should be more aware of risks and focus their activities on sites and operators which they can be satisfied are well regulated even if on the face of it they may not appear to offer best value.	2.85	1.22	26
e-banking regulation should require customer security education and advice.	2.64	0.76	25
ICT industries could work with regulatory and consumer bodies to ensure consumer protection and education issues in an e-setting can be tackled successfully.	2.50	0.76	26
Push strongly on BS7799 (ISO17799) programme for government departments; this seems to have subsided.	2.50	0.86	18
Encourage industry to comply with IT security standard ISO 17799. Government departments should require businesses that deal with them to be ISO 17799 compliant.	2.44	1.20	18
Enforce the law in simple area such as data protection to ensure senior management take notice of security issues.	2.42	1.21	26
Provide or recommend best practice configuration guides on commonly used products. Provide or recommend security auditing and testing services.	2.42	0.97	24
Industry should increase awareness to home users of threats.	2.37	1.08	27
Industry to do their part, training employees and create suitable 'usage' policies with regard to email/web traffic.	2.28	1.17	25
Prosecute offenders, enforce harsher penalties.	2.12	1.14	26
Industry should attempt to understand and comply with relevant guidelines and standards (e.g. ISO 17799).	2.05	0.74	21
Educate end-users. Insecure residential machines are going to be the biggest problem for the next few years.	2.00	1.14	27
Regulators (e.g. FSA) should make information security requirements explicit within regulations.	2.00	0.97	20
Take cases involving new technologies to court to establish precedents.	1.88	0.91	26
Amend Computer Misuse Act to ensure that identified classes of potential criminal activity are offences: presently neither denial of service nor unauthorised activities by authorised persons' are easy to deal with.	1.88	0.99	24
Government should Issue guidance on risks and protection measures to all senior schools. Make this mandatory education in all IT training in senior schools.	1.77	0.82	26
Organisations need an up-to-date security policy to facilitate communication with staff, customers, business partners and suppliers. Companies should perform regular system security audits.	1.70	0.82	27
Review legislation so that 'cybercrimes' are recognised and punishable (e.g. the Theft Act isn't strong enough). There must be no cyber safe havens or no-go areas.	1.56	0.89	27
UK government needs to provide leadership as recommended in the Burton Report.	1.45	0.69	11

*1=highest importance, 5=lowest importance

With or without adhering to externally recognised standards, the need for organisations to produce and ensure employee compliance with coherent security guidelines was repeatedly flagged, though again the need for security policies to be based on an informed risk assessment was made. Mere production of such policies is but a first step to compliance (Morris, 1994). Secure procedures can be detailed in security policies but also promoted via education and training, often in the form of formal guidance. As well as the workplace, the need for basic computing security awareness was raised in regard to children at school. Whilst this was generally supported, it was noted that such increased IT security education could also be used to educate potential young offenders. Finally, it was suggested that products, in this context normally software applications, should be accompanied by usage and configuration guides. It has, however, been pointed out that currently applications normally come with extensive documentation (physically or online) which is rarely fully consulted by the majority of users. Also, in some contexts, there is no best or recommended practice as products and services have to be configured purely on their specific application and integration with other system components.

Alerting conscience and controlling disinhibitors

The ‘alerting conscience’ technique is concerned specifically with “link[ing] conscience to a specific act to stimulate conscience at the specific point at which the offender may be contemplating action”. (Newman and Clarke, 2003: 133). Offline examples would include retail store signs with statements such as “We always prosecute shoplifters” or “Shoplifting is stealing”. Such measures are in contrast to a broader “battle for conscience that has been ‘neutralised’ by the culture of the Internet” (ibid.). Offline disinhibitors to illegal behaviour include alcohol, drugs and peer pressure. The ‘culture of the Internet’ referred to is broadly aligned to what is also known as the ‘hacker’s ethic’ (Furnell, Dowland and Sanders, 1999). The hacker ethic is a broad term alluding to an early, but still influential, Internet user culture that encompassed many elements but included a belief that information should be free, that the Internet should remain an essentially unregulated domain (by government or commerce) and free to explore (i.e. hack systems). More contemporary attitudes include a lack of respect for copyright as it pertains to software and other digital content such as music files, accompanied by a lack of triggers to prompt the user’s conscience. Such an ethos is considered a disinhibitor to normal social values which, in an offline context, would preclude individuals from stealing items from stores or entering private property.

