Australian Government
Australian Institute of Criminology

Future directions in technology-enabled crime: 2007–09

Kim-Kwang Raymond Choo

Russell G Smith

Rob McCusker

Research and Public Policy Series

No. 78

Future directions in technology-enabled crime: 2007–09

Kim-Kwang Raymond Choo
Russell G Smith
Rob McCusker

Research and Public Policy Series

No. 78

Australian Government

Australian Institute of Criminology

ISSN 1326-6004
ISBN 978 1 921185 44 1

Project no. 0074a

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9272
Fax: (02) 6260 9293
Email: front.desk@aic.gov.au
Website: http://www.aic.gov.au

Edited by the Australian Institute of Criminology
Typeset by CRE8IVE

A full list of publications in the Research and Public Policy Series can be found on the Australian Institute of Criminology website at **http://www.aic.gov.au**

Director's introduction

In September 2003, the Australian Institute of Criminology was engaged to undertake research services for the then newly-established Australian High Tech Crime Centre. The Centre is an internationally innovative approach to policing cyberspace where computer forensic specialists from state and territory police, government agencies, and the private sector work together in partnership with the Australian Federal Police to respond to the ever-expanding risks of technology-enabled crime.

The present report brings together a number of aspects of the research which the Institute undertook for the Centre. Its aim was to identify the crime risks which will arise over the next two years (2007–09) out of the environment in which Australians use information and communications technologies. Particular focus was placed on the impact these future developments will have for law enforcement in terms of creating needs for additional resources, law reform, the development of cooperative arrangements between Australian and overseas public and private sector organisations, and the creation and dissemination of public information and educational resources to minimise the risk of widespread harm to the community.

The report begins by identifying developments that will take place over the next two years that will be likely to facilitate technology-enabled crime. These include:

- changes arising from globalisation of business and the emergence of new economies in China and India
- developments in digitisation of information, especially relating to the widespread use of broadband services and mobile and wireless technologies
- the evolution of electronic payment systems, especially those being used in connection with online gaming and auctions
- changes in the use governments make of technology to allow members of the public to conduct transactions with government agencies securely and even to allow participation in democracy online.

These, and other developments, create not only benefits for the community but also risks. This report identifies the most likely areas in which opportunities for illegality may arise including fraud, identity-related crime, computer vandalism, theft of information, dissemination of objectionable material online, and risks of organised crime and terrorism.

The implications of these developments are then assessed in terms of their impact for policing, policy making and legislation. Suggestions are also made for responding effectively to these developments – a task that will entail close cooperation between government and those involved in developing new digital technologies and creating the infrastructure in which they operate. The solution to technology-enabled crime in the ensuing years will require government and business to be able to predict confidently how technological innovations will be misused by criminals, and to develop responses that will neutralise such opportunities before they arise. The present report should be invaluable in this.

Not everyone will agree with our predicted course of events. We hope, however, that the proposed opportunities for crime reduction and reform will be addressed and prove to be effective in preventing many of the risks of technology-enabled crime which we have suggested might occur in the future.

Toni Makkai
Director
Australian Institute of Criminology

Contents

Acknowledgments

This report was prepared with input from

- Professor Roderic Broadhurst and Dr Nicholas Chantler (Queensland University of Technology)
- Dr Tony Krone and Dr Gregor Urbas (former research analysts at the Australian Institute of Criminology)
- Dr Shane McKenzie (Victoria Police Computer Crime Squad).

It is based on research funded by the Australian High Tech Crime Centre.

We would also like to thank staff at Australian High Tech Crime Centre and Dr Judy Putt for comments on earlier drafts.

The permission of the Economist Intelligence Unit (Table 3) and the National Institute of Standards and Technology (Figure 3) for use of their material is acknowledged.

Disclaimer

The views expressed do not necessarily represent the policies of the Australian Government or the Australian High Tech Crime Centre.

Glossary

AJAX	Asynchronous JavaScript and extensible markup language
EMP	Electro magnetic pulse
FBI	Federal Bureau of Investigation (US)
IC3	Internet Crime Complaint Center (US)
ICT	Information and communications technologies
IFTI	International funds transfer instructions
IP	Intellectual property
ISP	Internet service provider
IT	Information technology
IRC	Internet relay chat
MEMS	Micro-electromechanical systems
MMOG	Massively multiplayer online games
MMORPG	Massively multiplayer online role-playing games
MMS	Multimedia messaging services
PDA	Personal digital assistant
RFID	Radio frequency identification
SMS	Short message service
VoIP	Voice-over-Internet Protocol

Executive summary

This report examines the future environment in which Australians will use information and communications technologies (ICT) and how this environment will provide opportunities for illegality and infringement of current regulatory controls. In identifying future risk areas, particular focus is placed on the impact these will have for law enforcement, the need for additional resources, law reform, development of cooperative arrangements between Australian and overseas public and private sector organisations, and development of public information and educational resources to minimise the risk of widespread harm to the community.

This report principally adopts the term 'technology-enabled crime' to refer to crimes which require the use of ICT for their commission. Where more specific forms of technology-enabled crime are discussed, terms including 'cybercrime', 'cyberstalking' and so on are used in conformity with Australian legislation such as the *Cybercrime Act 2001* (Cth) and international instruments such as the Council of Europe Convention on Cybercrime. These types of crime are likely to continue to develop over the next two years, the period that constitutes the focus of this assessment. In this report, the term 'organised criminal' refers to criminals or cybercriminals who are involved in the use of an organisational structure to pursue illegitimate goals.

Developments that may facilitate technology-enabled crime

Globalisation and emerging economies

Developments in ICT now greatly facilitate commerce between developed countries and newly emerging economies such as India and China. Although these new economies are developing quickly, their information security environment is less well developed, as is their legal and ICT policy environment. These differences are likely to create an environment in which technology-enabled crime directed at Australian organisations may emanate from, or make use of, security weaknesses in organisations in developing countries with which Australian organisations and individuals deal.

Threats to information and communications infrastructure could also arise from accidental causes and natural disasters, such as the earthquake in Taiwan on 26 December 2006 that disrupted telephone and internet services throughout Asia.

Electronic commerce (e-commerce) is likely to continue to grow in volume and sophistication given that the increased speed in connection and movement of data between computers will permit anyone to create an online business and/or to become an online consumer. The digital divide that exists between developed and developing countries will continue to create crime risks as those countries with poorer critical infrastructure may be driven, by globalisation demands, to engage with other countries while not having adequate technology-based security measures in place.

A further risk associated with globalisation is that of offenders ‘jurisdiction-shopping’. Trends in technology-enabled crime have shown that attacks are increasingly originating from regions such as Eastern Europe and Asia where sanctions are often more lenient and enforcement less robust. Australia has a relatively comprehensive legislative framework in place to deal with technology-enabled crime but, until the process of harmonisation of laws and sanctions is more advanced, disparities between countries will continue to create risks.

The growing acceptance of the internet as a communication tool and the tendency of corporations to locate their operations in developing countries where cheaper labour costs are present have resulted in an increasing number of outsourced operations being conducted offshore. Offshore outsourcing, particularly to lower-cost countries, is likely to increase in the next two years. In fact, it has been predicted that more than 3.4 million service sector and IT jobs in the United States are likely to be located offshore by the end of 2015. United States government spending on outsourced IT functions is also predicted to increase to US$17.4 billion in 2009. Global outsourcing trends beyond the next two years will also include computer game development that will be increasingly outsourced to studios around the world that specialise in specific aspects of games creation, such as cinematic, full-motion video and motion capture.

Outsourcing involves the transfer of a considerable amount of management control to offshore vendors that usually results in diminished control over security arrangements. It is also possible that vulnerabilities will be clandestinely introduced into software developed offshore (by corrupt offshore employees or foreign intelligence agents) and for loss or misappropriation of intellectual property rights to occur, particularly in countries with inadequate legal systems for protecting such rights.

To ensure regulatory compliance (e.g. proper data access, usage, storage, sharing, and transmission), protocols and legislation are needed to continuously monitor and to manage offshore vendors and their associated outsourcing relationships, perhaps through legally binding contractual arrangements, such as service level agreements and key performance indicators.

Developments in digitisation

The declining importance of dial-up connections and the expansion of broadband services have created an environment in which connections are maintained continually, providing greater opportunities for attacks against inadequately secured computers, particularly those in domestic situations, which may be compromised for use in botnets. The use of peer-to-peer file sharing programs or downloading files from unknown senders will also increase risks for domestic users. Rapid download times have facilitated dissemination of content, such as pornographic images and pirated software and music, particularly through peer-to-peer platforms and online content sharing websites that may also contain spyware.

Technology will become increasingly ubiquitous. Established technologies, such as mobile phones and computers, will continue to be widely used but there is likely to be a proliferation of auxiliary devices aimed at improving the performance and flexibility of those established products. There will also be an increasing convergence of technologies whereby a number of disparate goods and services may be coupled with information technology in the same way that mobile phones, for example, are currently capable of taking video footage and photographs and permitting access to the web.

The key threat emanating from the ubiquity and complexity of technology in an era of increasing connectivity will be viral contamination. This threat will be exacerbated by the reliance that businesses and individuals place upon technology to carry out their daily activities. Communication vehicles will increase exponentially and the danger of high-tech criminals breaching such communication conduits is likely to rise in tandem.

The technological capabilities of telecommunications devices will grow exponentially and it is inevitable that the benefits of such advances will be passed on to consumers. The process of disintermediation, currently experienced in areas such as banking (whereby physical contact between organisations and their clients is replaced by virtual contact), will extend to other business and social contexts. Disintermediation will increase given the plethora of wireless and mobile communication tools, such as personal digital assistants (PDAs) and wireless application protocol-enabled mobile phones. Businesses are becoming increasingly global and interconnected as they continue to engage in e-commerce. This will enhance the risks of identity-related financial crime through use of modern technology.

Although efforts are being made to ensure that new systems have appropriate security measures in place, risks will arise from users not having requisite levels of security awareness and not fully understanding how new security measures can be used to their advantage. Some new technologies may have effective security measures enabled, but consumers might not use them to full advantage. Wireless networks themselves create a number of vulnerabilities; key among these is that networks and their data can be accessed remotely without physical access being required. This facility assists both the user and the criminal.

The trend of workers becoming more mobile is likely to continue and consequently, mobile and wireless devices will become increasingly important tools for accessing information when desktop computers are unavailable. Mobile devices and networks including third- and fourth-generation networks, smart-phones and wireless PDAs, will continue to become more sophisticated and better able to support a wider range of communication and collaboration functions. Such devices will, however, continue to be used to store unencrypted personal data as well as corporate information. The ease with which erased data on such devices can be recovered increases their attractiveness to criminals. The advent of wireless networking increases the likelihood of such information and associated tools being uploaded and downloaded. New ways of abusing wireless and mobile devices to facilitate the commission of technology-enabled crime are likely to emerge.

Future technological innovations and the decline in prices of electronic data storage devices will continue to lower entry barriers for digitisation of information. Tomorrow's computing will see a combination of optical and silicon technologies to facilitate data transfer within chips via laser. Developments in nanoscience and nanoengineering will increase the use of micro-electromechanical systems that combine electrical and mechanical components to enhance information storage, processing and communication.

Networked technology will evolve through use of increasingly faster fibre optical systems that will improve transmission of data within and across networks. Mobile communications will be facilitated through a combination of low and high orbiting satellites; and the available frequency spectrum for digital exchange will increase through introduction of new compression methods for high-density data.

The exponential rise in information transfer and storage capacities will lead to enhancements in database technology which will improve the manner in which increasing volumes of data are categorised, stored and extracted. One important development will be the increase in the use of 'agile' databases in which large warehouses of data are drawn upon, as and when necessary, rather than being stored on discrete personal or business databases.

These developments will permit even greater access to the internet by individuals and organisations and enhanced use of communication vehicles such as email, instant messaging and high-speed connectivity. Emerging forms of modern day communication tools that allow internet users to disseminate and share information and ideas include:

- **Online chat rooms and social networking sites:** Popular online chat rooms and social networking sites such as Friendster and Myspace allow users to post their personal details and photographs and also to interact with other users in real-time. Information on such sites could be used to identify or profile a particular user and it has been known that malware authors exploit such sites to increase the yield of phishing attacks. Online sexual predators have also been known to make use of chat rooms. Personal information obtained from social networking sites could facilitate identity theft. Terrorists could use online chat rooms and social networking sites as vehicles to reach an international audience, solicit funding, recruit new members, and to distribute propaganda (internet-driven radicalisation).

- **Blogs (weblogs):** Various communities have emerged in the blogosphere ranging from technical support communities, such as Google™ blogs, to groups of bloggers who are opposed to other racist or extremist bloggers. Blogs can be abused to leak proprietary or confidential information and post defamatory and offensive content. There have been reported cases of employees losing their jobs for violating company policies when they posted information pertaining to their jobs on their blogs – an activity also known as 'dooce dodging'.
- **Online sharing websites (e.g. YouTube):** Law enforcement agencies have used YouTube as an investigative tool to disseminate information to the public and as a channel to bring matters of public interest to the attention of law enforcement agencies. However, online video sharing can be exploited as a means to distribute malicious code. Instead of embedding image spam in email, spammers could abuse online photo sharing sites by posting image spam on such sites and embedding the links to the posted image in the email.

Increasingly large amounts of data will be transmitted electronically, with data storage hardware becoming smaller and more portable. These developments will create risks for law enforcement in analysing computers forensically as well as providing enhanced avenues for theft of data by stealing hardware storage devices. Unless adequately protected through use of secure access codes and encryption, data leakage will be enhanced, creating risks for individuals, businesses and governments.

Payment and funds transfer systems

Continuing developments in electronic payment systems will create new risks of technology-enabled crime. Likely criminal threats in an environment in which internet International Funds Transfer Instructions (IFTIs) and e-currencies continue to grow arise from the fact that regulators are not capturing many electronic currency transactions, and that internet IFTIs may aid the money laundering process.

Risks will also arise if electronic purses and pre-paid card technologies continue to develop. The anonymity offered by pre-paid cards continues to act as a vehicle for facilitating illicit financial transactions, money laundering and bulk cash smuggling, particularly as value limits increase. The future will also see new hardware devices and software programs that seek to compromise the quality of data-protection mechanisms used in smartcards.

Advances in third- and fourth-generation wireless telephony that offer high-speed data access and widespread dissemination of Bluetooth-enabled mobile phones will increase the popularity of mobile payments and mobile gaming. Associated risks include the presence of fraudulent service charges (to both the carrier and to end users), the presence of malicious code, and wireless security threats.

Use of digital precious metals will increase as a means of transferring value online. User identification required for enrolment in such services can be easily fabricated and some digital precious metals allow users to establish anonymous accounts. As a result, it is likely that such systems will be used to facilitate money laundering and terrorist financing, perhaps with the assistance of an exchange agent such as shell corporations.

Online gaming such as massively multiplayer online games (MMOG) and massively multiplayer online role-playing games (MMORPG), typically played via local area networks and the internet, will remain popular with younger users. Virtual currency and goods gained while playing games can be converted into physical cash through exchange with or sale to other players. Players have also been known to purchase virtual properties, virtual accommodation and virtual merchandise or to inflate their virtual status using physical cash. The availability of a market in which to trade virtual goods for physical cash will provide criminals and hackers with financial incentives to commit crimes. The future will also see continued development of malicious code targeting the online gaming community such as:

- **'CopyBot'** that allows gamers to replicate virtual goods without paying the original designers
- **'grey goo'-type code** designed to self-replicate objects within the virtual world that might eventually cause a denial-of-service type attack
- **'Waigua'-type code** designed to carry out activities automatically on behalf of the players with the aim of increasing the levels of their characters.

Risks of money laundering will increase, as MMOG and MMORPG sites emerge as a potential vehicle for such activity online. For example, money launderers could purchase virtual currency using illicit cash and exchange the virtual currency back to physical cash. Existing avenues of money laundering such as online gambling, a multi-billion dollar industry, will continue to be used. Criminals will be able to establish online accounts with offshore casinos using stolen identities and illegally derived proceeds. To avoid detection, small numbers of transactions would be carried out and then requests made for repayment from offshore casinos. Although offshore casinos may not be required to maintain transaction records, payments can be deposited into bank accounts belonging to money mules to obfuscate the money trail.

e-Government

The Australian Government has resolved to implement a National Health and Social Services Access Card. Although not designed as a generalised identity card, the biometrically-enabled card will have widespread use and application, making it a likely target for criminals. Areas of risk will relate to dishonest initial enrolment of users as well as data insecurity, both with respect to the card's computer chip as well as supporting databases. Threats might also arise from organised criminal groups that seek to compromise the system's computer infrastructure, or others who seek to obtain personal information for use in identity-related crimes.

Traditional paper-based passports are also being replaced with radio frequency identification (RFID) enabled biometric passports (e-passports) conforming to International Civil Aviation Organization standards. Biometric passports are designed to provide strong authentication that unequivocally identifies the bearer. New hardware devices and software programs that seek to compromise the quality of data-protection mechanisms and supporting architecture, will include passport cloning, brute-force attacks on keys used for access control, and devising new ways of tracking and scanning covertly.

As applications of government issued smart technologies increase, risks will be enhanced, extending to systems used to facilitate new online services such as electronic voting in elections, electronic tendering and electronic democracy. Such applications would be attractive targets for groups wishing to disrupt or affect levels of confidence in government and businesses generally.

Risk areas and opportunities

Fraud and dishonesty

Globalisation and the new economy, enabled by the latest internet-based technologies and e-commerce, have created new and greater opportunities for criminals to commit fraud against both businesses and consumers. Computer-facilitated frauds include advanced fee scams, online auction frauds, fraudulent lottery schemes, modem and webpage hijacking and identity theft – amongst others. Major drivers having an impact on computer-facilitated frauds include the rapid expansion of the new and emerging technologies and the apparent ease of committing consumer fraud.

Several search engines and online sites are supported either in part or in full by pay-per-click advertising revenue models. In such revenue models, advertisers are charged based on the click-through rate of an advertisement. However, malicious hosting sites could abuse such a revenue mechanism. Click frauds have been identified as an emerging threat to e-commerce. In fact, some commentators have suggested companies should view click fraud as another business tax. Despite efforts to improve click fraud identification techniques and raise the entry barrier for fraudsters, financially motivated criminals and malware authors will continue to design malware that seeks to circumvent existing measures.

Online auction sites, providing buyers and sellers with a global virtual market and storefront at which to buy and sell a wide range of merchandise through competitive bidding, constitute one of the most successful internet-based business models. Crimes associated with online auctions, particularly online auction frauds, are likely to increase. Criminals and malware authors will continue to design malware that seeks to circumvent existing anti-fraud measures for illicit financial gain.

Phishing attacks will become more sophisticated and the number of such attacks will increase. Dissemination of spam will be facilitated not only through use of botnets, but also voice over internet protocols (VoIP) – known as Vishing – and mobile phones (via short message service – SMS) – known as SMiShing – which will be used to overcome spam-prevention and detection filtering software. The future will see an increase in persistent attacks using redirection or malware techniques that trap unwary internet users. Developments in technical attacks, such as animated images, pose a growing challenge as these are often more persistent and difficult to detect.

Another important threat to emerge will be the use of spoofed embedded links that look like links to the institution being impersonated but that lead to malicious sites. Some malicious sites may contain code that allows phishers to retrieve contextual information, such as sites visited from the browsers' cache. Such contextual information can be used to facilitate 'context aware phishing'. It is also likely that tools such as the 'Universal Man-in-the-Middle Phishing Kit' will be enhanced to include more sophisticated capabilities that seek to target two-factor authentication mechanisms, such as by subverting token-based logons, and acquiring and reusing one-time token data in real time. Although phishing attacks can be either syntactic – exploiting technical vulnerabilities – or semantic – exploiting social vulnerabilities, the future will see a continuing movement from syntactic attacks to semantic attacks. It is known that phishing attacks have been facilitated by publicly available personal information from social networks such as Myspace and Friendster.

Faced with these potential developments, the design of effective policies and strategies to combat consumer fraud will become more problematic. When coupled with the complexities associated with apprehending suspects, obtaining convictions and imposing sizeable penalties, the deterrent effect of the law will remain limited. Reduced deterrence may also increase the likelihood that re-offending will occur.

Unauthorised access

As measures employed by organisations to identify users of systems improve, criminals will seek to gain access to computers and networks in order to disable security and alarm systems or design malware programs to circumvent existing security controls.

Criminals will continue to employ semantic outsider attacks, committed through social engineering, to gain access to computers and networks. Social engineering involves the use of psychological tricks to manipulate human behaviour, often through deception of unsuspecting users, to gain access to information such as usernames and passwords, personal identification numbers, tokens and credit card information. Once offenders have gained access to systems they are able to erase, modify or copy the information to suit the needs of their attack.

Insider threats can be further divided into two categories: threats of insider attack on behalf of, and controlled by, an outsider; and self-motivated insider attacks. As critical systems are increasingly dependent on software and are connected to the internet, insider threats belonging to the first category will be of ongoing concern. Corrupt insiders could deliberately introduce vulnerabilities during the coding of in-house software that is used to manage sensitive military or intelligence networks. This could allow terrorists or foreign intelligence agents to exploit the vulnerabilities and surreptitiously enter systems, gain control, and launch online attacks via and against compromised systems.

With advances in communications technologies, there will be more avenues for insiders to leak sensitive documents or information. An example is the Wikileaks.org website that is designed for whistleblowers in authoritarian countries to post sensitive documents on the internet without being traced. The anonymity feature is provided with use of The Onion Router, an ‘anonymising protocol’ that allows data to be routed through a network of servers. The latter uses cryptography to further obscure the data path and hence make it untraceable.

Although organisations will continue to build a culture of vigilance to maximise the chances of detection of insider threat, the latter will continue to constitute a separate category of threats against the integrity, privacy and availability of computer systems and networks in the next two years. Perimeter security and network security in isolation are insufficient to counter insider threats. Efforts must also be taken to protect information and data in storage and in transit.

As methods of user authentication are enhanced, risks of crime displacement will increase. Use of multi-factor card authentication and biometrically-enabled systems will result in offenders employing a range of alternative strategies to obtain access to computers and funds. The use of violence, duress, bribery and corruption are the likely areas of concern for the future as criminals seek to circumvent digital identification systems. As information security increases, risks of insiders collaborating with external offenders, or becoming offenders themselves are likely to increase. This will require organisations to use more extensive and intensive personnel checks to monitor the activities of existing staff and to verify the credentials and backgrounds of new staff.

Malware

The development and use of malware is also likely to continue over the next two years, particularly through the exploitation of social vulnerabilities and the use of blended attacks. Malware authors will continue to explore ways in which to deny or delay victims’ access to information regarding the source or nature of malware infection. The availability of a market in which to sell malware provides criminals with more financial incentives to offend. The future will see the following trends emerge:

- Continued development of malware, such as viruses, worms and Trojans that will employ self-modifying (or self-mutating) code. This will allow malware to automatically inject random pieces of code such as Trojan program code before compilation and compression to create separate variants, and will enable code-obfuscation to occur in order to elude detection by antivirus and anti-malware products.
- Continuing availability of a market for the sale of malware such as password stealers and related Trojans and file infectors. These include password-stealing websites using fake sign-in pages and subscription-based services for malware updates (similar to the current subscription-based service offered by anti-virus software).
- Continuing enhancement of other stealth techniques to hide files, processes or registry values belonging to the malware such as installing an Application Program Interface that hooks into running processes or changes system APIs.

Examples of evolving malware include bot malware, kernel-mode malware and malware that exploits internet browsers and web services. Other stealth techniques will continued to be enhanced.

The level of sophistication of bot malware (and zombies) has increased considerably and will continue to do so in the next two years. New classes of bot malware that aim to elude detection by antivirus software will appear. Malware that exploits portable executable packers – originally designed to reduce the size of an executable on disk through compression – will also emerge.

Kernel-mode malware executes as part of the computer's operating system and has full access to the computer's resources. Unfortunately, it is hard to detect. Several working prototypes of kernel-mode malware and hypervisor have been identified as a risk. Although kernel-mode malware has yet to become popular, threats from kernel-mode malware are likely to increase.

Application of cryptographic tools and techniques to enhance new malware attacks will increase. One example is the ransomware program that cybercriminals often use to search for data on compromised systems. This activity is also termed cryptovirology or denial-of-resources attacks. Although incidents involving ransomware have yet to become widespread, it is likely that ransomware attacks will become more targeted, such as against certain organisations and industries like banking and finance. They will also use more complex encryption functionality.

Internet browsers and web services will also be of interest to criminals and malware authors. Users' computers can be infected by malware when they visit compromised websites (by exploiting vulnerabilities of web servers or operating systems) that host malware. Malware authors will target vulnerabilities introduced by user-generated web content. Existing security measures, such as network-based firewalls, may not be able to prevent threats of unauthorised access to a web service. Future exploitation of internet browsers and web services to disseminate malware will include design of malware to hide browser attack codes, circumvent existing anti-malware products and mix known exploit codes so they become unrecognisable to antivirus programs.

Intellectual property infringement

In today's knowledge-based economy, managing and protecting intellectual property (IP) has become one of the cornerstones of good corporate governance. Enhanced capacity of ICT systems will enable electronic products, such as songs and movies, to be copied and reverse engineered more quickly and easily than at present, thus giving rise to increased risk of counterfeiting and piracy. Electronic properties including video-on-demand; knowledge and information such as patents, copyrights and trademarks; and identity devices, such as biometric smartcards, will be the assets of interest for future criminals.

A secure legal environment is vital for protecting IP rights. It is, therefore, not surprising that transfer of technology to countries with less advanced IP protections as part of investment and outsourcing projects will increase the risk of counterfeiting, piracy, illegal transfer of technology and facilitation of industrial espionage. Increased use of open source or public domain software may, however, reduce the incidence of copyright infringement, as may the use of freeware and shareware. For the near future, however, criminal infringement of IP rights will remain of interest to law enforcement.

As digitisation continues to infiltrate all aspects of corporate life, a growing number of opportunities will arise for the commission of industrial espionage. Such attacks may use electronic surveillance and data capture technologies to steal commercial-in-confidence information, or may be directed at electronic IP such as trademarks or patents held electronically. Enhanced reverse engineering techniques (stripping down and analysing competitors' products) will also facilitate unauthorised access and exploitation of IP.

Criminals, competitors and foreign intelligence agents can also exploit commercial joint venture and offshore outsourcing relationships for financial gain. Risks of industrial espionage may also arise where confidential contractual negotiations are carried out using email and wireless communications that have not been encrypted or otherwise carried out over secure networks.

Offensive content

Affordable technology has greatly facilitated the production and distribution of child pornography – a multi-billion dollar industry globally. Although the level of knowledge of, and measures to combat, dissemination of child pornography and the sexual abuse of children has increased; individuals and groups of criminals will continue to use ICT to carry out such crimes. The use of ICT to carry out other related sexual abuses involving child victims are also likely to continue in the near future.

Offenders will continue to use cryptographic technologies to prevent detection and to enable images to be shared securely. This will increase the need for law enforcement to enhance its cryptanalysis, steganalysis, and data analysis and storage capabilities. It can also be expected that child exploitation will continue to involve the highly disturbing practice of live child sexual abuse videos being streamed to internet chat rooms, with the actual perpetrator responding in real time to commands from other participants who can see the images. Using the doctrine of constructive presence, it may be possible for such co-offenders to be prosecuted, not only in relation to child pornography distribution, but also as accomplices in sexual assault.

With the enactment of new federal offences dealing with child pornography and grooming, it is to be expected that a proportion of future prosecutions will rely on these offences rather than state and territory laws. Law enforcement authorities have, to date, been particularly focused on websites and internet service providers (ISPs) based in Australia that carry child pornography and child abuse material, although arrests for public order offences have also targeted the use of mobile phones and SMS to incite confrontations in public places. These types of acts can fall within the broad category of offences of using a carriage service to menace, harass or cause offence, where the offensiveness of material is to be assessed by 'the standards of morality, decency and propriety generally accepted by reasonable adults'. This provision may also extend to offensive website content such as racial vilification material. It is to be expected that the future will see an increased number of prosecutions for these various forms of content-related offences.

Exploitation of younger people

As increasingly younger people (the 'digital generation') make use of personal computers and mobile devices, risks may arise where inadequate security measures are in place to secure the technologies they use. Theft of laptops, USB drives, MP3 players and mobile phones from schools and entertainment venues will continue to create problems, not only in terms of replacement costs but also in relation to stolen personal information. Stolen personal and sensitive information will be used to facilitate other crimes such as identity theft and extortion. Online scams are also likely to target young users who may be less vigilant in detecting fraud than are adult users.

A new form of bullying, including harassment targeting young users, has emerged which makes use of communication technologies such as email, text messaging, chat rooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying will continue to be a problem. Victims may feel socially ineffective and, consequently, may experience greater interpersonal difficulties including a lowering of academic performance.

Organised crime

It is unlikely that traditional transnational organised crime groups will shy away from using the technology-enabled crime environment to facilitate and/or to disguise illicit proceeds of real world based crimes. The use, for example, of denial-of-service attacks to pursue extortion or the use of online banking to transfer laundered funds are both likely to continue. The development of traditional transnational organised crime groups into fully-fledged technology-enabled criminals will be determined as much by the diminished profitability, or increased risk, of real world criminal activities as it will by the innate attractiveness and relatively low risk of technology-enabled crimes. Organised operations that make use of conventional technology-enabled crime methodologies, such as financial scams or piracy, will also increase as the use of networked computers for criminal purposes develops.

Computers and computer networks will continue to be both the objects of terrorist attacks, and the conduit through which terrorists and other criminals will communicate in order to plan and carry out their destructive activities. Threats from (cyber) terrorism will carry serious economic and societal implications. Because many computer networks transcend international borders, it will increasingly become necessary for all countries to have adequate substantive and procedural laws, and to cooperate effectively in order to investigate, to prevent and to punish terrorist and other criminal activities perpetrated with the aid of computers and computer networks.

Threats to national information infrastructure

Tight couplings between different areas of critical infrastructure may result in rapid escalation of seemingly modest disruptions from within one sector to another. If unsecured sectors are successfully compromised, they can then be used as launching pads to attack other critical infrastructure sectors. Private companies responsible for the majority of the critical infrastructure are a major vector for cyber-terrorism and crime, although growing concern exists over networked computers in other contexts, such as households and educational institutions, due to the emergence of botnets and other network-oriented malware.
A successful attack on information technologies and communications infrastructure that supports many areas of critical infrastructure may disrupt supply chain management systems, financial sector networks or power grids. Consequences of these attacks

could continue to reverberate after the immediate damage has been done. Cross-sector interdependencies are of primary importance in securing critical infrastructure.

Specific examples of cyberterrorism activities are rare at present in Australia and internationally, although any instance of technology-enabled crime that exposes vulnerabilities in critical infrastructure security indicates the potential for a cyberterrorist attack. A further area of risk concerns planning of terrorist attacks that involve use of ICT. The continuing use of online resources to support terrorist incidents is an area of concern that is unlikely to diminish in the future.

Legal and evidentiary implications

Legislation

In Australia, the growing body of Commonwealth law relating to computer technology, particularly telecommunications systems is likely to increase. These laws operate alongside general criminal laws which are traditionally administered by the states and territories. Specific offences under other federal legislation dealing with such matters as IP rights, classification of publications, terrorism and national security are also likely to be subject to amendment over the next two years to deal with new technological developments and threats.

Although the process of harmonisation of cybercrime legislation throughout Australia has been proceeding, the need for uniformity will become more pronounced as the number of technology-enabled crimes continues to increase. In addition, existing offences, although technically adequate, may be practically impossible to use, such as occurs in the case of botnet-related crimes where evidence would need to be obtained concerning the thousands of computers that have been compromised. New offences of creating a network for illegal purposes and selling established botnets might need to be developed to deal with such emerging threats.

With the addition of Part 10.6 to the *Criminal Code Act 1995* (Cth), which contains offences prohibiting misuse of telecommunications networks for a range of illicit purposes, it can be expected that section 474.14 will largely displace the need to use previously enacted unauthorised access offences such as those in section 477.1. With these new telecommunications offences, it is also likely that Australian government agencies will assume a more dominant role in investigating and prosecuting technology-enabled crimes than was previously the case. Other offences in Part 10.6 are also capable of application to a range of conduct not previously covered by Commonwealth criminal law, such as child pornography, grooming, and racial vilification.

Installing programs that collect and send back information about internet usage (‘spyware’) is not currently criminalised in Australia. The enactment of legislation to proscribe the usage of spyware has been proposed and its application will need to be monitored to ensure it achieves its objective. In view of these changes, the need for additional resources by federal policing and prosecution agencies will become necessary in the next two years.

Criminal complicity

The future will see an increase in instances of individuals acting jointly in the commission of technology-enabled crime. Examples of potential accessories to such crimes include money mules; business employees who disclose passwords, security codes or database details to others and thereby intentionally or recklessly facilitate unauthorised access; members of hacker communities who share security information that allows others to obtain unauthorised access to computers or data; software 'crackers' who strip business or entertainment computer programs of their copyright and information management protections and distribute these through 'warez' websites; providers of illegal signal decoding hardware or similar circumvention devices that allow users to obtain unauthorised free access to subscription services such as pay television; creators and manipulators of malware such as viruses, worms, bots and spyware that can be used to steal confidential information or hijack computer functions in furtherance of financial or other crimes; users of card skimming or similar devices that can surreptitiously capture personal and financial details and facilitate identity fraud and financial crimes; and experts in encryption, steganography or data removal that can help conceal criminal activities or remove evidence that may incriminate offenders.

The implications of these trends are that investigations and prosecutions are likely to become more complex and lengthy than at present, with the need for investigators to take coordinated and timely action against multiple suspects contemporaneously. Again, this will entail resourcing implications for law enforcement throughout the country, and internationally.

Jurisdiction

Traditionally, courts have accepted jurisdiction if a person against whom legal proceedings are brought is physically present in the geographical territory in which the court operates, or is a citizen of the territory, or if there is some other sufficient 'territorial nexus'. Such a connection might arise if the alleged victim of a crime is in the territory, or some other effect of the crime sufficient to exercise jurisdiction is present. For crimes involving physical acts, rules of jurisdiction have largely been relatively easy to apply, but the situation is more complicated for online activity.

It can reasonably be anticipated that technology-enabled crime prosecutions involving multiple jurisdictions will continue to arise in the years ahead. Because online offending transcends borders so easily, numerous territories can simultaneously assert jurisdiction.

This leads to the necessity of choosing the most appropriate forum for proceedings, with the choice having important consequences due to the different legal systems and penalties that apply in different countries. It will be necessary for the international community to urgently address problems of multiple jurisdictions.

Issues relating to extradition are also likely to arise, although to date, there are no examples of Australians having been extradited overseas, or persons extradited to Australia, in relation to offences that could be characterised as technology-enabled crimes. There will continue to be demands placed on Australian law enforcement to work collaboratively with overseas law enforcement agencies in identifying and investigating cases suitable for extradition.

Defences

As cases involving technology-enabled crime continue to come before the courts, those accused will develop new and sophisticated defences to charges. It may be expected, for example, that 'public benefit' defences to child pornography charges will be increasingly relied upon, and that self defence may be used to resist charges relating to 'reverse hacking'.

Other defence arguments specific to technology-enabled crimes will continue to arise, such as challenges to the admissibility of electronic evidence, assertions that computers were under the control of other parties, and claims that online behaviour was merely role-playing. Defendants charged with technology-enabled crimes such as denial-of-service attacks may argue that their computer was infected with malware that made it perform functions beyond their control and knowledge. Similar arguments have sometimes been raised when child pornography is discovered on personal computers. It can be expected that such arguments will continue to be advanced.

Novel defence arguments raised in response to child pornography or child grooming prosecutions will continue to include the 'fantasy defence' according to which the sender of messages to underage children claims to have believed the person with whom they were dealing was an adult, and that all concerned were merely role-playing or engaging in sexual fantasies. Of course, in some cases such a belief would be accurate, as a number of successful investigations in Australia and overseas have involved law enforcement officers posing as children online and engaging in chat room conversations with predators. In some jurisdictions, the defence of entrapment might succeed in such situations if it can be argued that the defendant did not seek to engage in criminal activity but was merely enticed into doing so by a sting operation.

Some defendants have also argued, usually unsuccessfully, that engaging in such behaviour was 'therapeutic' or was part of a research project. Denial of improper purpose has also been a feature of some unauthorised access cases, where it is claimed that the defendant was merely pursuing the altruistic aim of exposing the vulnerabilities of computer systems and databases.

Evidentiary and procedural issues

It can be expected that those charged with technology-enabled crimes will continue to challenge the legality of electronic searches conducted by law enforcement officers who seek to obtain evidence of technology-enabled crime. Difficulties will continue to arise in determining 'reasonable suspicion' of the existence of evidentiary material relevant to the crime before private premises can be searched. Difficulties will also arise owing to search warrants being insufficiently precise or insufficiently related to the purposes for which the warrant was issued.

The need for law enforcement to be able to obtain evidence legally through remote access to computers located in other jurisdictions will become increasingly important, as will the need to obtain access codes to facilitate access to encrypted or otherwise protected data through using Trojan programs. The ability to obtain evidence in this way needs legislative clarification, as does the use of digital evidence obtained covertly in court proceedings.

Section 3LA *Crimes Act 1914* (Cth) provides a power to compel, by order of a Magistrate, any person suspected of having committed offences to which the warrant relates, or the owner or lessee of the computer or an employee of such a person, to provide assistance that is reasonable and necessary to allow the officer to access data held in, or accessible from, a computer that is on warrant premises; copy the data to a data storage device; and/or convert the data into documentary form. Failure to comply with such an order is punishable by six months. Similar powers are also provided under section 201A *Customs Act 1901* (Cth). It is likely that this provision will be used more often in the future to facilitate access to encrypted or password-protected data. Arguably, the maximum penalty may need increasing in view of the importance of the provision.

Although some memoranda of understanding have been negotiated with private sector organisations, it will become increasingly important to have the cooperation of ISPs and other organisations to facilitate access to data. It will also be likely that ISPs may, themselves, be subject to prosecution for failing to cooperate with law enforcement. There are now provisions that impose obligations on ISPs and internet content hosts to alert police to suspected online child pornography and child abuse material (*Criminal Code Act 1995* (Cth), Section 474.25), and enforcement powers to compel people with knowledge of passwords or computer security protections to assist investigators (*Crimes Act 1914* (Cth), Section 3LA). As organised crime groups move to greater use of the internet and other computer-related technologies, particularly in committing fraud and financial crimes, it can be expected that computer experts who assist by providing their tools of trade will face accessorial liability in relation to these activities.

Delays in the use of conventional mutual legal assistance applications will continue to make their use problematic in technology-enabled crime investigations where cooperation needs to be provided within hours rather than months. On the other hand, however, technology clearly facilitates surveillance and detection enabling law enforcement to follow electronic data trails. The use of data mining and database analysis tools, currently used by financial institutions to detect payment card transaction anomalies, will increase in importance and may lead to reductions in some types of technology-enabled crime.

Tighter regulatory controls may also need to be applied to private sector investigators. For example, at present the use of data surveillance devices by public police is regulated in most jurisdictions. Legislation does not, however, regulate data surveillance by private investigators that can use technologies for keyword searching and blocking of email, surveillance of internet usage and keylogging.

With increased digitisation of information, the future will see an increased likelihood of digital content being a source of disputes or forming part of underlying evidence to support or refute a dispute in judicial proceedings. Better-educated criminals are likely to explore alternatives to hiding data over the internet. These include storing data on password-protected file-sharing websites, email accounts and less reputable content providers hosted in countries with lax cybercrime legislation. Criminals are also likely to leverage the use of anti-forensic tools and information-hiding tools, including steganography, to further impede collection of evidence.

Developments in data storage and dissemination technologies such as proprietary storage media and proprietary cryptographic algorithms can also impede forensic investigators and prevent police from acquiring digital evidence and analysing digital content forensically. For example, the integrity of data can be compromised during extraction or conversion from incompatible proprietary formats. Therefore, an in-depth understanding of how different technologies and applications operate is crucial in collecting digital evidence. Moreover, in response to changing contexts, various computer forensic tools and techniques have to be re-designed and re-engineered.

Conversely, forensic investigators and incident handlers can also make use of searching utilities to reduce the time and resources needed to interrogate file systems for keywords.

Criminal trial and sentencing issues

Criminal courts hearing cases involving technology-enabled crime, or other cases involving electronic evidence, face particular issues that will continue to arise. Difficulties concern the presentation of complex and technical evidence, the heavy reliance on expert opinion in technology-enabled crime cases, the use of complex and novel arguments relating to admissibility of evidence or the exercise of discretions, difficulties of juror comprehension of offence elements and evidence, the use of novel defences and defence arguments, and devising appropriate sentences for convicted offenders.

Much of the legislation governing technology-enabled crime has only recently been introduced in Australia and is awaiting judicial interpretation. It can be anticipated that difficulties will arise as untested provisions are relied on in prosecutions.

The need to enhance the skill base of lawyers, judges, juries, and court officials when dealing with cases involving high tech forensic issues, through initiatives such as training materials exploring both legal and technical aspects of technology-enabled crime, will continue. In addition, use of networked and electronically enabled courtrooms that can display electronic evidence in a clear and accessible way to court officials and participants in proceedings will need to be extended. Information protection standards, including best practice guidelines for managing electronic records, will also need to be developed to ensure effective use of technology and to maintain the confidence demanded of courtroom systems.

The future will also see the need to harmonise legislation concerning sentencing and punishments for technology-enabled crimes throughout Australia, and, ideally, across the globe. Achieving some measure of uniformity will help minimise the risk of offenders jurisdiction shopping to seek out countries from which to base their activities that have the least severe punishments.

In sentencing hearings, it is likely that offenders will raise a range of new mitigating considerations. In view of the ever-expanding use of personal computers, it is likely that 'computer addiction' (or 'internet addiction disorder') will be raised more often as a mitigating factor, or even as a defence vitiating intent.

The courts will continue to experiment with new punishments such as forfeiture of computers and restriction-of-use orders. Restricting access to computers or the internet can have potentially profound consequences, making punishments of this kind arguably more severe than traditional conditional orders. Rather than seeking to impose restrictions on use of computers as a means of punishment, courts could perhaps adopt the alternative approach of requiring offenders to use their computer skills or knowledge for constructive purposes. This could include orders that require offenders to deliver lectures to the public or schools about the dangers of computer crime, and discouraging others from engaging in similar conduct, and performing supervised community service in the high-tech field.