One panel response, categorised as an attempt to control disinhibitors, was to suggest a public awareness campaign to inform individuals of the illegality of many activities despite their commonplace occurrence. The cited example was copyright abuse (e.g. music downloads) but other examples could include attempting to gain unauthorised access to a computer network (e.g. hacking) or the purchase of illegal items from overseas websites (e.g. cans of pepper spray). Another suggestion cited the formal promotion of cyberethics, cybercitizenship or netiquette. Such education can be promoted through various means, often in a multi-agency context. Existing formats include a website[28] or could be included in IT education classes for all ages. Other respondent contributions identified a number of influential educating roles. Parents and teachers were identified as educators for children (although this of course assumes that parents and teachers have a greater awareness of the issues than their young wards). Other institutions such as libraries which often offer public Internet access, also serve a source of basic education classes which could include computer literacy. Not mentioned by the panel, but comparable in function could be other institutions such as youth and adult drop-in/outreach centres, youth clubs and other educational institutions for all ages.

One suggested means of raising awareness was to include an examination of illegal activity in IT courses at all levels. Other respondents, however, believed awareness resources should focus on warning potential victims rather than dissuading potential offenders. Alternatively still, others believed more convictions for online offences would generate sufficient publicity which, by proxy, would generate an awareness of what is illegal online. Such awareness campaigns could highlight the potential impact of large-scale piracy such as the negative economic impact on the owners of the intellectual property pirated (e.g. companies could fail, jobs could be lost), alongside considerations of honesty and fairness.

[28] An example is the Cybercitizenship programme in the US www.cybercitizenship.org.

Table 3.8: Panel responses: alerting conscience and controlling disinhibitors techniques

Response item	Rating*	SD	N=
Public awareness campaigns on the consequences of committing criminal offences over the Internet. Intellectual property right owners to engage in long-term education/awareness programmes.	2.22	1.05	27
Government should educate citizens on e-crime prevention and response and highlight potential threat areas. Target young children and upwards. e.g. the Justice Department and the Information Technology Association of America cyber ethics programme.	2.12	1.03	26

*1=highest importance, 5=lowest importance

Newman and Clarke (2003) specifically identify three types of situational precipitators of crime: *prompt* (or provoke), *permit* and *pressure* (see also Wortley, 2001). Online examples of cues that may prompt hacker activity, particularly amongst young individuals, may include sensationalistic media portrayals of hacking in films, drama and the fame accorded to real life convicted hackers. The free availability of tools and guidance on how to hack a network, write a virus or download non-copyrighted music, permit and empower individuals to offend. For some individuals, particularly teenagers, the drive to belong and achieve status amongst a peer group may pressure them to offend, achieving 'bragging rights' through successful website hacks or other illegal activity.

Assigning responsibility

In considering the technique of 'rule setting' and 'alerting conscience and controlling disinhibitors' the legal and even moral ambiguity of much action is discussed. Tackling such ambiguity involves not only establishing statutes, rules, standards and ethics, but assigning such instruments to relevant parties to ensure their adequate implementation. The complexity of such a task has also been alluded to given the global and complex nature of the Internet. Discussion of the previous fourteen techniques has indirectly suggested a number of measures and those responsible for their ownership, but Newman and Clarke, along with the research panel make a number of direct recommendations regarding individual users, organisational users, service providers, vendors and so forth.

Table 3.9: Panel responses: assigning responsibility techniques

Response item	Rating*	SD	N=
Sanctions against corporations if appropriate protective and remedial measures are not taken. Have procedures to ensure compliance with data protection and other relevant regulatory requirements.	2.69	1.09	26
There needs to be a mindset change, from "I will assist investigations if I have to" to "I am keen and ever ready to assist investigations" on the part of ISPs and CSPs.	2.50	1.39	26
Pressure/legislation on ISPs to improve services that enable counter-measures to be taken, such as reverse DNS, and anti-IP spoofing measures.	2.43	1.27	23
IT users need to accept some responsibility for security issues, i.e. precautions in using credit cards, have a firewall, anti virus programme etc.	2.19	1.14	27

*1=highest importance, 5=lowest importance

The need for individual users to take measures to protect themselves was a priority for the panel. Such a belief echoes wider crime prevention measures in a variety of contexts from burglary to vehicle crime. Such action needs to be risk-based, founded on an awareness of the potential dangers faced and how they are avoided. In considering how to ensure organisations took adequate protective measures to safeguard their systems, the use of unspecified sanctions was suggested. Although there was some support for such an approach, in viewing IT security as a reasonable element of general corporate governance, such sanctions would require the definition of minimum security criteria, a potentially complex measure to achieve consensus on.[29] Issues of enforcement and sanction have to then be considered. Some respondents felt that the adequacy of organisations' security measures should be left to market forces, organisations that contributed to the critical national infrastructure considered a possible exception. The reliance on market forces infers that such organisations would lose customers, but this assumes that customers were

[29] However it is noted that legislation such as the seventh principle of the Data Protection Act 1998 adopts the unspecified term 'appropriate' when discussing the need for protective measures.

adequately aware of such security issues to differentiate between competing service providers, and poor security may only become apparent after an incident which may be too late for affected customers.

Moving beyond individual and organisational users, Internet Service Providers were targeted for taking more responsibility in countering various criminal and malicious activity over their network or other services they provide. Although there was general support in encouraging Internet Service Providers to facilitate various technical counter-measures, there was less consensus on whether Internet Service Providers should be held accountable for the actions of some of their users. Comparisons were made with the lack of responsibility faced by the manufacturers of fast cars involved in accidents due to their misuse by users. This is a debate that has been ongoing for some time and was perhaps first seen when Internet Service Providers were called upon to remove paedophile newsgroups. Similarly, one panel response called for greater co-operation from Internet Service Providers with law enforcement bodies, though a number of panel comments were favourable to current levels of co-operation. Others noted that such assistance would always be behind the need for such commercial organisations to focus on business issues rather than law enforcement requirements.

Facilitating compliance

To encourage users not to commit certain offences or other negative actions sometimes requires an understanding of what drives their behaviour. In considering the unlawful copying of some software, facilitating the back-up and restoration of the user’s software may reduce the perceived need for such illegal copying (Newman and Clarke, 2003). Kite mark or similar accreditation schemes may similarly enable and encourage online consumers to avoid merchants who trade in illegal products or services.

Specific suggestions for facilitating compliance in a target hardening context include government distribution of ‘protective software’ (e.g. anti-virus and maybe a basic firewall) to users who wish to use online government services. To help secure government networks, such measures may be made mandatory, which, unless provided by a government agency, could serve as a barrier to the public using such services if they failed to purchase such applications. Other suggested means of facilitating target hardening compliance was to improve the means by which users are kept informed of threats. Numerous sources do currently exist but some respondents felt a less technical approach was required for novice users and a single source of reference could also be convenient. Some panel members questioned if such measures would still get users attention, pointing out that perhaps the most inexperienced of users should simply be issued with ‘fixes’ rather than alerts as they would be unwilling and/or incapable of responding to even simplified warnings. Such an automated ‘patch and fix’ approach is now an option on one leading computer operating system, though this is perhaps only currently applicable to individual or small systems. For those with larger or more critical computer systems, particularly small businesses and upwards, it was suggested the availability of government-accredited IT security advisors would help promote good practice. Respondents, however, pointed out that a number of established certification schemes existed.

Table 3.10: Panel responses: facilitating compliance techniques

Response item	Rating	SD	N=
Provide a central public attack warning notice when incidents are expected.	2.96	1.24	25
Government to accredit independent advisors for the prevention of computer related incidents.	2.96	1.20	24
CESG and the Office of the e-Envoy should be funded to distribute free protective software to 'e-citizens' who are going to engage in online government transactions, so that perimeter defence includes end-users.	2.86	1.39	22
Global security alerts from credible source … CERT is okay but only addresses technical community.	2.70	1.03	20

Removing excuses recommendations

26. A broad government ‘safe and legal surf’ awareness campaign needs to be instigated to ensure online users are aware of basic security measures and the penalties for commonplace but illegal activity such as piracy and unauthorised system access. Specific attention to be given to educating children at school.
27. Providers of online services, which involve sensitive information, should provide suitable secure practice guidance for users.
28. All organisations need a risk-based IT security policy, thoroughly communicated to all staff.
29. Government should do more to promote the ISO 17799 IT security standard.
30. Government should facilitate the securing of the computer of online government service users through the provision of free software or other means.