Policing and preventive strategies

The role of industry

Poorly designed, executed and maintained security protocols, processes and devices leave computer networks open to attack. Many of these risks could be minimised though industry developing more secure hardware and software. Security should also be integrated into the software and system development life cycle.

Manufacturers need to be made aware that they could achieve marketing and competitive advantages if they produced new products with higher levels and more innovative types of security that would help combat technology-enabled crime. Law enforcement and security researchers could contribute to a stronger technology security environment by notifying manufactures and vendors of weaknesses that have been discovered in technologies to enable fixes to be formulated, by publicising weaknesses discovered during investigations, and by working with industry to identify potentially new and emerging risk areas.

Public–private sector partnerships

Government has driven much of the response to technology-enabled crime but the private sector plays a crucial role in the fight against technology-enabled crime. Partnerships between public sector police and private sector agencies will continue to be a guiding principle of technology-enabled crime policing in the future. The perceived benefits include increased reporting to police, more timely sharing of information, sharing equipment for processing digital evidence, better preservation of evidence, avoidance of duplicated effort, reducing costs and bi-directional training of investigators. For the private sector, partnerships will also result in commercial opportunities and perhaps more effective policing avenues for their clients. Such partnerships would also prepare businesses in times of pandemics and natural disasters.

Investigations by law enforcement agencies and private investigators will, however, continue to be hindered by the global distribution and increasingly corporate ownership of internet and cyberspace infrastructure and services. Trails of evidence may pass through innumerable hosts, each requiring legal authority to access evidence, while gambling at each step on evidence retention versus business demands for data storage. Both sectors face difficulties establishing identity from online identifiers. The potential sources of digital evidence have also multiplied and are increasingly wireless, miniature and encrypted. By virtue of global organisations spanning international and interstate jurisdictions, corporate investigators will continue to face difficulties of having to deal with many police forces and inconsistent local laws. Civil search and seizure powers available to private investigators are more restrictive than police warrants. Other impediments in relation to transnational policing of technology-enabled crime include deciding jurisdiction, negotiating mutual assistance and extradition, and logistical issues such as navigating time zones and languages.

Other likely risks associated with public–private investigative partnerships include inadvertent creation of opportunities for corruption, mishandling of investigations, misinterpretation or planting of digital evidence, and copying of seized, illicit materials. The potential to constrain public police in commercial-in-confidence situations may reduce transparency and possibilities may also arise for the referral of cases to ‘for-fee’ private investigators that may result in incidents not being investigated if victims cannot or choose not to pay.

The emergence of international networks of Computer Emergency Response Teams, 24/7 law enforcement contact points and other public/user interest groups underscores the intrinsic importance of information sharing in fighting crime. Law enforcement will need resources for ongoing research and development in technology-enabled crime and for sharing of information and intelligence between investigative, intelligence and forensic units. A more responsive distribution mechanism for information will be needed to enable effective responses to technology-enabled crime to be implemented.

Harnessing open source private sector resources, such as development of 'Intellipedia' currently used by the United States intelligence community to disseminate and share intelligence amongst 16 United States intelligence agencies, may assist. Such (confidential) information sharing channels will also be the target of malicious attacks by criminals and terrorists. Information leaked from these channels could potentially result in the compromise of national security.

The use of task forces and training

The organisational capacity of law enforcement and other agencies within and across national borders to deal with increasingly complex technology-enabled crime will continue to be constrained. The use of task forces to respond to particularly complex technology-enabled crimes will continue to be beneficial, although this may have the effect of reducing resources for investigation of more mundane, low-value computer crimes. The need for task forces to be established quickly also creates difficulties for investigation of new types of technology-enabled crime, where immediate response is invariably needed. Standing investigatory units may, therefore, offer greater benefits.

The need for training in technology-enabled crime laws targeting IT professionals and legal professionals, particularly concerning evidence and procedure, will increase as countries enact new legislation to deal with emerging threats. Developments in network vulnerabilities will require ongoing training in computer forensics. Although establishment of computer forensics accreditation programs will ensure standards of training are maintained, problems will arise in ensuring adequate staffing levels of accredited investigators. The use of private sector contractors will continue to be necessary, although risk management will be needed to ensure trained personnel do not misuse their skills for non-policing work.

Creation of resources, such as the *Handbook of legal procedures of computer and network misuse in European Union countries*, for police and legal practitioners will continue to be necessary. Australia is well placed to guide training in high-tech law and procedures across the Asia–Pacific region, although any initiatives should be harmonised with activities in Europe and North America.

Increasingly, well-organised groups of forensic examiners working in government facilities or private sector workplaces, such as leading accounting firms, are undertaking forensic analysis of computers for law enforcement purposes. An emerging issue is the desirability of accreditation both for individual examiners and for forensic laboratories, along with validation of forensic analysis tools. Over the next two years, developments will be needed to ensure standards of forensic computing are being maintained nationally and internationally.

Technical assistance to less capable (or less ICT-advanced) jurisdictions will also be essential as the widespread provision of training will allow the leading ICT advanced countries to manage if not prevent many of the cross-border problems now so evident in the delivery of phishing, denial-of-service attacks and other technology-enabled crime.

The absence of suitable training and inappropriate safety cultures appears to be a major challenge and includes household and end-users. For example, vulnerability in Microsoft Word allows remote code execution that requires users to open an infected Microsoft Office document. There is, therefore, a need for coordinated government agency action to promote a culture of security for information systems and networks among end-users, and to ensure the most effective crime prevention advice is provided to the community. User education, through dissemination of media releases by authoritative institutions such as the Internet Crime Complaint Center, enables users to keep abreast of the latest scams and the best fraud prevention measures available.

The complexity of the task of providing training and educational programs in the context of the transnational nature of technology-enabled crime will continue to be challenging and costly.

Prevention and deterrence

Law enforcement operates at three broad levels: crime prevention, investigation and prosecution. Public agencies have a limited role in the prevention of technology-enabled crimes, in part because the design of the personal computer and the global adoption of the internet have largely been in the hands of private sector forces with less focus on security than on functionality, and thus the burden of protection against misuse of the technology has fallen largely on individual users. There is a flourishing industry of computer security products and services, such as antivirus software, intrusion detection devices and encryption tools, servicing the increasing desire of individuals and businesses to protect themselves against computer-related threats.

Clearly, there is limited capacity in law enforcement to investigate a high volume of technology-enabled crimes, and the future of security will remain largely with system administrators and software developers. Nonetheless, the threat of prosecution and punishment will continue to be a powerful deterrent in this environment, particularly where substantial penalties can be imposed. There will be an ongoing need for effective publicity to be given to the results of successful prosecutions, particularly in new areas of risk. The use of international task force operations should also be widely publicised as indicative of the ability of law enforcement to carry out investigations against individuals located in multiple countries.

Ongoing needs exist for centralised sharing of information and intelligence across jurisdictional borders, both within Australia and internationally. New technology-enabled crime methodologies will continue to emerge and disseminate rapidly requiring the immediate sharing of intelligence and newly developed response strategies. Resources are also needed to map trends in technology-enabled crime to anticipate new areas of risk and to determine when previous types of crimes have dissipated. One of the keys to staying abreast of the latest technologies is to understand both the hardware and software characteristics of the technologies in question.

Knowledge about offender and victim behaviour, as it applies in the online environment, needs to be enhanced. Some of the information gaps are being addressed but further development, based on a clear and functional classification of computer crimes, is essential. To guide training and research, a number of cross-disciplinary applied and theoretical approaches will need to be tested. Along with these essential processes must be a greater willingness to test and re-test software and hardware defences as well as the best forms of general and specific forms of public–private partnerships in preventing technology-enabled crime.

Introduction

The future of technology-enabled crime sits within the broader digital environment, an environment created primarily to facilitate social and business relationships and transactions but one which is increasingly prone to degradation, infiltration and subsequent criminal activity. Although the precise future characteristics of technology-enabled crime cannot be accurately determined, it remains possible to assess the likely path that future technology-enabled crime risks will take, and which targets are likely to carry greatest risk.

Technology-enabled crime

Traditionally, academic discussions of computer crime have been somewhat imprecise in the terms they have used to delimit the scope of their inquiry. A range of adjectives have been used to describe various aspects of computer-related crime including: virtual, online, cyber-, digital, high tech, computer-related, internet-related, telecommunications-related, computer-assisted, electronic, ICT-related, and e- (as in 'e-crime'). Clearly, there are different contexts in which each of these descriptive terms is more appropriate than others. For example, hacking into free-standing un-networked computer systems and databases preceded the advent of the internet in its current form, so the terms internet crime or online crime are inappropriate to deal with these earlier forms of activity. Even spelling and usage show variations, particularly with regard to the use of the prefix 'cyber'. The literature contains references to cybercrime, cyber crime and cyber-crime, as well as more specific forms such as cyberterrorism (or cyber-terrorism), cyberstalking (or cyber-stalking) and so on. The same variability applies to terms such as e-crime (sometimes E-crime or eCrime) (see Smith, Grabosky & Urbas 2004: 5–6 for a discussion of this issue).

Primarily, a distinction can be drawn between crimes in which information and communications technologies are the object or the target of offending; and crimes in which technologies are the tool in the commission of the offence. The latter category incorporates two levels of reliance on technologies: offences which are *enabled* by technologies (i.e. in which a computer is required for the commission of the offence); and offences which are *enhanced* by technologies (i.e. in which computers make it easier to commit an offence).

This report focuses on technology-enabled crime which is, arguably, the type of offending that is most directly related to misuse of ICT. Where some specific forms of technology-enabled crime are discussed, terms such as cybercrime, cyberstalking and so on are used in conformity with Australian legislation such as the *Cybercrime Act 2001* (Cth) and international instruments such as the Council of Europe Convention on Cybercrime. The focus is, however, on crimes that require ICT for their commission, rather than conventional crimes which may, incidentally have ICT involved in some way.

Motivations

Technology-enabled crime is becoming increasingly pervasive and sophisticated, and can, arguably, have a more severe economic impact than many traditional crimes. A variety of motivations exist for individuals to commit technology-enabled crime. These include the 'thrill-seeking' pursuits of hacking and underground research, and the more focused criminal acts concerning financial gain, revenge and propaganda. Historically, the prime motivations for underground research and hacking included the following:

- **Curiosity and self-education:** Early instances of hacking (as opposed to the more damaging types of cracking) were carried out often by young people who were driven by curiosity and by the thrill of gaining knowledge and beating the system. Such motivations are still present today, although financially-driven crime is much more prevalent.
- **Fame-seeking:** Technology-enabled crime is also often committed by people who seek out fame or fantasise about being someone they are not. Often modelling their conduct on the exploits of infamous offenders, some are motivated to commit criminal acts because of the psychological need to be seen as having done something daring or risky.

Current trends, however, suggest that technology-enabled crime is more likely to be motivated by other factors:

- **Financial gain:** Greed, or financial gain, lay at the heart of some of the earliest attempts at theft of telecommunications services, such as phreaking in the 1970s. This motivation can be triggered by other reasons such as the need to support an addiction (to drugs or gambling), the desire to obtain money to enhance one's lifestyle, or the involvement of organised crime. This motivation has been explained through the use of a number of theoretical models. One, for example, is Bandura's (1999) social cognitive theory of behaviour. This argues that behaviour, first acquired vicariously through exposure to social models, is dependent on, and shaped by, positive reinforcement arising from different combinations of fundamental human incentives – money, power, status and sensory needs. The involvement of organised groups in technology-enabled crime now emphasises the importance of large-scale profit-driven incentives.
- **Revenge:** Revenge will continue to be a motivation for individuals such as disgruntled employees who use weaknesses within ICT frameworks to cause damage to former employers, be they corporate entities or individual within organisations. As business continues to become dependant on ICT, attacks on systems will represent an important means of exacting revenge.
- **Political motivations:** Politically-motivated criminals including terrorists and other issue-motivated groups will continue to be attracted by the damage that can be caused by attacks on financial and critical information infrastructure in developed countries. The internet is also a powerful took for disseminating propaganda and enabling individuals to communicate with each other securely.

Financially motivated crime is, arguably, the area in which technology-enabled crime will develop most rapidly over the next few years. This is not surprising as advances in ICT and the spread of the internet have revolutionised the way in which commerce operates (e.g. electronic payment systems and online auction sites). The financial incentive to do business electronically in today's highly competitive market is significant, with the cost of an online transaction often being a fraction of a non-electronic transaction (De Young 2001). While it is almost impossible to quantify the actual impact of ICT on world economics, Milburn (2006) has estimated the value of integrating ICT into traditional business models at US$30 trillion in relation to trade in goods and services transacted across the globe through computerised supply chains every year.

Various studies have indicated that the incidence of financially motivated technology-enabled crime is increasing. For example, the 2006 AusCERT (2006) survey and the DTI Information Security Breaches Survey 2006 (PwC 2006) found an increase in the views held by the businesses surveyed that electronic attacks are more often motivated by illicit financial gain than in the past, both in Australia and around the world. The United States Federal Bureau of Investigation (FBI) has estimated the financial loss due to cybercrime in 2004 as being approximately US$400 billion (McAfee 2005), while a United Kingdom survey (PwC 2006) found that information security breaches cost British companies across several industry sectors £10 billion per annum.

It seems likely that the number of potential victims of economic and technology-enabled crime will continue to increase along with the spread of internet capable devices, both fixed and wireless. Advances in modern technology offer anonymity to criminals by allowing them to hide their true identities with relative ease or to spoof the identities of others. As well as these current attacks, it has been suggested (Miller et al. 1998) that the volume of information likely to become available in the near future to the average private user may lead to the use of 'knowbots' (knowledge robots). These applications would navigate through data on a user's behalf and perhaps even organise part of their daily online routine, such as scanning email for particular addresses or subject matter. Knowbots controlled by a malicious third party could equally facilitate the navigation through bank accounts to extract confidential financial information.

Developing information risks

Advances in technology bring with them corresponding risks. Some may be of national importance such as when computer systems that control and operate critical infrastructure are compromised. Other risks have closer impact on the lives of individuals, such as when funds or personal information are stolen. Personal information is increasingly being kept in digital form and is being routinely disseminated between computer networks operated by both business and government. The acquisition and misuse of such information is (as confirmed by a number of annual surveys of corporations) likely to form the basis of future technology-enabled crime threats. Risks relating to digital information include:

- offences against CIA security notions (confidentiality, integrity and authentication) via activities such as hacking, deception, interception and espionage
- computer-related ‘traditional’ crimes, such as fraud and forgery
- content-related computer offences, such as website defacement and dissemination of objectionable or false information
- offences relating to the infringement of intellectual property (IP) rights, including unauthorised reproduction and use of programs and databases (Council of Europe 2004).

Business crime risks

Reports, including the IBM (2006b) *Global business security index report*, suggest that likely future ICT crime trends and targets will involve the following:

- insider attacks in which end users will be persuaded to execute attacks on organisations rather than outsiders attempting to circumvent increasingly secure software
- emerging markets in which advantage is taken of poor international cooperation against technology-enabled crime, so the threat to and from emerging and developing countries will increase. Trends show that attacks are increasingly originating from regions such as Eastern Europe and Asia where sanctions are more lenient and enforcement limited
- botnets will continue to constitute one of the internet’s biggest threats and will move to instant messaging and other peer-to-peer networks for command and control of infected systems
- malware affecting mobile phones, personal digital assistants (PDAs) and other wireless devices increased during 2005, but has not yet materialised into pervasive outbreaks since they cannot yet spread on their own.

The new threat landscape might be typified by malware attacks that facilitate subsequent criminal endeavours. Attacks are deemed to be moving away from large affairs (such as global spam incidents) to smaller, more focused attacks upon particular clients (Sophos 2007c). The motivation has become largely profit-oriented with technology-enabled crimes that increase profits most readily, such as identity theft, fraud and extortion, of greatest concern.

The gap that exists between the legislative framework, law enforcement capacity and response, and the exponential rise in electronic attacks continues to increase. It is clear from a number of corporate surveys (e.g. the CSI 2006 and AusCERT 2006) that the issue is as much about the unwillingness of corporations to report security breaches and dedicate sufficient resources to information security as it is about the capacity of law enforcement to remain equal to such threats.

Even if there are questions concerning the specific nature and impact of technology-enabled crime, it is possible to predict some likely consequences of developments in ICT. These include the likelihood that electronic crime will occur more quickly and that this, in turn, will reduce the risk to the perpetrators of being detected and apprehended. Information as to how online attacks may be perpetrated will probably become more readily available and spark an increase in the occurrence of technology-enabled crime.

The ability of criminals to operate in the online environment may alter the nature of the criminals encountered by law enforcement. This would in turn require changes in the training of law enforcement officers and in the ways in which law enforcement agencies operate. As IBM (2006a) has noted, the rise in cybercrime has created a situation in which '... management priorities, crime-fighting resources, investment, education and technologies are at the start of a rapid adjustment'. The issues that may need addressing as a result of such changing dynamics could include jurisdictional and legislative changes and the impact upon judicial systems. There may also develop an increasing evidentiary burden constituted by technology-enabled crime, which creates an additional burden on lawyers, judges and juries.

Drivers of technology-enabled crime

Several current and prospective features of ICT have facilitated technology-enabled crime. These include:

- ICT becoming intrinsically connected to daily personal and business life
- computer systems and networks that facilitate commercial and private use but also create risks of subsequent exploitation by criminals
- computer data that are intrinsically hard to control; this is particularly the case with the internet which was designed to resist outside attempts to control its content or fields of operation
- computer networks that are global, with information flowing via a number of networks and through a number of jurisdictions
- computers and computer networks that are fast (Council of Europe 2004).

Broadband facilitates the rapid downloading and uploading of large video, music and software files. The fact that many computers are now permanently connected to the internet, when coupled with the poor security awareness of many domestic users, renders such computers prone to exploitation. The potential rationale for such attacks could include the obtaining of personal information for identity theft or the use of the computer as a 'zombie' or storage facility for illegal material as has been found to be the case with commercial and university systems. These dangers are likely to be exacerbated by activities such as peer-to-peer file sharing programs or the downloading of files from unknown senders. Fast download times have also facilitated dissemination of content such as pornographic images and pirated software and music particularly through peer-to-peer platforms. Most peer-to-peer software is free and it is believed may contain overt or covert advertising related software. There is also the danger that the software may contain spyware (Morris 2004).

The increasing use of mobile phones and PDAs, each with ever-increasing storage capacity, constitutes another opportunity for online attacks. Research has indicated, for example, that such devices are routinely used to store personal data and corporate information. The advent of wireless networking increases the likelihood of such information being uploaded and downloaded. In 2005, 22 percent of people reported losing their mobile devices, and, of those, 81 percent had not encrypted the information contained therein (Millman 2005). Wireless networks themselves may bring a number of vulnerabilities, key among which is the fact that networks and their data can be accessed without physical access being required. This facility assists both the user and the criminal.

Computers and IT networks have long been a feature of business organisations and continue to be used to record financial and customer data. There has been an increase in the sharing of such information via the internet, but no apparent parallel commitment to secure that data via holistic rather than piecemeal means. Indeed, computer security for a number of organisations (particularly small to medium enterprises) still consists of products rather than processes and has resulted in a reactive rather than a proactive security philosophy.

The literature on technology-enabled crime threats is replete with references to 'cybercrime' and 'organised' cybercrime. The extent to which there has been major growth in criminal behaviour and activity as a direct or indirect result of technological developments is starting to be questioned. As Wall observes, '... when so-called cases of cybercrime come to court, they often have the familiar ring of the "traditional" rather than the "cyber" about them' (Wall 2004). Indeed, the 2006 IBM (2006a) survey on cybercrime did not, in fact, define cybercrime. Thus, there is a possibility that corporations attesting to the presence of cybercrime within their particular sector could actually be commenting upon a range of disparate security intrusions ranging from spam to major viral contamination, only some of which are truly technology-enabled.

Wall (2004) has suggested that the globalisation of crime opportunities may be constituted by globalisation and 'glocalisation'. The globalisation of crime through increased connectivity of computer networks has led to a new law enforcement relationship that is between the global and the local, that is, 'glocal'. The internet has transformed criminal opportunities in three major ways:

- the communication vehicle of the internet has allowed the increase of information flow that is useful to criminal individuals and organisations

- the internet has created a transnational environment that provides entirely new opportunities for harmful activities currently the subject of existing criminal or civil law
- the nature of the internet and the virtual environment it creates has encouraged the transfer of the notion of economic value from physical property alone to now include ideas, so that criminal behaviour may also take on the appropriation of intellectual rather than just physical property.

The advent of e-business has enabled the exploitation of traditional corporate vulnerabilities, for example, fraud, within a far more rapid timeframe than before. New weaknesses in the software and hardware architecture of corporations and weaknesses in the way in which such architecture is created, maintained and operated may also be exploited both within and without organisations.

The impact of e-commerce in the form of increased and increasing global connectivity of computer systems and networks is the creation of more complicated operating systems and reliance upon technology as much as human interaction. Detecting individual malfeasance in such an environment becomes more difficult and the evidence trails perpetrators leave can quickly gain anonymity within a corporate network. There is a danger that organisations incorporate new technology without necessarily being cognisant of the potential criminal exploitation of that technology and the vulnerability to which they open themselves through lack of well-trained staff.