4. Summary conclusions and recommendations

In discussing the suggestions and thoughts of the expert panel, two frames of reference have been adopted, mirroring to what extent the comments related to law enforcement activity or the wider community of interested and responsible parties. Figure 4.1 summarises the final thirty recommendations outlined in Chapters 2 and 3. Each proposal is positioned in regard to its emphasis on the four situational crime prevention categories: increasing the perceived effort for offenders; increasing the perceived risk to offenders; reducing the anticipated reward to the offender; and removing excuses.

Starting with prevention measures, tackling much netcrime involves established concepts: build it secure, educate users to operate it secure, and where appropriate, encourage high risk users to invest in matching preventive measures. This simple message, aimed largely at manufacturers and service providers, has been applied to many offline crime phenomena with good effect (e.g. vehicle crime). Moving from the target to the offender, measures to remove or restrict the resources at their disposal can be taken, again an established practice. Both sets of intervention will help increase the effort required by the criminals in going about much of their offending.

A large number of law enforcement-oriented measures may be considered to impact both the effort required from, and the risk of detection to, offenders. Informed investigation management, coupled with improved forensic capability, will require offenders to increase the sophistication of their offending (hacking a network is one thing, covering your tracks so no one knows it has been hacked, or how, is a lot more difficult) and their forensic awareness to avoid investigation detection (hackers or holders of illegal content will have to be more sophisticated in how they ‘clean’ their computers to remove incriminating evidence). National, and international, cross-sector forums will facilitate the sharing of information to assist all parties to harden systems, detect incidents and track offenders. Similarly, private sector law enforcement can assist such efforts by providing specialist knowledge, and often, technical and human resources.

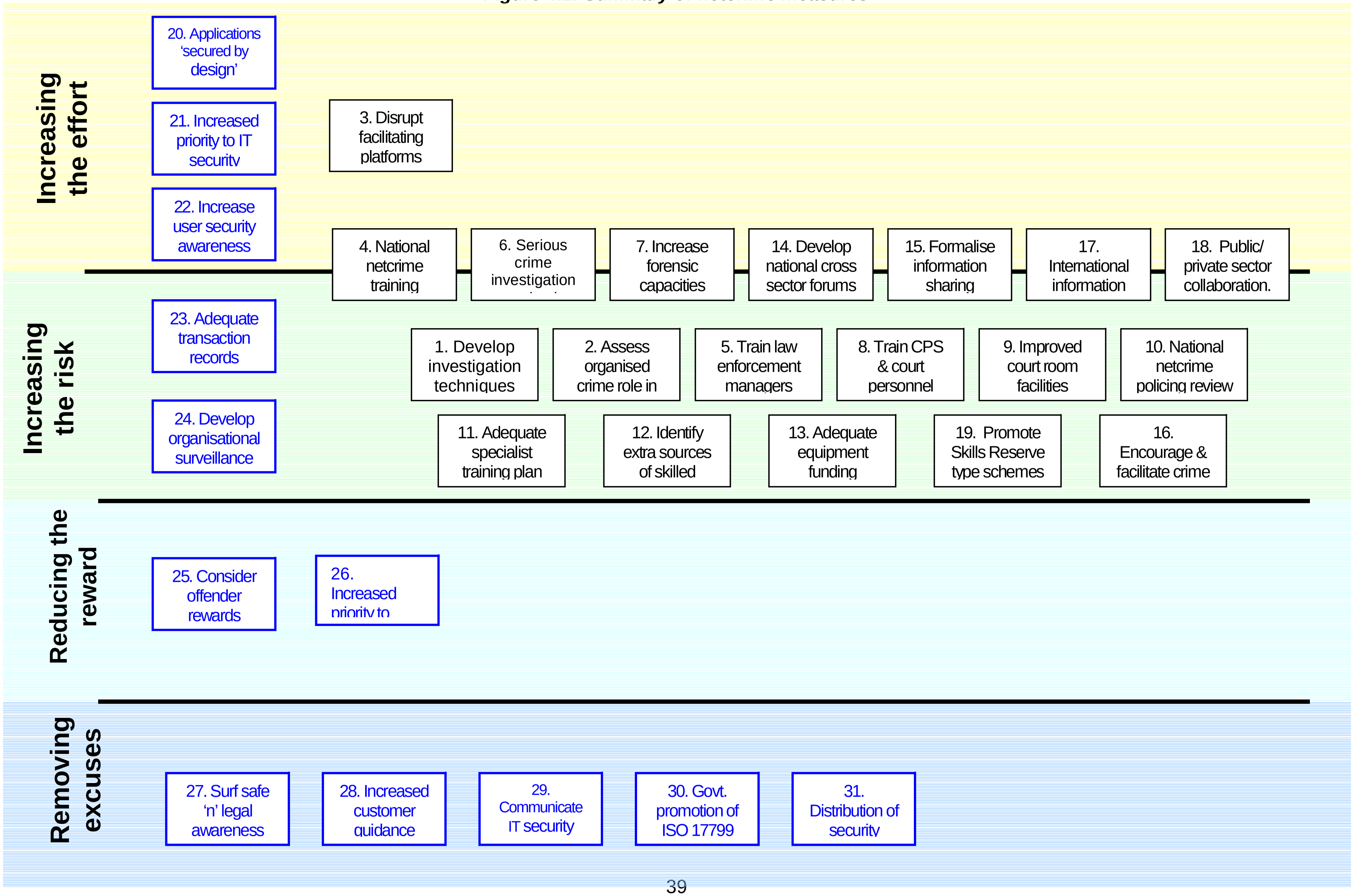
A number of law enforcement measures could improve investigative and intelligence gathering capabilities, increasing the risk to offenders of detection, disruption and arrest. A number of recommendations focus on the continual need for adequate training and resourcing of officers in this area, a request mirrored by almost all police teams. Such resources and training at the local level need to be provided in a strategic framework to ensure good and consistent operational practice between forces, and as much as possible, other agencies. Policing, in certain cases, may warrant the use of techniques deployed in serious crime cases, as netcrime investigation moves beyond its niche network investigation and forensic evidence recovery mode to a more aggressive but also mainstream role. As the final goal of many investigations is a conviction, then here also measures such as specialist training and, occasionally, the provision of the necessary equipment can increase the chances of a successful prosecution. Resources for the development, delivery and uptake of training and staffing is an issue for the Home Office, NSLEC, and ultimately, local forces. Other non-law enforcement-oriented measures to increase the risk to offenders include the detailed and long term holding of online transaction records for e-government services (so as to maintain evidence) and increasing the capacity for natural surveillance and incident reporting by users of various online services such as chat rooms. The former will assist post-offence investigations, whilst the latter measure will increase the chances of immediate intervention if criminal or malicious behaviour is occurring.

Despite all such measures it must be assumed that incidents will continue to succeed and such eventualities should be planned for. Where defensive network hardening measures are overcome, then continuity plans are essential to re-establish online service provision, whatever its role. As well as minimising the impact on service users, the display of such resilience will help reduce the planned benefit or reward to offenders, and may serve to dissuade further attacks once their reduced impact has been demonstrated. Such defensive measures must be implemented not just by industry, but also by central and local government.

Finally, a number of broad impact measures are proposed that serve also to assist a number of those already cited. Users need to change their behaviour in a number of ways, in regard to the adoption of secure, but also legal, practice. Despite the many calls for service providers and hardware manufacturers to make their services more secure, many security features and practices are not being utilised due to lack of user awareness, and perhaps the complexity of such features. In this respect users must accept responsibility for their own actions following adequate efforts to bring such issues to their attention by companies and public sector bodies. Similarly, following private and public sector awareness campaigns, users should increasingly be unable to plead ignorance for criminal acts (e.g. hacking, breaching copyright laws, attempting to purchase from overseas items banned in the UK). Organisations need also to increase their efforts to secure themselves against netcrime in all its forms. The government may contribute to this by promoting the BS7799 (now also known as ISO 17799) standard to appropriate categories of IT users, though this is a significant undertaking for small organisations. For individual home users, the government may directly contribute to hardening the outer perimeter of its own e-government services through the distribution of basic security measures to registered users.

Whilst each of the above recommendations individually contribute to one of the four crime prevention categories, the overlap and synergy between a number of them should not be missed. For example, to increase the security of its e-government online services (increasing the effort through target hardening), government agencies may demand that registered users have minimum safeguards such as up-to-date anti-virus protection and an active firewall (removing excuses through rule setting). However, to ensure such requirements do not become a barrier to the use of online government services, agencies may provide such defensive measures (removing excuses through facilitating compliance). Similarly an increased priority to security measures by an organisation (increasing the effort through target hardening) will require the establishment and implementation of a security policy (removing excuses through rule setting), which should lead to increased organisational user security awareness (increasing the effort through target hardening). Such plans should normally also include a consideration of continuity planning (reducing the reward through denying benefits).