As has been noted, the internet was never designed to be secure from exploitation. The strength of the internet in terms of its rapid communication facility has become one of its weaknesses. Extraterritoriality, the notion that the internet has no geographic boundaries, has driven the e-commerce revolution. Unfortunately, the criminal fraternity operates online under the same free market principles, while legislative and law enforcement endeavours launched against them suffer from geographical and cultural restrictions.

The AusCERT (2006) survey found that organisations had improved the protection of their IT systems in the three key areas of the use of security technologies, the use of information security policies, practices and procedures and the use of information security standards or guidelines. There remained, however, a number of vulnerabilities such as inadequate staff training in computer security management, and poor security culture within organisations. Along with a general recognition that information security breaches were increasing, most respondents to the survey were dissatisfied with the level of funding allocated to IT security within their organisation.

A major factor in technology-enabled crime threats remains the human element, with a continuation of the movement from syntactic (attacking the computer) to semantic (attacking the computer user) attacks likely. An indication of human vulnerabilities may be seen in the study by Dhamija and colleagues in 2006 on the rationale for the success of phishing attacks.

The study showed 22 participants 20 web sites and asked them to determine which were fraudulent and why. The best phishing site was able to fool more than 90 percent of participants. Indicators that are designed to signal trustworthiness were not understood or even noticed by many participants. Five of the 22 participants (23%) only used the content of the website to evaluate authenticity, without looking at any portions of the browser. Fifteen of the 22 participants proceeded without hesitation when faced with a popup warning about fraudulent certificates.

> Participants proved vulnerable across the board to phishing attacks. In our study, education, age, sex, previous experience, and hours of computer use do not show a statistically significant correlation with vulnerability to phishing (Dhamija et al. 2006).

The study suggested that a different approach is needed in the design of security systems. As the authors observe: '[r]ather than approaching the problem solely from a traditional cryptography-based security framework (what can we secure?) a usable design must take into account what humans do well and what they do not do well.' The authors argued that computer users must be educated to distinguish legitimate security indicators from spoofed ones. This educative process may include the use of colours in the address bar to indicate suspicious and/or trusted sites, respectively.

Developments in information and communications technologies that may facilitate technology-enabled crime

Although technology developed dramatically throughout the late 20th century, it has been argued that in the early to mid 19th century the impact of the railway, steamship and telegraph was far more revolutionary than the internet or mass air travel have been (Naylor 2000).

> Indeed, virtually every kind of crime now conducted through modern electronic communications technology had some equivalent in the telegraph age – which saw everything from insider trading to price fixing to financial fraud conducted by and through the telegraph, while telegraph companies faced problems of breaches of security by hackers threatening, in particular, telegraphic money transfers (Naylor 2000).

Technology has even been said to have democratised crime owing to the fact that:

> smaller players have an easier time entering the market … [that is] why the notion of the great crime 'cartels' may increasingly be a myth as the contemporary criminal market place changes in origin (Thoumi 2000 as cited in Naylor 2000).

Van Duyne (2000 as cited in Naylor 2000) argued that although technology may facilitate crime it could also facilitate surveillance and detection given that all electronic patterns leave a virtual trail. A preliminary observation is that there have, arguably, been two key periods of significant ICT infrastructure development. The first, which began in the 1980s, involved the movement of computing power from mainframes to personal computers. The second, which began in the 1990s, involved widespread access to the internet and enhanced communication vehicles such as email, instant messaging and high-speed connectivity. Gorbis and Pescovitz (2006) suggest that those two trends are set to continue. Other current and prospective features of ICT developments that may facilitate technology-enabled crime are described below.

Similarly, Grabosky and Smith (1998: 213) noted how the development of digital crime reflected the development of certain key technologies – thus, substantiating the 'crime follows opportunity' thesis of routine activities theory.

Information and communications technologies take-up

A primary vehicle for technological innovation has been, and will continue to be, the internet which was created in 1969 as a research network sponsored by the Advanced Research Project Agency (ARPA) for the Department of Defense in the United States, hence its original name, ARPANET. The internet's primary function at this time was to maintain the flow of defence-related information during a catastrophic nuclear attack. Given that rationale, it was not required, nor designed, to be a highly developed or intelligent system. Internet use has grown since the initial handful of ARPA machines so that in June 2006, there were 439,286,364 internet hosts (Internet Systems Consortium 2006) and in December 2006 there were 1,091,730,861 users (Internet World Stats 2006). However, the basic nature of the internet, a vehicle for conveying packets of data between devices – the 'end-to-end principle' – has remained unchanged and the resultant architecture, whilst embracing the original unfettered communication precept of the internet, has facilitated an increasing vulnerability to inadvertent technical failings as well as to advertent criminal activity.

Observers of the internet and its use have suggested that it is simply becoming less and less able to cope with the exponential demands, in terms of information storage and exchange, being placed upon it. Consequently, a project launched by the National Science Foundation in the United States is examining how best to equip the internet for the needs of the future. A member of the project team has argued that:

> [t]he challenging question is: can we conceive a vision for what a global communications network will look like in ten or fifteen years? To do that, you have to free yourself from what the world looks like now. The internet is so obvious that it is hard to contemplate what a non-internet would look like (Reinventing the internet 2006).

Arguably, any view of possible future types and use of technology needs to be considered in terms of if, how and when societies to which technological advances are introduced are in a position to embrace change per se. At the very least, consideration should be given to the manner in which a newly configured internet would mitigate or facilitate more sophisticated forms of criminal endeavour.

Brief insights into potential abuse of the internet are provided in the *Online fraud report* (National Cyber Security Alliance and Bank of America 2006) and the *2005 IC3 internet fraud crime report* (Federal Trade Commission 2006). In the former, it was noted that approximately one in 10 Americans use the Internet and conduct a number of online financial transactions. The findings suggested that:

- 87 percent of respondents felt extremely or somewhat confident in their ability to recognise a fake email. In practice, however, 61 percent failed to correctly identify a legitimate email
- 97 percent of respondents failed to correctly identify a secure and safe website and 58 percent of respondents remained vulnerable on the Internet because of an over-reliance on the appearance of a 'padlock' on a website as their only indication of a secure site
- Whilst over 80 percent of consumers stated they understood that not opening unsolicited email, using security software and ensuring that such software remained updated were all integral to preventing internet fraud, 80 percent of respondents in a separate study (AOL/NCSA 2005) said they did not practice most of those security protocols.

In the latter, the internet complaints division of the United States Federal Trade Commission, the Internet Crime Complaint Center (IC3), processed more than 228,400 complaints that could lead to internet crime investigations by law enforcement and regulatory agencies nationwide. These complaints consisted of many different fraud types such as auction fraud, credit/debit card fraud and non-fraudulent complaints, such as computer intrusions, spam, unsolicited email, and child pornography.

Although Asia represents about 56 percent of the world population only about 11 percent of its population has access to the internet. However, this represents just over one-third of the world's current population with access to the internet and thus a highly significant market. North America (70%), Oceania/Australia (54%) and Europe (39%) have the highest levels of access per head of population; while in Africa a mere 3.6 percent of the population has internet access (Internet Systems Consortium 2006). The general variations in access around the globe are shown in Table 1.

Table 1: World internet usage and population statistics

World regions	Population % of world (2007 estimated)	Number of internet users	% population (penetration)	Usage % of world	Usage growth 2000–07
Africa	14	33,334,800	4	3	638
Asia	57	398,709,065	11	36	249
Europe	12	314,792,225	39	28	200
Middle East	3	19,424,700	10	2	491
North America	5	233,188,086	70	21	116
Latin America/Caribbean	9	96,386,009	17	9	433
Oceania/Australia	1	18,439,541	54	2	142
World total	**100**	**1,114,274,426**	**17**	**100**	**209**

Note: Internet usage and world population statistics at 19 March 2007

Source: adapted from http://www.internetworldstats.com/stats.htm

Thus the gap between ICT-rich and ICT-poor countries continues to reflect global disparity in wealth and trade while English remains the dominant language. As at September 2004, 35 percent of the estimated online population of 801 million people used English, followed by Chinese (14%), Spanish (9%), Japanese (8%), German (7%), French (4%), Korean (4%), Italian (4%), Portuguese (3%) and Dutch (2%) (Global Reach 2007).

Similar trends were observed in a more recent study shown in Table 2. Note, however, that the countries are slightly different in each study.

Table 2: Top 10 languages used in the web

Top 10 languages in the internet	% of all internet users	Number of internet users by language	Internet penetration % by language	Internet growth % for language (2000–07)	2007 estimate world population for the language
English	30	328,666,386	29	140	1,143,218,916
Chinese	14	159,001,513	12	392	1,351,737,925
Spanish	8	88,920,232	20	260	439,284,783
Japanese	8	86,300,000	67	83	128,646,345
German	5	58,711,687	61	113	96,025,053
French	5	55,521,294	14	355	387,820,873
Portuguese	4	40,216,760	17	431	234,099,347
Korean	3	34,120,000	46	79	74,811,368
Italian	3	30,763,940	52	133	59,546,696
Arabic	3	28,540,700	8	932	340,548,157
Top 10 languages	82	910,762,512	21	181	4,255,739,462
Rest of world languages	18	203,511,914	9	445	2,318,926,955
World total	**100**	**1,114,274,426**	**17**	**209**	**6,574,666,417**

Note: Internet usage and world population statistics at 10 March 2007

Source: adapted from http://www.internetworldstats.com/stats7.htm

The negative economic consequences of these digital divides are significant and mean many countries are unable to benefit from the efficiencies and opportunities provided by e-commerce. In addition, the social capital associated with access to markets, networks and educational resources should not be underestimated.

Online sales as a proportion of market share have been estimated at 13 percent in the United States, 16 percent in Korea and Australia, about 9 percent in Japan and the Netherlands, and 7 percent in the United Kingdom. Forrester Research also noted that, while the United States and North America currently preside over the majority of online transactions, Asian and European nations will become more active in the future. North America had the lion's share of the e-commerce market with 51 percent (47% in the United States); while Asia had about 24 percent; Japan 13 percent; Europe 23 percent (Germany 6 percent) and Latin America 1 percent. These global differences may also be reflected within a single country; for example, China's urban wealthy generally have internet access while those among the rural poor do not.

At the end of 2002, an estimated 57 million people in China had access to the internet and by the end of 2004 this had reached 94 million approximately 7 percent of the Chinese population of whom 45.5 percent were broadband users. The number of hosts in 2004 was estimated to total 41.6 million, Internet Protocol version 4 addresses 60 million, domain names 432,077 and websites 668,900.

In 2001, Neilsens estimated that China would have 200 million internet users (15 percent of the population) and 500 million mobile/land phones by 2006 (Neilsens/Netrating 2002 as cited in Broadhurst & Chantler 2006: 3–4). However, by end of 2005 access to the internet in China had reached 111 million, or approximately 9 percent of its population, of whom 64 percent were broadband users. The number of internet hosts was estimated to total 50 million, internet protocol version 4 addresses 74 million (3rd largest in the world according to the China Internet Network Information Centre), domain names 2,592,410 (53 percent of these are .CN) and 694,200 websites. According to the China Internet Network Information Centre this now makes the People's Republic of China first in Asia and sixth worldwide for domain and websites. In 2006 it was reported that the population of internet users in China has risen by 30 percent to 132 million as at December 2006 (AP 2006). At the current annual growth rate of about 19 percent, Chinese users will take longer to exceed the number of North Americans on the internet (estimated at 227 million), originally predicted to occur in 2008.

Despite these impressive growth rates, rural and urban differences are dramatic with an average access rate of 16.9 percent in urban areas and only about 3 percent in rural areas. Cities such as Shanghai (27% access) and Beijing (29%), have access rates approaching those of many advanced western and industrialised nations.

Internet access is already between 60 and 70 percent of households for Japan and the Tiger or 'little dragon' economies of Hong Kong, Singapore, Taiwan, and South Korea. These may be regarded as e-nations; those capable of fully exploiting the benefits of e-commerce and ICT, and with broadband access rates comparable with or better than most Western countries. For Malaysia and Macao, between 37 and 42 percent of households have access, and these two countries continue to grow e-commerce and other ICT capabilities. A large number of Asian countries are in the early stages of developing their ICT infrastructure and have begun to reach critical mass at around 7 to 15 percent of the population: these include Vietnam, Thailand, Philippines, Indonesia, China, Mongolia, and Brunei. India's 50.5 million users (approximately 5 percent of the population) have now qualified as a significant market, with an astonishing growth rate of 900 percent since 2000. At the lower end of the spectrum are several countries whose internet access is less than 2 or 3 percent of the population. This group includes Afghanistan, Laos, Bangladesh, Cambodia, Myanmar, East Timor, Nepal and Sri Lanka who are also among the most economically disadvantaged nations in the region. Within these cross-national digital divides there are also stark differences between the urban and rural users, as well as gender and class differences in internet access.

Possible security threats to Australian e-businesses emanating from Asia

Developments in ICT now greatly facilitate commerce between developed countries and newly emerging economies in Asia. Although these new economies are developing quickly, their information security environment is less well developed, as is their legal and ICT policy framework. These differences are likely to create an environment in which technology-enabled crime attacks on Australian organisations may emanate from, or make use of, security weaknesses in organisations in developing countries with which Australian organisations and individuals deal. Threats to information and communications infrastructure could also arise from natural disasters. For example, the 26 December 2006 earthquake in the southwest city of Pingtung in Taiwan disrupted telephone and internet services throughout Asia.

The declining importance of dial-up connections and the expansion of broadband services have also created an environment in which connections are maintained continually, thereby providing greater opportunities for attacks against inadequately secured computers, particularly those in domestic situations, which may be compromised for use in botnets (Choo 2007). The use of peer-to-peer file sharing programs or downloading files from unknown senders will also increase risks for domestic users. Rapid download times have also facilitated dissemination of content such as pornographic images and pirated software and music particularly through peer-to-peer platforms and online sharing websites that may also contain spyware.

The path of technological development

Moore's Law (1965,1998) predicts that the number of transistors able to be positioned per square inch on an integrated circuit will double every year (which to date has proved to be a correct assertion) and a common route to imagining the technological future is to consider the performance of technology in terms of its relative speed, size or cost. The first computer occupied 70 cubic metres of floor space (Gallaire 1998). In the 1970s a megabyte of semiconductor memory cost approximately $550,000. In the 1990s it cost $4. Microprocessors in the 1990s were 100,000 times faster than their 1950s predecessors. Based on those rates of change, a desktop computer in 2020 will be as powerful as all the computers currently situated in Silicon Valley in the United States (Miller et al. 1998).

Miller and colleagues (1998) have suggested that such rapid improvement may be accelerated by computers that combine optical and silicon technology to facilitate transfer of data within a computer chip via laser. The National Nanotechnology Initiative in the United States (National Science and Technology Council 2000) projected that developments in nanoscience and nanoengineering were likely to change the way things are designed and made; things like vaccines, computers, automobile tires and objects not yet imagined. In relation to such technology the likely increased use of micro-electromechanical systems (MEMS) is set to have a great potential impact and significance. MEMS are small – from a micrometre (one-millionth of a metre) to a millimetre – devices or systems that combine electrical and mechanical components and currently permit industry to add beams, gears and springs to minute devices. A potential future use of MEMS might be to enhance information storage, processing and communication.

In the next few decades significant progress is likely to be made in relation to the application of technology or, as Deloitte Touche Tohmatsu (2006) prefer, TMC (Technology, Media and Communications).

> We will not be teleporting breakfast or using quantum computers, nor will we be watching holographic TV or travelling to work in flying cars. A lucky few may likely be flying to the edge of space but for the rest of us, change will probably be more subtle, with TMC advances pervading ever more deeply into our daily lives (Deloitte Touche Tohmatsu 2006).

Technology will become increasingly ubiquitous. Established technologies such as mobile phones and computers will continue to be widely used but there is likely to be a proliferation of auxiliary devices aimed at improving the performance and flexibility of those established products (Deloitte Touche Tohmatsu 2006). More broadly, Newton and Lawrence Pfleeger (2006) have mooted that there will be an increasing convergence of technologies whereby a number of disparate goods and services may be coupled with IT in the same way in which mobile phones, for example are currently capable of taking video footage and photographs and permitting access to the Web.

The key threat emanating from the ubiquity and complexity of technology in an era of increasing connectivity will be viral contamination. This threat will be exacerbated by the reliance businesses and individuals place upon the technology to function in their daily lives. Communication vehicles will increase exponentially and the danger of such communication conduits being breached by high-tech criminals is likely to rise in tandem.

Networked technology is also destined to evolve through use of increasingly faster fibre optical systems that will improve transmission of data between computers and computer networks. Indeed, Coates (1998) has suggested that technology will become ‘intrinsically smart’. In a manner analogous to light-responsive glasses, technology will be able to evaluate its own performance and initiate repairs or upgrades as that evaluation dictates. Other technological developments include wearable computers, that is, computational devices embedded in clothing, handbags or jewellery, and quantum cryptography which would use quantum mechanical methods to encode information for more secure transfer (Silberglitt et al. 2006). Voice-over-Internet Protocol (VoIP) communication together, in the developing world, with solar-powered Wi-Fi network hubs and low-cost laptop computers is increasing the geo-political parameters of the information age (Gorbis & Pescovitz 2006).

Ultimately, systems operating critical infrastructure will be able to be managed remotely. Whilst this augurs well for efficiency it bodes ill for technology-enabled crime infiltration.

E-commerce

Electronic commerce is likely to continue to grow in volume and sophistication given that the increased speed in connection and movement of data between computers will allow anyone to create an online business and/or become an online consumer. The world is one of global economies. More accurately, and more worryingly perhaps, the world is a world of aspiring global economies. There are many countries who have until now been unable to enrich their economies through ordinary industrial growth. In part, this was because they lacked the requisite financial resources to do so; in part it was due to increasing, if unfair, western moratoria on ecologically damaging latent development. The beauty and potential danger of the internet-driven economy lies in the ability of emerging economies to create and sustain at least the illusion of industrial and capitalist parity with the developed economies of the west until such time that that parity is actually achieved. The problem with illusions is, however, that they require creative misdirection. The dangers of such sleights of hand being used by emerging economies are potentially grave. The digital divide that exists between developed and developing countries remains an issue of concern. The danger of this situation is that those countries with poorer critical infrastructure may be driven, by globalisation demands, to engage with other countries whilst not sufficiently prepared, in technological terms, to do so.

The process of disintermediation currently experienced in areas such as banking (whereby physical contact between organisations and their clients is replaced by virtual contact) may actually transpose to the generic business and social worlds. As some observers put it:

> there is likely to be an accelerating trend away from the reassurances, subtle information-sharing and planning assumptions that were once offered by stable career patterns, fixed responsibility pyramids, familiar local shops, and face-to-face encounters at work or in the schoolyard or doctor's office (Miller et al. 1998).

In addition, given that the primary reason e-commerce was developed was to engage online with other organisations, there is a danger that organisations with weaker critical infrastructure protection may harm those organisations boasting relatively secure systems. This connectivity danger has been asserted by the notion of 'e-readiness' a scale that more accurately reflects the potential dangers of global connectivity.

The e-readiness survey (Economist Intelligence Unit 2006)[1] examines the world's leading economies in order to determine their true technical ability to engage securely in the online

[1] The 2007 EIU e-readiness rankings have been released since this report was prepared. They are available at http://graphics.eiu.com/files/ad_pdfs/2007Ereadiness_Ranking_WP.pdf

environment. Countries are assessed on six issues according to a 10-point scale (10 constituting the highest ranking). The scale is:

1. **Connectivity and technology infrastructure** – the access that individuals and businesses have to fixed and mobile phone services, personal computers and the Internet and the affordability, quality and reliability of such services.
2. **Business environment** – the strength of the economy, the quality of infrastructure and openness to trade and investment.
3. **Consumer and business adoption** – the proportion of trading that occurs online, the development of online payment systems and government investment in ICT.
4. **Legal and policy environment** – the nature and quality of the legal framework and specific legislation concerning the internet and its use and the protection of IP.
5. **Social and cultural environment** – the levels of e-literacy in terms of the population's experience of the internet, the technical skills of the workforce and the levels of innovation.
6. **Resource use and environmental health** – the availability and accessibility of natural resources can both enhance and hinder technology implementation. Developing countries might benefit greatly from advances in genetic modification technology but not have the financial wherewithal to pay for such technology.
7. **Research and development investment** – for technological advances to be used effectively within a society, the skill base necessary to adopt, use and maintain the technology must, of necessity, be present.
8. **Education and literacy** – the ability of countries to embrace technological change depends in large part upon them having educated and literate populations. China has a large and literate population and has thus managed to exploit technological demand to great effect.
9. **Population and demographics** – the size and demographic distribution of a population can determine the nature of technological need and the rate and nature of technological change. Countries that have experienced large population losses to human immunodeficiency virus/acquired immune deficiency syndrome (HIV/AIDS), as well as those with populations subject to outbreaks of severe acute respiratory syndrome (SARS) and avian flu etc., may have difficulties in maintaining new technologies. This failure may of course have significant and long-term socio-political impacts.
10. **Governance and stability** – corruption can render the cost of technology more expensive than the primary cost of that technology through the insistence of payments for provision of infrastructure necessary to apply technology as well as for facilitating introduction of the technology itself.

As can be seen from Table 3, the relative positions of Australia, India and China in the e-readiness scale are telling. The potential impact of a critical infrastructure or network security breach in either India or China upon the security of information stored on computers in Australia is likely to be high.