Figure 4.1: Summary of netcrime measures


Increasing the effort
20. Applications 'secured by design'
21. Increased priority to IT security
22. Increase user security awareness
3. Disrupt facilitating platforms
4. National netcrime training
6. Serious crime investigation
7. Increase forensic capacities
14. Develop national cross sector forums
15. Formalise information sharing
17. International information
18. Public/ private sector collaboration.
Increasing the risk
23. Adequate transaction records
24. Develop organisational surveillance
1. Develop investigation techniques
2. Assess organised crime role in
5. Train law enforcement managers
8. Train CPS & court personnel
9. Improved court room facilities
10. National netcrime policing review
11. Adequate specialist training plan
12. Identify extra sources of skilled
13. Adequate equipment funding
19. Promote Skills Reserve type schemes
16. Encourage & facilitate crime
Reducing the reward
25. Consider offender rewards
26. Increased priority to
Removing excuses
27. Surf safe 'n' legal awareness
28. Increased customer guidance
29. Communicate IT security
30. Govt. promotion of ISO 17799
31. Distribution of security

Moving forward

The Delphi research identified a number of threats and challenges and this report has detailed the panel contributions on tackling such issues. However, the development of crime prevention measures and the criminal countermove has been described as a continual ‘arms race’ (Ekblom,1997) between those charged with securing assets and offenders. Similarly crime prevention or security measures can be seen as a depreciating asset and thus any recommendations in this report can potentially be seen in this context. However, most of the recommendations have been articulated to address fundamental issues or approaches to crime problems. Law enforcement agencies are familiar with the continual struggle to keep up to date with new technology, as embodied by the Police Science and Technology Strategy. Hence the call here is for the tackling of netcrime to be moved, over time, from being seen as a single specialist policing capability to an element of mainstream capabilities. Discussing the research findings using the whole of the Police Science and Technology Strategy framework has gone some way to illustrate this. Similarly, by discussing the research in established crime prevention terms of the situational model, netcrime can break out from its criminological niche, and be seen as a problem that is permeating mainstream criminal activity. Thus those tackling other offences, through various roles, must accept and indeed explore the implications of netcrime for their own area of responsibility, rather than dismiss it as the responsibility of the computer crime or IT security community. Almost all parties involved in tackling crime must recognise that they are now, or will very shortly, be faced with some form of netcrime and it is not going to disappear. Indeed, it is suggested that future efforts in this area should take the form of the development of a ‘future scanning’ capability. Central government has undertaken a number of large-scale initiatives in this area under the auspices of the Foresight[30] programme, whilst the Home Office is conducting similar focused reviews. Such exercises are perhaps best undertaken at a localised level where they may be focused on the environmental and organisational specifics of the organisation undertaking the scanning exercise. This is in contrast to the high level but broad questions behind this research. Such activity should not be seen as a one-off exercise, but a permanent and ongoing task, affirming that the challenges of netcrime are not transitory, waiting to be ‘solved’ with the emergence of yet more new technology. Rather, the day-to-day criminal challenges facing us all have gained another element.

[30] www.foresight.gov.uk

Appendix C: Acknowledged panel participants

The following participants completed all rounds of the survey and agreed to be cited, whilst a number of additional participants declined to be acknowledged. Thanks goes also to other participants who completed a number, but not all rounds of the survey.

J Ames, Home Office

Peter Anaman, Business Software Alliance

Dr. Andrew Blyth, University of Glamorgan

Paul Brennan, Federation Against Software Theft

Bruno Brunskill, Anite Public Sector

Martin Carden, NTL

John Carr, NCH

Richard Clayton, University of Cambridge

Andrew Cormack, UKERNA

Geoff Fellows, Northamptonshire Police

Dr. Steve Furnell, University of Plymouth

Riten Gohil, APACS

Mike Haley, Office of Fair Trading

Clive Hawkswood, Department for Culture, Media and Sport

Ian Hodges, HM Customs & Excise

Simon Janes, Ibas Computer Forensics

Tony Lever, BT

John MacGowan, Consultant

Dr Allyson MacVean, Buckinghamshire Chilterns University College

Dr. Frank Marsh, British American Tobacco plc

Vijay Mistry, National Hi-Tech Crime Unit

Michael A. Penhallurick, South Yorkshire Police

Steven Philippsohn, Philippsohn Crawfords Berwald

Andrew Powell, National Infrastructure Security Co-ordination Centre

Peter Robbins QPM, Internet Watch Foundation

Dr L.W. Russell, Forensic Science Service

Peter Sommer, London School of Economics

Richard Starnes, Cable and Wireless

Professor Michael Walker, Vodafone Group Services & Royal Holloway, University of London

Graham Walsh, Federation Against Copyright Theft Ltd

Jeff Yan, University of Cambridge

Peter Yapp, Control Risks Group

References

Casey, E. (2000) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* Academic Press.