Table 3: Summary of e-readiness

2006 e-readiness rank (of 68)	2005 rank	Country	2006 e-readiness score (of 10)[a]	2005 score	2006 e-readiness rank (of 68)	2005 rank	Country	2006 e-readiness score (of 10)[a]	2005 score
1	1	Denmark	9.00	8.74	35	32	S. Africa	5.74	5.53
2	2	US	8.88	8.73	36	34	Slovakia	5.65	5.51
3	4	Switzerland	8.81	8.62	37	35	Malaysia	5.60	5.43
4	3	Sweden	8.74	8.64	38	40	Lithuania	5.45	5.04
5	5	UK	8.64	8.54	39 (tie)	37	Latvia	5.30	5.11
6	8	Netherlands	8.60	8.28	39 (tie)	36	Mexico	5.30	5.21
7	6	Finland	8.55	8.32	41	38	Brazil	5.29	5.07
8	10	Australia	8.50	8.22	42	39	Argentina	5.27	5.05
9	12	Canada	8.37	8.03	43	41	Jamaica	5.03	4.82
10	6	Hong Kong	8.36	8.32	44	42	Bulgaria	4.86	4.68
11	9	Norway	8.35	8.27	45	43	Turkey	4.77	4.58
12	12	Germany	8.34	8.03	46	46	S. Arabia	4.67	4.38
13	11	Singapore	8.24	8.18	47	44	Thailand	4.63	4.56
14 (tie)	16	New Zealand	8.19	7.82	48	45	Venezuela	4.47	4.53
14 (tie)	14	Austria	8.19	8.01	49 (tie)	50	Peru	4.44	4.07
16	15	Ireland	8.09	7.98	49 (tie)	47	Romania	4.44	4.19
17	17	Belgium	7.99	7.71	51	48	Colombia	4.41	4.18
18	18	South Korea	7.90	7.66	52	52	Russia	4.30	3.98
19	19	France	7.86	7.61	53	49	India	4.25	4.17
20	–	Bermuda[a]	7.81	–	54	–	Jordan[a]	4.22	–
21	21	Japan	7.77	7.42	55	53	Egypt	4.14	3.90

Table 3: Summary of e-readiness (continued)

2006 e-readiness rank (of 68)	2005 rank	Country	2006 e-readiness score (of 10)[a]	2005 score	2006 e-readiness rank (of 68)	2005 rank	Country	2006 e-readiness score (of 10)[a]	2005 score
22	20	Israel	7.59	7.45	56	51	Philippines	4.04	4.03
23	22	Taiwan	7.51	7.13	57	54	China	4.02	3.85
24	23	Spain	7.34	7.08	58	55	Ecuador	3.88	3.83
25	24	Italy	7.14	6.95	59	56	Sri Lanka	3.75	3.80
26	25	Portugal	7.07	6.90	60	58	Nigeria	3.69	3.46
27	26	Estonia	6.71	6.32	61	57	Ukraine	3.62	3.51
28	27	Slovenia	6.43	6.22	62	60	Indonesia	3.39	3.07
29	28	Greece	6.42	6.19	63	63	Algeria	3.32	2.94
30	–	UAE[a]	6.32	–	64	62	Kazakhstan	3.22	2.97
31	31	Chile	6.19	5.97	65	59	Iran	3.15	3.08
32 (tie)	29	Czech Rep.	6.14	6.09	66	61	Vietnam	3.12	3.06
32 (tie)	30	Hungary	6.14	6.07	67	64	Pakistan	3.03	2.93
34	32	Poland	5.76	5.53	68	65	Azerbaijan	2.92	2.72

a: New to the annual rankings in 2006

US = United States, UK = United Kingdom, UAE = United Arab Emirates

Source: Economist Intelligence Unit 2006

The impact of multidisciplinary technological developments is likely to affect social, economic, political and personal spheres of life. This impact may be tempered or facilitated by a number of concomitant factors including acceptance of technological change, the level of available technology and related infrastructure investment and the nature of technological developments. The variance in such factors at the global level may result in differing implementation and effects of technology and create related issues of potential concern. The technology revolution that is creating the future digital environment is deemed to involve consequences beyond the simple creation of products and services. Those products and services will have a direct impact upon the way in which people interact and work, e.g. mobile workforce and the social networking sites being more popular.

Outsourcing of information technology operations

The growing acceptance of the internet as a communication tool and the tendency of corporations to locate their operations in developing countries with cheaper labour costs have resulted in an increasing number of outsourced operations being conducted offshore. According to Colwill and Gray (2007), '[g]lobalisation has had a fundamental impact on the way that business is conducted and approaches to sourcing work have evolved. Outsourcing is here to stay and the proportion of worldwide spend in this market-place will continue to rise.' Trends in outsourcing have recently moved from outsourcing peripheral business functions to much more vital business functions, particularly IT operations (Hoecht & Trott 2006, Quelin & Duhamel 2003). Outsourced IT operations include database administration, IT helpdesk, software maintenance, third party software development, applications management, business analysis, IT consultancy, IT project management, IT program management and systems integration, and technical specialisms (Colwill & Gray 2007).

Outsourcing of IT operations offshore is a key driver of the new post-dot-com era of the global IT industry. Several organisations have established their support, research and development facilities in lower-cost countries particularly China and India. Examples include Microsoft Asia and Hewlett-Packard research laboratories both based in Beijing, and IBM India research laboratory in Delhi. In Australia, Qantas announced in October 2006 that the airline would be moving its IT development offshore to India (Crawford & Pauli 2006).

Offshore outsourcing, particularly to lower-cost countries, is likely to increase in the next two years. According to Erber and Sayed-Ahmed (2006), 'globalisation in IT is driven by cost optimisation: the expected cost savings of up to 40 percent by offshore outsourcing IT services are simply too compelling to be ignored in today's economy'.

In fact, McDougall (2004) predicted that more than 3.4 million United States service sector and IT jobs are likely to be located offshore by the end of 2015 and Soat (2004) suggested that government spending on outsourced IT functions will increase to $17.4 billion by 2009. Global outsourcing trends beyond the next two years will also include computer game development. Such development will be increasingly outsourced to studios around the world that specialise in specific aspects of games creation, such as cinematic, full-motion video and motion capture.

Possible security threats to outsourced operations

There are, however, security risks associated with outsourced operations. The security of the outsourced IT services (e.g. effectiveness, efficiency, adequacy, integrity, validity, authorisation and privacy) depends on the offshore operations. In general, security risks faced by both onshore and offshore operations are similar, such as the various key factors identified in computer security assessments as responsible for electronic attacks (e.g. poor security cultures within organisations, inadequate human resources to enable system hardening, and the exploitation of unpatched or unprotected software vulnerabilities). These factors include:

- **Failure to report attacks** often means that those responsible for the attack are not prosecuted and remain free to re-offend either against their current or future employers.
- **Failure to upgrade security arrangements** regularly means that systems that initially may have been secure become less so over time. This could result in data compromise and information leak at offshore entities.

  For example, a 2006 incident demonstrating the ease with which identity thieves can obtain credit card details of 200,000 banking customers in Bangalore (Crawford & Pauli 2006) is a reminder about the risk of information leakage at offshore operations. The information obtained could subsequently be used to facilitate identity theft and commit fraud.

  A further example is the case of Terrence D Chalk and Damon T Chalk, of New York. Both were indicted for making false statements on applications for loans, lines of credit and credit cards using personal identification information of Chalk employees or clients without their knowledge or permission (Duo charged in credit card fraud scam 2006).
- **Loss or misappropriation of IP rights**, particularly to countries with an inadequate legal system for protecting them (see ‘Industrial espionage’ below), could result in loss of technology-based competencies.

Outsourcing involves transfer of a significant amount of management control to offshore vendors and this usually results in diminished control over security arrangements. The benefits of offshore outsourcing can easily be offset by these risk factors if they are not properly addressed at the outset of any outsourcing venture. A report by Ernst and Young (2006) further suggested that more organisations with outsourced vendors need to adopt and validate formal procedures for vendor risk management, given only 6 percent of the responding organisations use formal procedures, validated by a third party to manage risks with vendors and 21 percent do not address the issues at all. There is also the possibility for vulnerabilities to be clandestinely introduced into software developed offshore, either by corrupted offshore employees or by foreign intelligence agents.

To ensure regulatory compliance (e.g. proper data access, usage, storage, sharing, and transmission), protocols and legislation must be in place to continuously monitor and manage offshore vendors and the outsourcing relationships, perhaps through legally binding contractual arrangements such as service level agreements and key performance indicators.

Expansion of wireless and mobile technologies

Wireless technologies have advanced with great speed in the past few years. The capacity and performance of wireless communications systems have improved exponentially, as has the range of information and services that can now be accessed using mobile devices due to their pervasive, anytime and anywhere, connectivity. Enhanced computational capabilities in mobile devices (e.g. mobile phones and other handheld devices) greatly increase the amount of information to be retrieved, stored and transmitted in real time.

Such information includes text, audio and video data. Witness the ease with which today's mobile phone users are able to converse by voice, email or SMS; take and transmit digital photographs; stream audio and/or video files; upload/download a range of material directly via the internet; and conduct mobile-commerce (m-commerce) transactions. The January 2007 launch of Apple's iPhone – a combination of mobile phone, iPod and instant messaging – and the proposed launch of Windows' Mobile 6 around May 2007 at the 3GSM World Congress Telecommunications Conference 2007 signal the trend of mobile and wireless technologies within the next two years.

The wireless and mobile technologies revolution will continue as more users adopt mobile and wireless systems, both for personal uses and in business dealings. A Gartner Research report (Gutberlet 2006) estimated that, as at December 2005 the total mobile service revenue worldwide is US$610 billion. In 2007 Optus announced that between $500 and $800 million would be invested to enhance their existing third-generation networks over the next three years (Optus to pour $800m into 3G network 2007). Given the plethora of wireless and mobile technologies, disintermediation (where the physical contact between organisations and their clients is replaced by virtual contact) in business sectors including banking is set to increase. In December 2006, Google™ reportedly signed an agreement to provide mobile search services for China's biggest mobile phone operator, China Mobile, where subscribers can search for news, videos and other content from their mobile phone (Niccolai 2007).

Multiple wireless providers and access points are increasingly servicing major cities, so that wireless devices can be used from almost any urban location. For example, up to half of all broadband-connected households in some countries today have wireless access. In Australia, no limit has been placed on foreign equity ownership (e.g. Vodafone and SingTel) and the number of carriers that can be licensed to operate. The number of internet subscribers in Australia reached approximately 6 million in mid 2005, with strong growth in the proportion of non-dialup subscribers, such as integrated service digital network and digital subscriber line broadband connections (ABS 2005). Many households and businesses have introduced some elements of wireless connectivity into their networks either through fixed wireless or mobile wireless (hotspot) internet access, although direct wireless access to internet service providers (ISPs) remains less common. Other applications of wireless connectivity include automated transmitting technologies such as radio frequency identification (RFID) and other identification and access devices used in transport and building security. Table 4 describes the various standards for wireless connectivity.

Table 4: Types of wireless connectivity

Abbreviation	Name	Example	Distance
WWAN	Wireless wide area network	GSM mobile phones, 3G mobile phones	10 km
WMAN	Wireless metropolitan area network (IEEE 802.16)	Suburb of city connected to the internet at broadband speeds	1 km
WLAN	Wireless local area network (IEEE 802.11)	Local area network on the floor of a building connecting all workstations and servers	100 m
WPAN	Wireless personal area network (Bluetooth, Infrared)	Connecting and controlling various products and devices	1 m

Note: Terminology varies and further technical variations exist within each of these categories. For example, WMAN is also known as WiMAX (worldwide interoperability for microwave access). WPAN uses IEEE 802.15 standard (which includes Bluetooth from June 2002) and IEEE 802.15.3a (known as Ultrawideband). WWAN includes wide coverage area technologies such as 2G cellular, cellular digital packet data (CDPD), global system for mobile communications (GSM), general packet radio service (GPRS) and Mobitex. WMAN along with mobile broadband wireless access (MBWA) includes 802.16 and emerging standards such as 802.20

Sources: adapted from NIST 2006b, TISN 2006c

The range of some of these technologies means that networks can now be accessed from previously unconnected locations. For example, travellers using wireless-enabled laptops and other mobile devices can now connect to their offices and exchange data from the comfort of an airliner flying at 10,000 metres above land (TISN 2006b). Technological changes such as these can have significant effects on behaviour (Urbas & Krone 2006).

Behavioural changes

As more people become connected online through mobile technologies, there is evidence of a shift in behavioural patterns, including social interaction. This is particularly so in the ways in which the demarcation between public and private space is understood. Davis and Pease (2000) have observed that:

> [t]here are increasing opportunities for people to be isolated in public space. Business, inter-personal and entertainment activities have moved from the social and static to the personal and mobile. People have greater choice as to who they 'meet' and how. Physical society may, therefore, become a more hostile place, through which people travel rather than in which they expect to interact. In a dehumanised environment, people may become less 'real' to one another, leading to more extreme reactions and interactions.

Part of this social change is illustrated by behavioural patterns associated with mobile phone usage, whereby many people conduct private conversations in public places with little regard for their own privacy or security (or the sensitivities of those around them). To an increasing extent, mobile access to the internet is also shaping behaviour in public:

> As the internet becomes more pervasive, a blurring will occur between online and the 'real world'. It will become commonplace for people to store many personal items online. It will also affect socialising, in terms of the places where people congregate and the people with whom they interact (Isobar & Yahoo 2006).

These behavioural aspects of new technologies are not only interesting from a sociological perspective but also in terms of the criminal opportunities they create to exploit the security vulnerabilities that mobile and wireless networks entail. These opportunities can be understood in terms of the benefits and risks associated with the technologies.

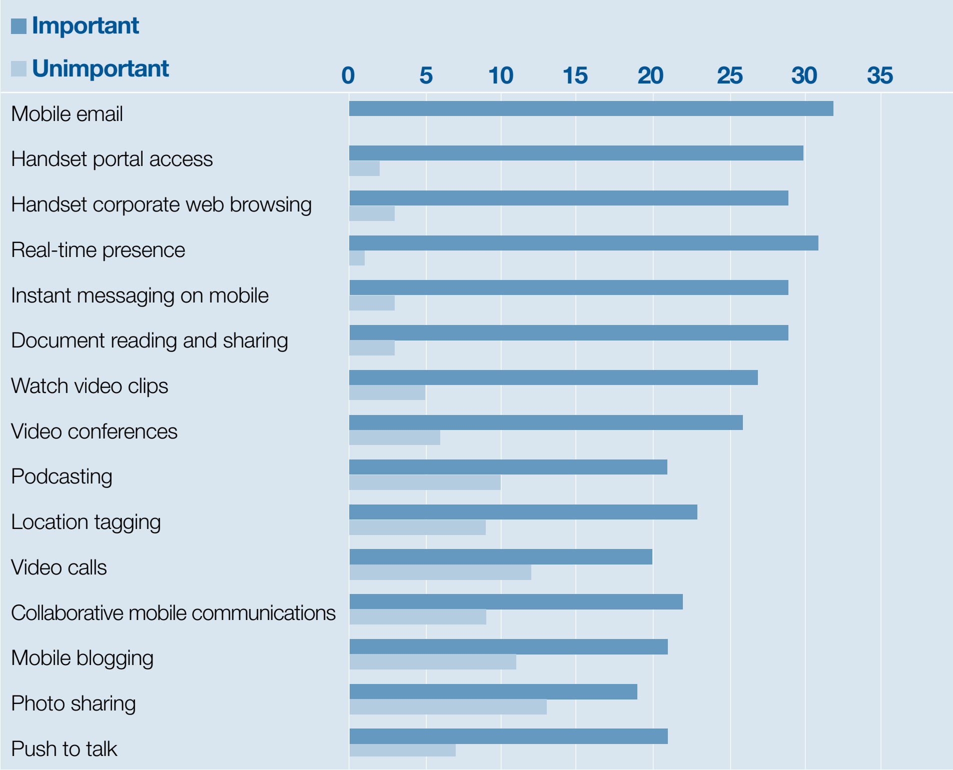
Further developments in wireless and mobile technologies

Investment in network expansion by telecommunications companies will see a further expansion in capacity that will result in an increase in bandwidth availability and greater adoption of wireless and mobile technologies. Mobile communications will also be facilitated through a combination of low and high orbiting satellites.

Working and networked mobility are enduring characteristics of today's knowledge-based society; enhanced wireless communication systems will continue to result in a significant transition from e-commerce to m-commerce. The trend of workers becoming more mobile is likely to continue and consequently, mobile and wireless devices, such as mobile phones and PDAs equipped with global system for mobile communications/general packet radio service (GSM/GPRS), will become increasingly important tools for assessing information when personal (desktop) computers are unavailable. Mobile devices and networks will continue to become more capable and better able to support a wide range of communication and collaboration functions (Jones 2006); and key technologies will include third-generation and fourth-generation networks, smart-phones and wireless PDAs.

Based on a relatively small number of attendees at a presentation on mobile collaboration, Gartner Research's survey (Jones 2006) results – as depicted in Figure 1 – suggests that mobile devices and systems are likely to play a major role in future collaborative knowledge work.

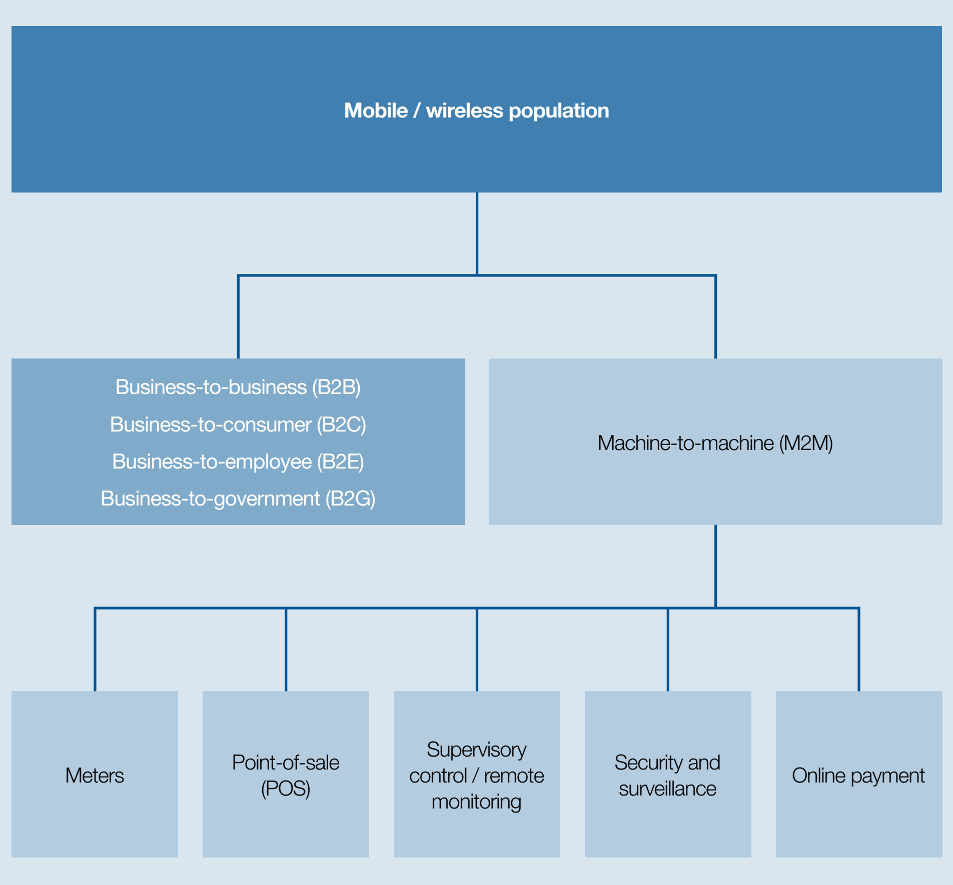
Figure 1: Mobile collaboration survey (number)



Source: Adapted from Jones 2006: 3

The use of mobile phones in developing countries has, as of 2005, reportedly exceeded 1 billion (Gohring 2006). Market demand will continue to drive overall mobile subscription growth in the next two years. For example, market demand for mobile content that includes mobile adult material has been estimated to be worth approximately US$3.3 billion by 2011; up from its current level of US$1.4 billion (Ryan 2006). Another Gartner research report (Clark 2006) predicted that, by the year 2009, an estimated 70 percent of the modern workforce would go mobile or wireless. The popularity of the machine-to-machine e-commerce model, introduced in the same report (as depicted in Figure 2), is likely to increase in the next two years.

Figure 2: Mobile and wireless taxonomy


Mobile / wireless population
Business-to-business (B2B)
Business-to-consumer (B2C)
Business-to-employee (B2E)
Business-to-government (B2G)
Machine-to-machine (M2M)
Meters
Point-of-sale (POS)
Supervisory control / remote monitoring
Security and surveillance
Online payment

Source: Adapted from Clark 2006: 3

Possible threats

The technological capabilities of telecommunications devices will grow exponentially and it is inevitable that such advances will be passed on to both businesses and consumers. Although efforts are being made to ensure that new systems have appropriate security measures in place, risks will arise from users not having the requisite levels of security awareness and not fully understanding how new security measures can be used to their advantage. Some new technologies (such as VoIP over wireless local area networks based on the IEEE 802.11 specifications and trusted platform such as Microsoft Vista) may have effective security measures enabled, but consumers might not use them to their full extent.

As businesses continue to engage in e-commerce and m-commerce, they will become increasingly global and interconnected. This will enhance the risks of identity-related financial crime through the use of modern technology. Wireless and mobile technologies are examples of possible threats in the next two years.

MOBILE DEVICES

The increasing use of mobile devices such as mobile phones and PDAs, with ever-increasing storage capacity, constitutes a key threat for the future. Such devices will continue to be used to store unencrypted personal data as well as corporate information. The ease with which erased data on such devices can be recovered increases their attractiveness to criminals.

Moreover, advances in third and fourth generation wireless technologies that offer high speed data access and the widespread dissemination of Bluetooth-enabled mobile phones will increase the popularity of multimedia services, such as multimedia messaging services (MMS). Criminals and malware writers could potentially target the latter. For example, Mulliner and Vigna (2006) have detailed the proof-of-concept code that shows how vulnerabilities can be exploited in the MMS in mobile phones that run mobile versions of Windows.

INSTANT MESSAGING

Popular internet-based instant messaging programs, such as Microsoft's MSN, Yahoo!®'s Messenger, America Online (AOL)'s Instant Messenger (http://www.aol.com.au/site/website/aolproducts/aim/index.php) , ICQ (http://www.icq.com/) and Internet Relay Chat (IRC) are estimated to have more than 800 million active user accounts (Gutberlet 2006). Tencent QQ (http://im.qq.com), one of the most popular instant messaging programs in China, is estimated to have more than 22.4 million users (Wang & Wang 2006). Proliferation of instant messaging programs constitutes another threat for the future. Malware authors will continue to target instant messaging programs with malicious code such as W32.heartworm (a worm that installs files on victims' computers that records personal and financial information) and Pipeline (a worm that installs rootkits and Trojans on systems running AOL's Instant Messenger programs), and potentially unwanted application such as Winfixer (that falsely warns the computer has been infected with malware in order to ask users to buy a program to remove said malware). Botnets, one of the internet's biggest threats, will also target instant messaging and other peer-to-peer networks for command and control of infected systems. This will allow command and control servers to be arranged in a distributed structure to limit traceability by law enforcement and forensic investigators.

WIRELESS NETWORKS

Wireless networks themselves create a number of vulnerabilities. Key among these is the fact that networks and their data can be accessed without physical access being required. This facility assists both the user and the criminal. The advent of wireless networking increases the likelihood of such information and associated tools being uploaded and downloaded. Enhanced methods of exploiting wireless vulnerabilities include drive-by subversion of wireless home routers through unauthorised access by mobile Wi-Fi clients (Tsow et al. 2006) and other forms of attacks. These include eavesdropping and sniffing of the VoIP calls, man-in-the-middle attacks, denial-of-service attacks, call interruption, and making 'free' calls on VoIP network built over wireless local area networks (Me & Verdone 2006).

Digitisation of information: increased data holding and dissemination capabilities

Digital content – also known as electronic content, IT content and electronically stored information – can be broadly defined as information and data extracted from a computer or electronic storage media (Standards Australia International 2003). A 2003 study by researchers from University of California at Berkeley indicated that information is increasingly being stored or archived in electronic forms; indeed, in 2003, approximately 92 percent of data was created in electronic-only form, particularly on hard disks (Lyman & Varian 2003). This is, perhaps, not surprising considering that digital content today can be disseminated expeditiously across different jurisdictions and stored safely in inexpensive portable devices, such as magnetic tapes and optical hard disks, portable computing devices including digital cameras, mobile phones, MP3 players and high-capacity memory sticks (e.g. USB drives).

Future technological innovations and the decline in prices of electronic data storage devices will continue to lower entry barriers for digitisation of information. In the next two to five years, the size and capability of data storage devices will also be enhanced by advances in technologies, such as perpendicular storage techniques, holographic media storage techniques,

> heat-assisted magnetic recording and patterned media. These approaches could increase hard-disk storage densities from today's 100 gigabits per square inch to perhaps 100 terabits per square inch … New approaches could also increase data-transfer rates from the maximum 300 megabytes per second of today's hard drives (Lawton 2006:19).

The exponential rise in information transfer and storage capacities will lead to enhancements in database technology which will improve the manner in which increasing volumes of data are categorised, stored and extracted. Such databases containing sensitive personal data provide criminals with financial incentives to offend as data obtained from the databases can be used to facilitate other technology-enabled crimes. For example in 2005, Professor Avi Rubin of Johns Hopkins University designed a graduate course 'Security and Privacy in Computing' project to demonstrate how a database can be built to facilitate identity theft (Rubin 2005).

One important development will be an increase in the use of 'agile' databases in which large warehouses of data are drawn upon as and when necessary, rather than being stored on discrete personal or business databases. These developments will result in even greater access to the internet by individual and organisational users, and enhanced use of communication vehicles such as email, instant messaging and high-speed connectivity.

New ways of accessing and sharing information electronically

Ease in accessing and sharing content electronically offers governments and businesses the opportunity to engage the public online and to bridge the gap between sectors. The emerging trend of individuals using the internet to access public-domain services in preference to more traditional offline modes will increase the popularity of digital content in e-commerce, e-government and social-related activities. Examples include:

- **e-tendering:** In the New South Wales Government e-tendering system (https://tenders.nsw.gov.au/nsw/index.cfm), expressions of interest or other such public calls are released by a principal entity inviting other interested entities to tender their submissions before the specified tender closing date. Within a specified period of the tender closing date (e.g. seven working days), the names and addresses of all responding entities will be disclosed unless this would reduce competition in the e-tender process.
- **e-voting:** The Victorian Electoral Commission allows Victorian voters to use designated voting kiosks to cast electronic votes from 13 November 2006.
- **e-reporting:** The United States-based Internet Fraud Complaint Center allows anyone to report information pertaining to online fraud activities. This information is subsequently evaluated and referred to the appropriate agency or jurisdiction.

The increasing popularity of second generation of internet-based services – emphasising online collaboration and sharing among users (i.e. Web 2.0) and supporting virtual communities – will result in new ways of assessing and sharing information electronically, such as:

- **Online chat rooms and social networking sites:** Popular online chat rooms and social networking sites such as Friendster and Myspace allow users to post their personal details and photographs and also interact with other users in real-time.

Information on such sites could be used to identify or profile a particular user and it has been known that such sites can be exploited by malware authors to, for example, increase the yield of phishing attacks as described in the next chapter. Online sexual predators have also been known to make use of chat rooms. In the first investigation leading to prosecution and sentence under s218A of the *Criminal Code Act 1899* (Qld) after it came into effect on 1 May 2003, Queensland investigators posed as a 13 year-old girl (becky_boo 13) in a chat room and received emails from a man wanting to engage the girl in sexual activity. They arrested a 25 year-old man when he appeared at an agreed meeting point to meet the girl. After a guilty plea, the defendant was sentenced to imprisonment for two and a half years, suspended after nine months. This was reduced on appeal to an 18-month term, suspended from the time of the appeal, the defendant having already served 90 days in custody (*R v Kennings* [2004] QCA 162). In another more recent case, Richard Gerard Meehan was charged with one count of using a carriage service – internet chat rooms and mobile phone text messages – to transmit communications to a person under 16 years of age with the intention of procuring that person to engage in sexual activity, contrary to ss474.26(1) of the *Criminal Code Act 1995* (Cth). On 21 July 2006, Meehan was sentenced by the Victorian County Court to 24 months' imprisonment, to be released after having served three months of that term (Hoare 2006).

The House of Representatives in the United States approved the *Deleting Online Predators Act 2006*, which requires schools and libraries in the United States to block access to such sites. Pieces of personal information obtained from social networking sites could also facilitate identity theft (Parker 2007).

Terrorists could, potentially, use online chat rooms and social networking sites as vehicles to reach an international audience, solicit funding, recruit new members, and to distribute propaganda. In March 2007, Singapore's Deputy Prime Minister and Minister of Home Affairs told Parliament that the Internal Security Department of Singapore has investigated internet-driven radicalisation cases involving 'Singaporeans who had become attracted to terrorist and radical ideas purveyed in the mass media, particularly the [i]nternet' (Ahmad 2007).

- **Online gaming:** Online games typically played via the local area network and internet form part of a growing industry. Games, particularly massively multiplayer online games (MMOG) and massively multiplayer online role-playing games (MMORPG), that allow players to compete with and against each other on a grand scale in real-time, such as Half-Life, Second Life and Warcraft, are likely to remain popular with the digital generation.
- **Online video sharing websites:** An example of a popular online video sharing website is YouTube (http://www.youtube.com/) that allows users to watch, upload and share videos online. Law enforcement agencies can also use YouTube as an investigative tool to disseminate information to the public, particular the digital generation. For example, in December 2006, Canadian police posted surveillance video of a murder case that

took place in a bar located in Hamilton, Ontario (YouTube turned crime-fighter in Canada 2006). YouTube can also be used as a channel to bring matters of public interest to the attention of law enforcement agencies. Examples include:

- The Los Angeles Police Department and the FBI commenced an internal investigation after video footage was uploaded to YouTube showing two police officers allegedly beating a man during an arrest (Winton & Hong 2006).
- In February 2007, three men were arrested and charged with possessing a thing (spray paint) with the intention to damage, enter and remain on running rail lines, and two counts of malicious damage, after one of the offenders uploaded the video, filming the act of spraying a CityRail train, to YouTube (Baker 2007).

Online video sharing can, however, be exploited to host offensive content. A recent example is a three-minute video 'lebothugs', uploaded to YouTube in November 2006 that was reportedly watched more than 8000 times.

> [t]he video is backed by a rap song and includes an image of Skaf with a rifle on his lap, footage of a Cronulla riot revenge attack, a photo montage of a group referred to as the 'Soldiers of Granville Boys', and a map of Australia in the colours of the Lebanese flag with the words 'under new management'. Another scene shows a school shirt with a knife on it. (Gibson & Creagh 2007)

Online video sharing can also be exploited as a means to distribute malicious code (e.g. embedded malicious code in MPEG files).

- **Online photo and image sharing websites:** Websites such as http://www.polarrose.com allow users to upload and share photos and images online. Instead of embedding image spam in email, spammers could abuse online photo sharing sites by posting image spam on such sites and embedding the links to the posted image in the email. Using facial-recognition technology, some sites (e.g. Polar Rose website) allow users to search uploaded photos and images based on facial attributes. This could, however, be abused by criminals and individuals to track and stalk their victims online and across websites.
- **Weblogs (Blogs):** Blogs are an emerging form of modern day communication (Rosenbloom 2004, Vogelstein et al. 2005) that allow internet users to disseminate and share information and ideas. Various communities have emerged in the blogosphere (the world of blogs) ranging from technical support communities, such as Google™ blogs (http://googleblog.blogspot.com/), through groups of bloggers who are known to each other, to hate blog groups formed by bloggers who are racists or extremists (Chau & Xu 2007). In fact, it has been predicted that blogs and Wikipedia will dominate the Web 2.0 landscape in 2007 (Hinchcliffe 2006); the number of bloggers in China is estimated to be 20.8 million (China tops 20m bloggers 2007).

Blogs can, however, be abused to leak proprietary or confidential information, and post defamatory content. There have been reported cases of employees losing their jobs for violating company policies when they posted information pertaining to their jobs on their blogs; such an activity is known as 'dooce dodging'. The United States Army has established the Army Web Risk Assessment Cell to review the content on publicly accessible websites including blogs to prevent leakage of confidential information (EFF 2007, United States Army 2004).

Blogs such as Google's Blogger.com have recently been used as vehicles to direct unsuspecting users to phishing sites (Fortinet 2007). Blogs can also be compromised by criminals and malware authors exploiting vulnerabilities of web servers or operating systems to host malware (e.g. ransomware and self-mutating Trojan malware). Unsuspecting users' computers can be infected by malware when they visit these compromised blogs (by exploiting vulnerabilities of web servers or operating systems) that host malware (e.g. ransomware and self-mutating Trojan malware).

Blogs can be used to host offensive content including racial vilification material and insensitive statements about a particular segment in the population. For example, in October 2005, two Singaporeans were convicted under s4(1)(a) of the Sedition Act for posting invective and pejorative remarks on their blogs and a general discussion forum on the internet – see *Public Prosecutor v Koh* (2005) DAC 39442 and *Public Prosecutor v Lim* (2005) DAC 39444.

- **Wikis (such as Wikipedia):** Implementation of wikis includes Intellipedia, used to disseminate and share intelligence among the 16 United States intelligence agencies (Shrader 2006). Wikis could potentially be exploited by posting malicious content or sensitive information. Examples include a link to the Blaster worm, disguised as a fix to the malware, posted on the German edition of Wikipedia (Leyden 2006b) and a link to the internal documents of global pharmaceutical company, Eli Lilly, alleging that the company was deliberately downplaying the side effects of the drug Zyprexa was posted on the Wiki site http://zyprexa.pbwiki.com/.
- **Digital television (or internet television):** Research by the Australian Communications and Media Authority (ACMA 2006) indicated that, as at mid 2005, approximately 41 percent of Australian households had some form of digital television. Gartner research (Dulaney & Hafner 2006) and Microsoft chairman Bill Gates (Reuters 2007) also suggested a similar trend; increasing popularity of internet television. This will potentially be another target for distributed denial-of-service attacks and online extortion.

Networked technology will continue to evolve through the use of increasingly faster fibre optical systems that will improve transmission of data within and across networks. Future developments in computing such as web services, such as service-oriented architecture, that provides a framework for building, running, and managing services, and the combination of optical and silicon technologies to facilitate data transfer within chips via laser will also increase the popularity of electronically stored information. Developments beyond the next two years in nanoscience and nanoengineering will increase the use of micro-electromechanical systems that combine electrical and mechanical components to enhance information storage, processing and communication.

New payment methods

ICT has a wide-ranging influence on how the banking and finance industry operates. This includes customer service (e.g. internet banking, electronic securities trading and electronic payment systems) and business operations (e.g. electronic clearing and settlement). Electronic-based transactions have increased considerably in countries such as the United States (FRS 2004) and the United Kingdom (Conroy 2006).

In Australia, the volume and value of cheque transactions in paper-based clearing systems fell from an average of 2.7 million per day in 2001 to 2.1 million in 2005 and from an average of $8.3 billion per day in 2001 to $6.3 billion in 2005 (APCA 2005) while a considerable increase in electronic banking has been observed. This is hardly surprising as the cost of an internet-based transaction is a fraction of what 'bricks-and-mortar' based transactions cost (De Young 2001). The propensity for consumers to buy online was indicated in a report that online spending on retail websites in the United States has exceeded US$100 billion (Ames 2007).

ELECTRONIC PAYMENT SYSTEMS

Electronic payment systems can be broadly categorised as (AIC 2007a):

- **Software-based or hardware-based:** The former scheme, implemented in software-only form, includes virtual currency used in MMOG and MMORPG. Hardware-based money (or card money) includes bank-driven and bank-backed key stored value systems such as Mondex, VisaCash, NETS cashcard (Singapore) and NTT's NCash (Japan).
- **Online-based or offline-based schemes (based on the type of payment validation):** In the former scheme (e.g. BPay), issuing banks have to be contacted at the point of purchase to provide authorisation when payments are made. Offline-based schemes, on the other hand, provide offline authorisation capability where validation is made based on information contained on the card (e.g. pre-paid cards including Mondex, VisaCash, NETS cashcard and NTT's NCash).
- **Picopayment, micropayment or macropayment systems (depending on the dollar amount of transactions):** Requirements for these systems differ. To be viable, picopayment and micropayment systems need to be efficient, low-cost and secure. Due to the larger amount of transactions involved, macropayment systems typically require higher level of security and non-repudiation of transactions.

Increased dependence on global electronic payment systems and the ability to move large amounts of money expeditiously across different jurisdictions exposes both payment processing companies (payment bureaus) and consumers to an evolving spectrum of threats. For example, in 2004, concerted distributed denial-of-service attacks were launched against the website of a London-based online payment processing company, Protx, after the company refused to pay online extortionists.

ELECTRONIC CASH (E-CASH)

Electronic cash (e-cash), first introduced by Chaum (1982), is primarily designed to retain the same properties as physical cash. That is:

- **untraceability** – it offers users unconditional anonymity
- **unlinkability of payments** – one is unable to identify whether payments originated from a particular customer account
- **unforgeability** of e-cash
- **protection** against double-spending to different payees and to the same payee.

Unconditional anonymity and unlinkability, however, could be abused to facilitate money laundering and other crimes such as fraud as it prevents the monitoring of financial transactions. In order to minimise the risk of money laundering, e-cash schemes require a 'traceability against dishonest users' feature (e.g. escrowed cash systems). In escrowed cash systems, a trustee is able to revoke anonymity when triggered by suspicions about transactions or if transactions exceed $10,000 (the point where a report must be filed with the relevant authority). Moreover the ability to trace dishonest users may allow victims (e.g. banks) to initiate litigation to recover financial losses resulting from fraud and double spending.

Despite widespread support for e-cash among cryptography and security researchers, e-cash has not been widely adopted in the industry, arguably due to the lack of a common standard.

ELECTRONIC PURSES, SMARTCARDS AND PREPAID CARDS

Electronic purses, electronic wallets, smartcards and prepaid cards, which have been adopted in many countries, are typically used for micropayments in view of their limited storage capacity. In October 2006, the Royal Bank of Scotland conducted a trial of the contactless Europay, MasterCard and Visa standards consortium debit cards. The NETS cashcard is also currently used in Singapore. The cashcard can be used to pay any amount up to a limit of S$500 such as paying fines, and buying food and other small-value consumer items. The cashcard can be topped up at various places including automated teller machines and designated convenience stores.

The anonymity offered by pre-paid cards could be abused for illicit financial transactions, money laundering and bulk cash smuggling particularly as value limits increase. For example, a former employee of the Ohio Bureau of Motor Vehicles was paid using US$10 phone cards for her role in selling fraudulent Ohio driver's licences (US ICE 2005); and a United States National Drug Intelligence Centre report (US NDIC 2006) identified pre-paid cards as a potential tool for laundering drug proceeds.

The future will see the development of new hardware devices and software programs that seek to compromise the quality of data-protection mechanisms used in electronic purses, electronic wallets, smartcards and prepaid cards. For example, researchers from the University of Massachusetts Amherst, RSA Laboratories and Innealta Inc. (affiliated with the RFID Consortium for Security and Privacy) studied 20 different RFID-enabled credit cards issued in the United States by Visa, Master Card and American Express. The study found that:

> (1) the cardholder's name and often credit card number and expiration are leaked in plaintext to unauthenticated readers, (2) our homemade device costing around $150 effectively clones one type of skimmed cards – providing a proof-of-concept of the RF replay attack for cards, (3) information revealed by the RFID transmission cross contaminates the security of non-RFID payment media, and (4) RFID-enabled credit cards are susceptible in various degrees to a range of other traditional RFID attacks such as skimming and relaying (Heydt-Benjamin et al. 2007).

MOBILE PAYMENTS (M-COMMERCE)

Micropayments can also be made using mobile phones (e.g. Telstra's 'Dial a Coke' service in Australia and Vodafone's m-PayBill service in the United Kingdom) and other wireless communication devices (via wireless application protocols). Mobile payment initiatives include:

- The **Mobile Visa wave payment scheme** in Malaysia launched by Visa International, in collaboration with Maybank Malaysia, Maxis Communications Berhad (Maxis) and Nokia, in April 2006 (Glenbrook Partners 2006, Visa Southeast Asia 2007). In this system, subscribers are able to logon to their online banking site to program their mobile phones with their credit card details to enable mobile payments to be made.
- **BankID** launched by Norway's banking industry in October 2006 allows subscribers to be authenticated while on the move to facilitate mobile payments and signing of contracts.
- The **mobile banking** service recently launched by the Argentine bank Banco Francs and the mobile operator Movistar Argentina allows subscribers to use the SMS service to make micropayments, bank transfers and requests for information (Banco Francs launches m-banking with Movistar 2007, Mobile Payments World 2007a).
- **PayPal** mobile that allows money to be sent to friends and family and payments using SMS on mobile phones.

- The **M-Pesa** service developed by Vodafone was recently launched in Kenya allows subscribers to send cash to other telephone users using SMS (Vodafone 2007, Guardian News & Media 2007).

Advances in near-field communications technologies, third- and fourth-generation wireless telephony that offer high speed data access and widespread dissemination of Bluetooth-enabled mobile phones will increase the popularity of mobile gaming, and mobile and contactless payments.

> With adoption driven by some of the world's largest card associations and banks, wireless operators and merchants, spending on contactless payments hardware and software will reach $870 million by 2011, up from just $260 million in 2006, amounting to a compound annual growth rate of 27 percent, according to a new study from ABI Research (Mobile Payments World 2007b).

There are, however, potential risks including fraudulent services charges to both carriers and to end users, malware and malicious code targeting mobile devices (e.g. mobile phone viruses such as crossover, SymbOS.Cardtrp and the Viver Trojan) and wireless security threats.

DIGITAL PRECIOUS METALS

Digital precious metals, a relatively new way of transferring value online (FATF 2006), enable users to secure cash deposits against precious metals held offshore. Before trading online, users establish online accounts by providing their name, email address and physical address. The required identification, however, can be easily fabricated and some digital precious metals allow users to establish anonymous accounts.