Cornish, D.B. and Clarke, R.V. (2003) Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention, in Smith, M. and Cornish, D.B. (eds.), Theory for Situational Crime Prevention, *Crime Prevention Studies*, vol.16. Monsey, New York: Criminal Justice Press.

Coutorie, L. E. (1995) The Future of High Technology Crime: A Parallel Delphi Study *Journal of Criminal Justice,* Vol. 23, No. 1, pp.13-27.

Ekblom, P. (1997) Gearing Up Against Crime: a Dynamic Framework to Help Designers Keep up with the Adaptive Criminal in a Changing World *International Journal of Risk, Security and Crime Prevention*, October, Vol 2/4:249-265. Available also at http://www.homeoffice.gov.uk/rds/pdfs/risk.pdf

Ekblom, P. and Tilley, N. (2000) Going Equipped: Criminology, Situational Crime Prevention and the Resourceful Offender. *British Journal of Criminology*, Volume 40, No 3.

Furnell, S.M., Dowland, P.S. and Sanders, P.W. (1999) Dissecting the "Hacker Manifesto" *Information Management & Computer Security* 7/2, 69-75.

Johnston, J., Eloff, J.H.P. and Labuschange, L. (2003) Security and human computer interfaces, *Computers and Security*, Vol.22, No.8, 675-684.

Hyde-Bales, K., Morris, S. and Charlton, A. (2004) *The Policing Recording of Computer Crime* Development and Practitioner Report 40, London: Home Office.

Lang, T. (1995) An Overview of Four Futures Methodologies, *Manoa Journal of Fried and Half-Fried Ideas*, Volume Seven: Occasional Paper Seven, August Hawaii Research Center for Future Studies.

McGraw, G. (2002) On Bricks and Walls: Why Building Secure Software is Hard. *Computers and Security*, Volume 21, No. 3, 229-238.

Mann and Sutton (1998) NetCrime: More Change in the Organisation of Thieving *British Journal of Criminology*, Vol.38, No.2. Spring.

Morris, S. (1994) Security implementation in a computer environment: people not products, in *Crime at Work: Studies in Security and Crime Prevention Volume I* Gill, M. (Ed.) Perpetuity Press: Leicester.

Morris, S. (1996) *Policing Problem Housing Estates*. London: Home Office.

Morris, S. (2004) *The future of netcrime now: Part 1 – threats and challenges* Online Report 62/04 London: Home Office.

NCIS (2003) *National Criminal Intelligence Service 2003 UK Threat Assessment*, Section 8.3.

NISCC (2002) *National Infrastructure Security Co-ordination Centre*, public briefing document. See also http://www.niscc.gov.uk/cni/index.htm

Newman, R. and Clarke, R.V. (2003) *Superhighway Robbery, Preventing e-commerce crime* Portland: Willan Publishing.

Ofcom (2004)
http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/int_bband_updt/may2004/?a=87101

Power, R. (2000) *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*. Indiana: QUE Corporation.

Preble, J. (1983) Public Sector Use of the Delphi Technique in *Technological Forecasting and Social Change* Vol 23, pp 75-88.

Tafoya, W.L. (1986) *A Delphi forecast of the future of law enforcement*. Unpublished doctoral dissertation, The University of Maryland.

Wortley, R. (2001) A classification of techniques for controlling situational precipitators of crime *Security Journal,* 14 (4), 63-82.

Woudenberg, F. (1991) An Evaluation of Delphi *Technological Forecasting and Social Change* 40, 131-150.

Produced by the Research Development and Statistics Directorate, Home Office

This document is available only in Adobe Portable Document Format (**PDF**) through the RDS website

Home Office
Research, Development and Statistics Directorate
Communication Development Unit
Email: publications.rds@homeoffice.gsi.gov.uk

ISBN 1 84473 499 4