As a result it is likely that such systems could be used to facilitate money laundering and terrorist financing, perhaps with the assistance of an exchange agent such as shell corporations. For example, e-gold (a digital currency offered by E Gold Ltd) has been one of the avenues used by organised crime group, Shadowcrew, members to send and receive payments for illicit merchandise and services (US DoJ 2005).

> E Gold has been a highly favored method of payment by operators of investment scams, credit card and identity fraud, and sellers of online child pornography. The indictment alleges that the defendants conducted funds transfers on behalf of their customers, knowing that the funds involved were the proceeds of unlawful activity; namely child exploitation, credit card fraud, and wire (investment) fraud; and thereby violated federal money laundering statutes (US DoJ 2007b).

On 24 April 2007, E Gold Ltd; Gold & Silver Reserve, Inc and their owners were indicted on charges of money laundering, conspiracy, and operating an unlicensed money transmitting business in the United States (US DoJ 2007b).

ONLINE GAMING AND GAMBLING

Online gaming, typically played via local area networks and the internet, is a growing industry. Major online gaming vendors include Microsoft (Xbox) and Sony (Playstation). Broadband connection, technological innovations and a reduction in the price of electronic data storage devices continue to lower entry barriers for new entrants into the gaming industry and contribute to the richness and diversity of gaming content. Games, particular MMOG and MMORPG, are increasingly gaining popularity with the digital generation. MMOG and MMORPG allow players to compete with and against each other on a grand scale in real-time.

> Not only do MMORPGs appeal to a broad age range (M age = 26.57, range = 11–68), but the appeal is strong (on average 22 hours of usage per week) across users of all ages (r = -.04) ... MMORPGs are not simply a pastime for teenagers, but a valuable research venue and platform where millions of users interact and collaborate ... on a daily basis (Yee 2006:309).

The virtual worlds in MMOG and MMORPG, representing the persistent social and material world, provide a synthetic environment in which people communicate with each other using a virtual persona – avatar – and allow strangers who do not necessarily speak the same language to establish relationships (in the virtual worlds). Players are also able to receive education, to purchase virtual properties, acquire virtual accommodation and trade in virtual merchandise, and to inflate their virtual status using physical cash in the virtual worlds. A study by Chen et al. (2004) suggested that, as at March 2003, an exchange rate was estimated to be 10,000 in virtual cash unit to US$1. It was also reported on LindeX, the official Second Life currency exchange (http://secondlife.com/whatis/currency.php), that an exchange rate was estimated to be L$250 (Linden Dollars in Second Life) to US$1 as at January 2007.

The availability of a market for virtual currency exchange has attracted the interest of individuals and multi-national corporations. In November 2006, the first self-proclaimed virtual world millionaire, Anshe Chung, announced that she had accumulated virtual assets worth more than US$1 million in physical currency (Hutcheon 2006). Multi-national corporations such as IBM, Toyota, Adidas, Telstra, the Australian Broadcasting Corporation and MTV have established or intending to establish a presence in these virtual worlds. In 2007 Sweden announced establishment of a diplomatic presence in Second Life (AAP 2007b) and in 2006 popular music band Duran Duran announced purchase of a luxury island (Wallace 2006a). On the island, live concerts and media appearances will take place alongside the band’s media, public and live engagements in the physical world.

The availability of a market for virtual goods trading (e.g. http://www.itembay.com.tw/) provides criminals with financial incentives to offend. Organised criminal groups and hackers are targeting MMOG and MMORPG sites to steal gamers' usernames, passwords, credit-card numbers, and virtual game pieces and accessories. Stolen virtual characters are then 'sold' to the original owners or to other players (Ortega 2006). Examples include:

- In June 2002, it was reported that virtual currency with an estimated value of S$15,000 was stolen from four compromised players' accounts in Singapore (IMCYC 2005).
- In 2003, JB Weasel was arrested and charged in the United States District court under the federal Computer Fraud and Abuse Act for allegedly hacking into another player's GettaLife game account and stealing the player's virtual assets (BlackHat 2003).
- In September 2006, the database of Second Life was reportedly hacked into and information about 650,000 game users, including addresses, passwords and encrypted credit card details, stolen (Sophos 2006a).
- In November 2006, the United States FBI closed the website www.l2extreme.com that hosted the 'Lineage' online game using pirated source code. A California man was arrested for criminal copyright infringement and faces up to five years in prison and a US$250,000 fine (FBI 2007a).
- In December 2006, 44 suspects were arrested in China for stealing more than 700,000 Yuan (approximately A$112,000) worth of virtual items by selling properties belonging to compromised Tencent QQ users' accounts (Zhu 2006).

The future will see the continued development of malicious code targeting the online gaming community such as:

- 'CopyBot'-type code that allows gamers to replicate virtual goods without paying the original designers
- 'Grey goo'-type code designed to self-replicate objects within the virtual world that might eventually cause a denial-of-service-type attack
- 'Waigua'-type code (popular in Chinese online games) designed to automatically carry out activities on behalf of the players with the aim to increase the levels of their characters.

Risks of money laundering will also increase as MMOG and MMORPG sites emerge as a vehicle transferring value online. For example, money launderers can purchase virtual currency using illicit cash and exchange the virtual currency back to physical cash. Alternatively, colluding avatars (controlled by criminals) can also launder illicit proceeds in the form of gifts or mutually beneficial economic exchanges in the virtual worlds. A 2007 report pointed out that a criminal could purchase virtual properties in the virtual world worth 1000 Linden dollars, but actually pay A$2 million in cash (Palmers 2007). Although online gaming site operators are required to monitor and report any suspicious transactions under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) since they provide the facility to exchange real cash for virtual currency, such privately-conducted transactions are unlikely to be captured by the operators (and authorities).

Existing avenues of money laundering, such as online gambling, a multi-billion dollar industry, will continue to be used. Criminals will be able to establish online accounts with offshore casinos using stolen identities and transfer funds anonymously. To avoid detection, small numbers of transactions will be carried out and then requests made for repayment from offshore casinos. Although offshore casinos may not be required to maintain transaction records, payments can be deposited into bank accounts belonging to money mules to obscure the money trail.

COUNTERMEASURES

Criminal threats in an environment in which Internet International Funds Transfer Instructions (IIFTIs) and e-currencies exist are likely to increase, as regulators fail to capture many transactions. IIFTIs may also aid money-laundering activities. Possible countermeasures include:

- Regulating online payment systems and internet payment intermediaries (including offshore banking services and financial entities) through international collaboration and legislative efforts; for example, the recommendations in the Financial Action Task Force report (FATF 2006) and enacting of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- Regulating virtual currency in online gaming through legislative efforts. For example, South Korea was reportedly considering introducing legislation to ban commercial trading in virtual currencies (Burns 2006). It was also recently reported that the People's Republic of China is considering regulating the use of virtual money, QQ's coin, to combat money-laundering activities in China (AP 2007).
- Technical assistance and open exchange of control solutions among banking services and financial entities and governments to less capable or advanced jurisdictions on detection techniques against money laundering and other crimes.
- Unified approach to security standards; for example, the Payment Card Industry Data Security Standard (PCI DSS) developed jointly by Visa and MasterCard.

Government access cards and biometric passports

Low-cost cryptographic devices include hardware (circuitry)-only devices such as radio frequency identification (RFID) devices and hardware devices with built-in software components such as microcontroller based smartcards. Smartcards and RFID devices are emerging as important technologies in a variety of online, offline and hybrid applications in the public and private sectors. Government initiatives in Australia include the National Health and Social Services access card, Centrelink Staff Identification Cards, Queensland's smartcard licence and RFID-enabled biometric passports (or e-passports).

Access cards

The Australian Government has resolved to implement a National Health and Social Services access card, which includes a microchip with detailed personal information. The access card would be issued to more than 16.7 million people by 2010 (Hart 2007). Similar initiatives have been implemented in the United States such as the government ID card based on the Federal Information Processing Standards issued by the National Institute of Standards and Technology. Although not designed as a generalised government identity card (AAP 2007a), Australia's biometrically enabled card will have widespread uses and applications, making it a likely target for criminals. Privacy and accountability concerns have been cited with the access cards (ALRC 2006, Greenleaf 2007) as such cards may facilitate the surreptitious collection of personal data. For example, the unique multi-purpose identifiers ease the monitoring of individuals' activities across different organisations and could be exploited by rogue employees.

Other areas of risk include those associated with dishonest initial enrolment of users as well as data security, both with respect to the card's computer chip as well as supporting databases. As applications of government issued smart technologies increase, risks will increase, extending to systems used to facilitate new online services such as electronic voting in elections, electronic tendering and electronic democracy. Such applications would be attractive targets for groups wishing to disrupt or affect levels of confidence in government and business generally.

Despite the security architecture – supported by rigorous access controls, logging and auditing – that will be deployed, organised criminal groups will seek ways of compromising the system's computer infrastructure or obtaining personal and confidential information. The obtained information could be subsequently used in identity-related crimes (e.g. more sophisticated malware and social engineering) and other technology-enabled crime.

Biometric passports

Traditional paper-based passports are also being replaced with RFID-enabled biometric passports (e-passports); a contactless smartcard with a secure microprocessor that employs a passive radio frequency to transmit data over an encrypted wireless link to a reader. E-passports are designed to conform to International Civil Aviation Organization standards. Although biometric passports contain similar information as is found on the data page at the front of traditional paper-based passport, e-passports are designed to provide strong authentication that unequivocally identifies their bearers.

Academic researchers such as Smith (2006) have raised issues relating to privacy, security and effectiveness of biometry. Researchers from Vrije Universiteit Amsterdam and SRI International have suggested that RFID chips could be used to compromise computer systems by sending malicious data to vulnerable systems (Ortiz Jr 2006). The likelihood of this happening in the real world, however, is rather low at this time. Researchers from Germany also demonstrated that e-passport RFID chips could be skimmed and cloned easily with inexpensive and easily obtainable equipment. They then speculated that the RFID tags embedded in United States e-passports could potentially be used to identify them from a distance (Evers & McCullagh 2006); a form of short-range clandestine tracking and scanning. To prevent long-range scanning of closed passports, metallic material is included in e-passport covers to limit RF penetration; and Basic Access Control can be deployed to encrypt the contents of e-passports such that optical scanning is required to obtain the decryption key from e-passports.

Despite the preventive mechanisms deployed, the future will see new hardware devices and software programs seeking to compromise the quality of data-protection mechanisms and supporting architecture. Such devices and programs aim to clone e-passports, facilitate brute-force attacks on keys used for access control, and devise new ways of tracking and scanning covertly (to circumvent the use of Faraday cages). In 2006, Rieback and colleagues presented design principles for RFID malware together with supporting proof-of-concept examples to underscore the feasibility of RFID devices being abused and exploited in attacks against e-passports (Rieback et al. 2006).

Summary

In many ways anticipating the future technological environment in which technology-enabled crimes will be perpetrated is a relatively simple task. Technology will continue to advance rapidly and while those advances may permit faster access to, greater storage capacity within, and greater speed and ease of information dissemination from, computer systems, the potential for witting or unwitting negative impacts upon that information will occur. Poorly designed, executed and maintained security protocols, processes and devices leave computer networks open to attack both by critical infrastructure incidents and deliberate criminal malfeasance. The typology of recent and anticipated security breaches has been typified by the quest for and abstraction of information needed by criminals for committing large-scale and profitable financial crimes. The ability for law enforcement to maintain a watching brief on the potential impact of new technologies and to convey that knowledge to organisations through their own endeavours and/or through legislation and regulation remain ingredients to the effective understanding and mitigation of the future technology-enabled crime environment.

Risk areas and opportunities

Although proliferation of ICT and connectivity of the internet opens the door to increased productivity, faster communication and enhanced convenience, it also offers more opportunities for criminals to commit economic crimes with larger payoffs and fewer risks. In fact, Davis and Pease (2000) have suggested that ICT will play a prominent role in defining what is likely to become of greater value to a criminal in the future and might dictate that electronic property, such as video-on-demand; knowledge and information, such as copyrights or trademarks; or identity devices, such as biometric smartcards, will be the assets of interest in the future (Davis & Pease 2000).

Technology-enabled crimes will continue to be driven by illicit financial gain, particularly as the internet is increasingly used for the conduct and development of e-commerce. In the same way that legitimate businesses will look at market forces and new opportunities, criminals will also explore new areas that can be exploited to maximise their profits and to evade the scrutiny of law enforcement agencies.

Computer-facilitated frauds

Globalisation and the new economy, enabled by the latest internet-based technologies and e-commerce, have created new and greater opportunities for criminals to commit fraud against both businesses and consumers (Smith 2007). Computer-facilitated frauds include advanced fee scams (also known as the ‘419 fraud’), online auction frauds, fraudulent lottery schemes, modem and web page hijacking and identity theft (including phishing) (Smith 2007, OECD 2006).

The latest Australian computer crime and security survey (AusCERT 2006) indicated that computer-facilitated fraud, that cost Australian businesses nearly $1 million in 2005-06, was consistently viewed by Australian businesses as one of the major sources of financial loss throughout the four-year period surveyed (that is, from 2003 to 2006). The estimated total financial loss to business throughout those four years was $7.5 million. Other independent surveys have also found increasing economic losses through computer-facilitated fraud against both businesses and consumers.

Click frauds

Several search engines and online sites are supported either in part or in full by pay-per-click advertising revenue models. In such revenue models, advertisers are charged based on the click-through rate of an advertisement. However, hosting sites could abuse such a revenue mechanism in an action known as a ‘click fraud’. Click frauds have been identified as an emerging threat to e-commerce.

One of the existing countermeasures taken to detect click frauds is to monitor click-through patterns based on the geographical locations of IP addresses. However, botnets usually control a large number of geographically dispersed IP addresses. Zombies located at different parts of the world infected with bot malware (e.g. Clickbot.A. coded to obtain financial profit from fraudulent clicks on online advertisements) can be abused to circumvent such measures (Choo 2007). This poses a threat to both the advertisers and the content providers. For example, if each of a 20,000 member-strong botnet clicks on 20 different advertising sites per day, the advertisers will suffer a substantial financial loss. Content providers could also face a ban or possibly litigation for charging advertisers over fraudulent click referrals. In July 2006, Google™ agreed to pay up to US$90 million to settle a lawsuit alleging it had overcharged thousands of advertisers for bogus sales referrals (Montalbano 2006, OUT-LAW 2006). Several content providers, including Google™, have chosen not to charge clicks that are deemed fraudulent to the advertising customer to prevent lawsuits. In fact, Knight (2006) has suggested that companies should view click fraud as another business tax. Another example involving the use of bots to facilitate click fraud is the exploitation of 34,000 zombie computers infected with Clickbot.A. and controlled remotely through several web servers to defraud pay-per-click advertising systems (McKewan 2006).

Despite efforts to improve click fraud identification techniques and raise the entry barrier for fraudsters, financially motivated criminals and malware authors will continue to design malware that seeks to circumvent existing measures (e.g. viruses such as KMeth worm that will direct infected users to fraudulently increase traffic to specific online advertisements).

Online auction frauds

Online auction sites provide buyers and sellers with a global virtual market in which to buy and sell a wide range of merchandise through competitive bidding. They constitute one of the most successful internet-based business models. One of the largest consumer-oriented auction sites, eBay, reported a total net transaction revenue of US$4.4 billion from approximately 72 million active users (people who bid on, bought, or listed an item during the reporting period) as of 31 December 2005 (eBay 2006).

Crimes associated with online auctions (see Table 5), particularly online auction frauds, are on the rise and increasingly becoming more sophisticated. Statistics released by the National White Collar Crime Centre and the FBI indicated that between 1 January 2006 and 31 December 2006, 207,492 technology-enabled crime complaints were reported to the Internet Crime Complaint Center. Online auction fraud, the most prevalent offence type, accounted for 45 percent of the 86,279 referred cases to United States law enforcement agencies and 33 percent of the total reported dollar loss (NW3C/FBI 2007).

Table 5: Examples of online auction crimes

Seller crimes	Bidder crimes
Shilling: Auctioneers, in order to drive up the selling price, spuriously place bids on their own auction. **Bid siphoning:** Auctioneers avoid paying commissions to auction sites by contacting and transacting with interested bidders directly. **Second chance offers:** Losing bidders of a closed auction are offered a second chance to purchase the same item off-site. **Shell auction:** With no intention of selling, auctions are established for the purpose of obtaining names and credit cards, which can then be used to facilitate crimes such as identity theft. On 6 October 2006, two Romanian nationals were indicted on charges of wire fraud and identity fraud related to a US$150,000 internet scheme. With no intention of selling, the defendants masqueraded as Hurricane Katrina relief organisations and held bogus auctions on eBay, Yahoo!® Auctions and Autotrader.com. They then collected money from the successful bidders (FBI 2006c). **Misrepresentation:** Specifications for the merchandise for sale are intentionally described incorrectly or auctioneers intentionally overstate the actual quality of the merchandise for sale. **Failure to ship:** Auctioneers fail to send the merchandise upon receiving the money. On 17 February 2005 a man was convicted in Queensland of this offence (see *Ferrus v Queensland Police Service* [2006] QCA 57). **Counterfeits/pirated software:** Counterfeits, usually luxury items, and pirated software are offered for sale on online auction sites. On 26 April 2007 four men pleaded guilty in Milwaukee to selling counterfeit Rockwell Automation computer software on eBay, in violation of criminal copyright infringement laws (US DoJ 2007e). **Sale of non-existent merchandise:** In February 2007, four suspects in Atlanta, United States were indicted for posting non-existent items for sale on eBay. Funds amounting to half a million dollars were then collected from the successful bidders (US DoJ 2007f). **Fee stacking:** Hidden costs are added to the transaction after the auction has ended. **Triangulation/fencing:** Stolen goods are offered for sale.	**Bid shielding:** A dishonest bidder places a low bid while another colluding bidder places an inflated bid. The colluding bidder will withdraw immediately upon winning the auction, hence, resulting in a lower bid being accepted. **Failure to pay:** Bidders fail to pay for the received merchandise. **Buy and switch:** Buyers switch received merchandise with other inferior merchandise and then request a refund. **False-name bid:** Bids are made under fictitious names and winning bids are made using stolen credit cards.

Source: AIC 2007a

Authenticating the identity of online auction site bidders and sellers is the primary fraud minimisation strategy. A common authentication mechanism is to identify users by their email address and a corresponding password. This can, however, be used by fraudsters to facilitate fraudulent transactions since the email address is a perfect pseudonym that does not reveal any links to the original user. Moreover, password-based authentication has its disadvantages despite being cheap to deploy, easily revocable, and with wide user acceptance (Zhang & Wang 2003). In terms of user accountability, it might be hard to hold a user legally accountable for any actions attributed to that user in a password-only authentication system (Choo 2006). Moreover, most online auction sites only authenticate that the user has a valid email address, and clearly this is a weak form of authentication.

An additional security feature deployed by most online auctions is secure channel sign-in where the browser and the auction sites employ an Secure Sockets Layer/Transport Layer Security (SSL/TLS) connection. This encrypts the user's password when transmitting to ensure secure communication between the browser and the site, which helps to prevent password leakage via eavesdropping and illicit capture. However, a keylogger would still pick this up if such a program were installed on the user's computer.

Criminals and malware authors will continue to design malware that seeks to circumvent existing measures for illicit financial gain (e.g. viruses such as Trojan-Spy.Win32.Bancos that will intercept and modify information transmitted during the 'secure' communication between two parties).

Major drivers having an impact on consumer fraud include the rapid expansion of new and emerging technologies (see previous chapter) and the apparent ease of committing consumer fraud (Smith 2007).

ICT enhances economic opportunities, expands markets, minimises the effects of distance and time when conducting transactions, and increases fluidity and the interdependence of users. Rapidly changing IT and telecommunications sector is one of the key drivers of long-term economic growth. Important developments in the last 10 years – mobile phones, personal computers, email and the internet – have markedly changed the way consumers live and work and how they relate to business and government. For example, the mobile phone is being transformed into an electronic wallet, allowing consumers to shop, bank and pay bills. Removable media devices – MP3 players, USB data keys, digital cameras and portable hard disks – are becoming smaller, more powerful and more common.

These enhanced powers of communication and transaction have brought with them enhanced opportunity for criminal activity. Smith and colleagues have reported that some scams (e.g. phishing) that use the internet and new forms of technology are easy to learn, entail minimal cost to offenders and yield high profits. They require few resources relative to the potential damage that can be caused; they can be committed anonymously, perhaps in another jurisdiction or country without the perpetrator being physically present, and often may not be clearly illegal (Smith, Grabosky & Urbas 2004). These types of consumer fraud dramatically increase both the technical and legal complexities for detecting, investigating and prosecuting, but also leave consumers particularly exposed and vulnerable. While the business sector generally has its own anti-fraud arrangements in place, individual consumers may be more exposed as 'soft targets' for criminals. If business practices could be made safer and more secure for consumers with strengthened privacy and security-related measures in place, confidence would be enhanced and the perceived risk of consumer fraud minimised. Ultimately, failure to effectively safeguard consumers against fraud and to apprehend perpetrators can erode public trust and respect for law generally.

Due to the obstacles associated with reporting consumer fraud and its ever-changing nature, the full extent of the problem remains unknown and many perpetrators are able to escape punishment. As a consequence, the level of risk to which consumers are exposed by the different techniques perpetrators use is equally difficult to determine. Incidents involving the use of technology to deceive consumers into parting with information or funds are unlikely to decrease over the next two years.

Phishing and spam

Phishing attacks will become more sophisticated and the number of such attacks is likely to increase. A 2005 report indicated that an estimated 75 to 150 million phishing emails are circulated each day over the internet (McAfee 2005). A year later, the number of phishing emails has increased by 25 percent (McAfee 2006). In August 2006 a single botnet that controls more than 20,000 distinct IP addresses was reportedly used to send United Kingdom firms millions of phishing emails with subject lines referring to either NatWest or Bank of Scotland (Jaques 2006). The email contained an inline image. Once the email recipients clicked on the image, they were directed to a website where they were instructed to input their personal information. The attackers could then use the obtained information to siphon cash from the victims' bank accounts. In another non-related incident, three botnets were reportedly behind the January 2007 distributed denial-of-service attacks against several sites including the stock-fraud investigation website http://www.stockpatrol.com/ (Lemos 2007b).

Dissemination of spam will be facilitated not only through the use of botnets, but also voice over internet protocols (VoIP) – known as Vishing – and mobile phones (via SMS) – known as SMiShing – which will be used to overcome spam-prevention and detection filtering software. The future will see an increase in persistent attacks using redirection or malware techniques that will trap astute internet users. For example, the inclusion of random data in spam messages can be used to bypass first-generation anti-spam technologies and the evolution of image-based spam over the years. The development of technical attacks (e.g. animated GIF images) poses a growing challenge as these are often more persistent and difficult to detect. Once detected, they require the development of a patch that needs to be implemented by the computer user.

Another important threat to emerge will be the use of spoofed embedded links that look like links to the institution being impersonated but which lead to malicious sites (i.e. drive-by download). In the *Security Threat Report 2007* an average of 5000 new websites hosting malicious code were reportedly discovered daily (Sophos 2007c). Some malicious sites may contain code that allows the phishers to retrieve contextual information such as sites visited from the browsers' cache and history. Such information can then be used to facilitate 'context aware phishing' (Jagatic et al. 2007) whereby phishers

> target the users in question with phishing emails that – by means of context – appear plausible to their respective recipients. For example, phishers can infer online banking relationships, and later send out emails appearing to come from the appropriate financial institutions. Similarly, phishers can detect possible online purchases and then send notifications stating that the payment did not go through, requesting that the recipient follow the included link to correct the credit card information and the billing address. The victims would be taken to a site looking just like the site they recently did perform a purchase at, and may have to start by entering their login information used with the real site (Jakobsson & Stamm 2006).

In January 2007, RSA Security's anti-fraud command center reportedly discovered a phishing toolkit – 'universal man-in-the-middle phishing kit' designed to post legitimate and actual content on a fraudulent URL in real time – is available for sale online (RSA Security 2007). It is likely that such tools will be further enhanced to include more sophisticated capabilities targeting two-factor authentication mechanism such as subverting token-based logons, acquiring and reusing one-time token data in real time.

Although phishing attacks can be either syntactic (exploiting technical vulnerabilities) or semantic (exploiting social vulnerabilities), the future will see a continuing movement from syntactic attacks to semantic attacks. For example, it is known that phishing attacks have been facilitated by publicly available personal information from social networks such as Myspace and Friendster. A phishing experiment conducted by researchers at Indiana University in April 2005 (Jagatic et al. 2007) suggested that phishers can easily exploit social network data found on the internet to increase the yield of a phishing attack as internet users may be over four times as likely to become victims if they are solicited by someone appearing to be a known acquaintance.

Faced with these considerable unknowns, developing well-designed and effective policies and strategies to combat consumer fraud becomes more problematic and, when coupled with the complexities of apprehending suspects, obtaining convictions and imposing sizable penalties, the deterrent effect of the law is limited. Reduced deterrence may also increase the likelihood that re-offending will occur.

Unauthorised access

As security measures organisations employ to prevent computer security breaches involving unauthorised access improve, criminals will seek to gain access to systems to disable security and alarm systems or design new malware programs to circumvent security mechanisms. Stolen computers, laptops and mobile phones also pose security challenges for individuals and organisations (including universities). Most laptops today have integrated wireless local area network capabilities that enable users to access organisational resources via third-party networks. Such stolen laptops may be used to facilitate unauthorised access into an organisation's internal network. An audit report by the United States Treasury Inspector General for Tax Administration found that

> The IRS annually processes more than 220 million tax returns containing personal financial information and personally identifiable information such as Social Security Numbers. We found hundreds of IRS laptop computers and other computer devices had been lost or stolen, employees were not properly encrypting data on the computer devices, and password controls over laptop computers were not adequate. As a result, it is likely that sensitive data for a significant number of taxpayers have been unnecessarily exposed to potential identity theft and/or other fraudulent schemes (US TIGTA 2007).

Displacement from high-tech to low-tech responses will also increase with opportunities for social engineering, corruption of IT personnel and other insiders being used, in addition to the use of violence and duress to compel users to disclose access codes or to facilitate the use of biometric user authentication systems. Either insiders, who enjoy privileged access, or outsiders can carry out attacks. For example, Berkman & Ostrovsky (2006) highlighted the possibility of bank employees stealing customers' PINs by exploiting weaknesses in verification facilities and network switches used at the banks. The 'motivation to damage an organisation through breaching its information security is greatest from external sources whilst the ability to cause such damage is greatest for insiders' (Walton 2006).

Threats from outsiders

Examples of security incidents involving unauthorised access by outsiders include the following:

- in December 2006, at the University of California Los Angeles, it was reported that personal details of 800,000 current and former university students might have been exposed to a hacker who broke into the university's computer systems (UCLA 2006)
- in September 2006, Eric McCarty of San Diego was arrested and charged for hacking into a computer system at the University of Southern California and accessing confidential information submitted by students applying to the university (FBI 2006d)
- in April 2007, a teenager was charged for hacking into America Online (AOL)'s networks and databases containing customer information and infected servers with a malicious program to transfer confidential data to his computer (Perez 2007; Schram, Bulliet & Gittens 2007)
- in May 2007, the computer system at the University of Missouri was allegedly compromised and the names and Social Security Numbers belonging to 22,396 individuals stolen (Gaudin 2007, University of Missouri-Columbia 2007).

Stolen information could be used to facilitate identity theft. In June 2006, the FBI arrested a man associated with a credit card fraud ring for defrauding credit card companies of more than US$1.7 million through the use of stolen social security numbers and fictitious names. He was sentenced to four years in federal prison (FBI 2006b). In another more recent example, Gregory A. White of Strongsville, Ohio allegedly 'opened at least 35 brokerage accounts via the [i]nternet at Ameritrade and E*Trade, using the names, Social Security account numbers, dates of birth and other personal identifying information of other individuals without their knowledge, using fraudulent Electronic Funds Transfers (EFT) from various banks in the Cleveland area, and elsewhere' (US DoJ 2007c). The indictment alleged that 50 interstate Electronic Funds Transfers from various banks to Ameritrade and E*Trade totalling approximately US$3,348,000.00 had been made.

Semantic attacks committed through social engineering will continue to be employed by criminals to gain access to computers and networks. Social engineering involves the use of tricks to manipulate human behaviour often through the deception of unsuspecting users to gain access information (e.g. usernames and passwords, personal identification numbers, tokens and credit card information). Once they have gained access to the system offenders are able to erase, modify or copy information to suit the needs of their attack. For example, information gained from unauthorised intrusions into computer systems that process and store information on customer transactions can facilitate other crimes.

> Banks and retailers in the United States and Canada have begun to report an increasing amount of illicit transactions thought to be linked to the server breach announced last week by the TJX Companies, the commercial giant that owns retail chains in the United States, Canada, and Europe (Lemos 2007a).
>
> Six individuals have been detained in Florida on suspicion of fraud through using credit card information stolen from TJX. These are the first arrests connected with the theft of customer details from the company, which owns retail outlets including TJ Maxx, Marshalls, HomeGoods and AJ Wright (Goodin 2007c).

Threats from insiders

Academic researchers have studied the threat of malicious exploitation by insiders (e.g. employee-related crime) since the 1980s (Harrington 1996, Kesar & Rogerson 1998, Straub 1986), and it is still widely recognised as an issue of utmost importance for information security management today (Power & Forte 2006, Theoharidou et al. 2006). The latest AusCERT (2006) survey indicated that malicious exploitation by insiders ranked second among the various concerns voiced by the survey respondents from the public and private sector organisations surveyed. Another independent 'Insider Threat Study' by the United States Computer Emergency Readiness Team (CERT) and the United States Secret Service (Cappelli et al. 2006) indicated that the resulting financial costs of insider attacks ranges from a few hundred to tens of millions of dollars.

The global business security index (IBM 2006b) suggested that future trends are likely to include insider attacks in which end users will be persuaded to execute attacks on organisations rather than malfeasants attempting to circumvent increasingly secure software.

Insider threats can be further divided into two categories:

- Threats of insider attack on behalf of or controlled by an outsider (e.g. zombie computers controlled by bot malware).
- Self-motivated insider attacks.

As critical systems become increasingly dependent on software and are connected to the internet, insider threats belonging to the first category will be of ongoing concern. For example, corrupt insiders could deliberately introduce vulnerabilities during the coding of in-house software that is used to manage sensitive military or intelligence networks. This could allow terrorists or foreign intelligence agents to exploit the vulnerabilities and surreptitiously enter systems, gain control, and launch online attacks via and against compromised systems.

Two widely-reported security breaches belonging to the second category are as follows:

- In Maroochydore in Queensland in March–April 2000, a disgruntled employee of a Maroochydore company, used the internet, a wireless radio, and stolen control software to access a sewage management system by exploiting vulnerabilities in the supervisory control and data acquisition system. He released up to 1 million litres of sewage into public areas of Maroochydore causing significant environmental damage (*R v Boden* [2002] QCA 164 10 May 2002).
- In another incident, reported in mid 2006, nearly 800 instances of inappropriate access by Centrelink staff to customer records were discovered (ABC 2006).

The ABC reported a further incident in 2007 that involved a former police sergeant in Perth, William Andrew Harrison, allegedly leaking confidential information on a police computer. Harrison received a suspended term of imprisonment (ABC 2007b).

With advances in communications technologies, there will be more avenues for insiders to leak sensitive information. An example is the Wikileaks.org website (http://www.wikileaks.org/index.html) that is designed for whistleblowers in authoritarian countries to post sensitive documents on the internet without being traced. Marks (2007) reported that the anonymity feature is provided with the use of The Onion Router, an 'anonymising protocol', which allows data to be routed through a network of servers. The latter uses cryptography to further obscure the data path and hence, make it untraceable.

Countermeasures

Security products such as antivirus software, firewalls, intrusion detection systems and virtual private network products will increasingly become a security challenge themselves. High tech criminals may seek to gain access to systems to disable security and alarm systems or design new malware programs to circumvent existing security mechanisms. Once those security systems are disabled, attacks become easier to perpetrate. Exploitation of vulnerabilities in security infrastructure leaves organisations significantly vulnerable to further attack. Increasingly cryptography, such as steganography, and encryption will be used to protect and transmit data. For example, in June 2006, the United States government mandated the use of full disk encryption on government-owned computers (US OMB 2006).

Although organisations will continue to build a culture of vigilance to maximise the chances of detection of insider threat, the latter will continue to constitute a separate category of threats against the integrity, privacy and availability of computer systems and networks in the next two years. Perimeter security and network security in isolation are insufficient to counter insider threats. Efforts should, arguably be taken to protect information and data in both storage and in transit.

Evolution of malware

Malicious software – malware – facilitates technology-enabled crimes by providing criminals with the means of installing malicious programs on computers and allowing them to cause damage without the computer users' consent and knowledge. Malware includes a variety of computer code such as worms, viruses, backdoors, keyloggers and Trojans. The principal method of disseminating malware is through disguised email. For example, the Dumaru worm disguises itself as a security patch from Microsoft, and installs an internet relay chat Trojan onto the infected machine once the victim executes the 'patch'. In disseminating malware, 'preying upon public interest by using breaking news events is a tried and trusted trick. It has proven to be a remarkably effective method of fooling recipients into lowering their guard' (Sophos 2007b).

This trend of exploiting social vulnerabilities to disseminate malware is likely to continue in the next two years and so too will the trend of designing malware for facilitating blended attacks such as spy-phishing.

> Spy-phishing is a complicated phishing attack that also involves the use of various malicious applications, typically Trojan horses and spyware, to perpetrate online information theft. The most common targets are banking credentials, but this could easily escalate into proprietary and corporate information, as well. The downloaded applications sit silently on the user's system until the targeted URL is visited wherein it activates, sending the information to the malicious third party (Aboud et al. 2006).

Victims of malware infection often use search engines to research the malware that infected their machines. Malware authors have deployed file-naming tactics, such as associating files generated by self-replicating malware with common extensions such as .exe and .dll, to delay the searching process. 'If a user searches for a suspect file name on Google™ or Yahoo!® and nothing is found, then the assumption is that the file is probably nothing to worry about' (Dunn 2007).

Malware authors will continue to explore ways in which to deny or delay victims accessing information about the source or nature of malware infection.

> IDefense Labs is offering more than US$50,000 to researchers who submit serious flaws in Windows Vista and Internet Explorer 7, as part of a challenge designed to beef up the company's security products .... Trend Micro last month discovered that Vista exploits were being offered for sale on underground sites for US$50,000 each (Broersma 2007a).

The availability of a market (AIC 2007b) in which to sell malware provides criminals with more financial incentives to offend. In January 2007, Li Jun from Central China's Hubei Province was arrested for reportedly authoring the password stealer W32/Fujacks (also known as the

‘Panda joss-stick’ worm) and selling W32/Fujacks to other internet hackers for more than 100,000 Yuan (Dao 2007).

The future will be likely to see the following malware trends take place:

- The continued development of viruses, worms and Trojans, that employ self-modifying (or self-mutating) code allowing malware to automatically inject random pieces of code, such as Trojan program code, prior to compilation and compression. This aims to create separate variants, and code-obfuscations in order to elude detection by antivirus and anti-malware products.
- The continued availability of a market for the sale of malware such as password stealers like W32/Fujacks and related Trojans and file infectors (including password-stealing websites using fake sign-in pages) and subscription-based services for malware updates. These are similar to the current subscription-based services offered by anti-virus software.
- The continued enhancement of other stealth techniques to hide files, processes or registry values belonging to the malware, such as installation of Application Program Interface that hooks into running processes or changes system Application Program Interfaces.

Examples of evolving malware include bot malware, kernel-mode malware, ransomware and malware that exploits internet browsers and web services.

Bot malware (and zombies)

Bot malware is just as dangerous as the other cyber threats with which many users are familiar, such as viruses, worms, Trojan horses and network intrusions (Schaffer 2006). A positioning paper released in August 2006 highlighted that an unpatched computer with neither antivirus protection nor firewalls installed would have a 50 percent chance of becoming a zombie within 30 minutes of being connected to the internet (Sophos 2006b). These commandeered zombies can then be abused to facilitate other technology-enabled crimes such as distributed denial-of-service attacks, facilitating phishing, hosting illegal data, disseminating other malware, facilitating click fraud and disseminating spam. On 6 February 2007, distributed denial-of-service attacks, reportedly carried out by botnets, targeted several root servers hosting the domain name service that translates domain names to numeric IP addresses, including one maintained by the United States Department of Defense (Goodin 2007a, McMillan 2007a, Sophos 2007a).

Botnets can speed up the spread of worms (Choo 2007). For example, the Symantec Security Response Team speculated that 2004’s Witty worm that infected and crashed tens of thousands of servers, was probably launched by a botnet with a membership size of 2400 (Lemos 2004). In fact, Mathieson (2006) estimated that 70 percent of stock-related spam is forwarded using botnets and the unavailability of a major botnet was attributed to a 30 percent drop in the number of spam emails detected in the first week of January 2007 (Broersma 2007b).

Examples involving botnets to disseminate spam include the January 2006 case of a 20-year-old Californian named Jeanson James Ancheta who pleaded guilty to computer fraud and spam offences connected to his dealings in botnets. Ancheta created new variants of the 'rxbot' robot family.11 and distributed these variants to establish several botnets. He then hired out the botnets to others for the purposes of sending spam and launching distributed denial-of-service attacks, thus allegedly earning Ancheta thousands of dollars. It was also alleged that Ancheta used the botnets to generate income from the surreptitious installation of adware on the zombies. In May 2006, Ancheta was sentenced to 57 months in a federal prison (US DoJ 2006a).

Membership of botnets ranges from hundreds to hundreds of thousands of zombies. Recently observed trends, however, suggest that botnet sizes have been decreasing, so as to evade detection since smaller botnets are often more difficult to detect (Cooke et al. 2005). The level of sophistication of bot malware has also increased considerably in recent times. In October 2006, the computer security community discovered a new 'spam-bot' malware, SpamThru, (Stewart 2006) which has the following sophisticated features:

- The installation of its own antivirus scanner to eliminate competing malware installed on compromised machines.
- The ability to download and leverage a template containing the spam to become its own spamming machine (instead of being a spam proxy).
- The use of an advanced encryption scheme, an encryption standard adopted by the United States government, to prevent unauthorised third parties downloading the spam templates.
- The ability to send randomised GIF-based spam messages to avoid anti-spam measures that reject messages based on a static message.

In 2006, the security community highlighted a new class of bot malware – Queen Bots – that 'packed' (and 'repacked') the executable files containing the malicious codes to further obfuscate the signatures of the malicious codes, that aim to elude detection by antivirus software. They also noted that Queen Bots comprise half of the known bot programs operating today (IEEE 2006). Although there are no known published statistics or reported incidents involving Queen Bots, it is likely that malware designed to exploit portable executable packing technologies – originally designed to reduce the size of an executable on disk through compression – will emerge. Several antivirus researchers including Schipka (2006) and Josse (2006) have highlighted similar concerns.

Kernel-mode malware

Kernel-mode malware executes as part of a computer's operating system and has full access to the computer's resources. It is, unfortunately, hard to detect (Crandall et al. 2006). 'To the end-user this means malware that can bypass software firewalls and can be almost impossible to detect or remove even if the best antivirus solutions are being used' (Kasslin 2006).

Although kernel-mode malware has yet to become popular, threats from kernel-mode malware are likely to increase. Joanna Rutkowska, a Singapore-based stealth malware researcher, has provided details of a working kernel-mode malware prototype – Blue Pill – that is purportedly undetectable even on Microsoft Vista x64 systems (Rutkowska 2006). Blue Pill uses a thin hypervisor, a software layer implemented between the operating system and the processor hardware, to take control of a computer's operating system. Independently, Zovi (2006) also presented a kernel-mode virtual machine rootkit targeting the Intel VT-x platform.

Ransomware

The application of cryptographic tools and techniques to enhance new malware attacks will also increase. One example is a ransomware program that cybercriminals often use to search for data on compromised systems and then to encrypt these data. The key or password to recover the encrypted data can only be 'purchased' from the perpetrators. In April 2006, cases of cybercriminals using ransomware programs, 'Arhiveus.a' aka 'MayAlert' and 'Cryzip', to encrypt data on compromised computers were reported (Keizer 2006). The owners of those data are coerced into making purchases from one of three online pharmacies in return for the password to unlock their data. This activity is also termed cryptovirology or denial-of-resources attacks. The ransomware, 'Win32.Gpcode.ag', that appeared in June 2006 reportedly uses a 660-bit RSA encryption key that, for most victims, renders brute-force cracking of the key computationally infeasible.

Although incidents involving ransomware have yet to become widespread, it is likely that ransomware attacks will become more targeted, such as against certain organisations and industries. They will also use more complex encryption functionality (e.g. the use of enhanced-strength encryption algorithms).

Internet browsers and web services

Internet browsers and web services are becoming more important in the development of enterprise e-business applications in today's electronic marketplaces (e-marketplaces). Other applications of web services include e-commerce (such as business-to-business communications), middleware, interfaces to legacy systems, Asynchronous JavaScript and extensible markup language (AJAX) (e.g. in Google Maps™ http://maps.google.com/) and application programming interface (APIs) for added functionality.

Due to their increasing popularity, internet browsers and web services will also be of interest to criminals and malware authors. For example, users' computers can be infected by malware, including ransomware, when users visit compromised websites (by exploiting vulnerabilities of web servers or operating systems) that host malware. In February 2007 investigators found that several United States-based websites (e.g. the SuperBowl 2006 webpage hosted by Dolphin Stadium and the main podcasts page on the website for the Center for Disease Control and Prevention) were infected with the Backdoor-DKT Trojan (Krebs 2007, McAfee 2007). Moreover, users visiting websites infected with self-mutating Trojan malware can be infected with a different version of the same program. Malware authors will also target vulnerabilities introduced by user generated web contents. IBM reported, in 2007, that approximately 50 percent of websites that host malicious content now use encryption of the payload to further obfuscate their attack (IBM 2007).

Existing security measures such as network-based firewalls may not be able to defend against threats of unauthorised access to a web service. For example in the December 2006 demonstration at the 23rd Chaos Communication Congress, Di Paola and Fedon (2006) showed how AJAX could be exploited to facilitate attacks against web services.

Future exploitation of internet browsers and web services to disseminate malware will include the design of malware to hide browser attack codes, circumvent existing anti-malware products and mix known exploit codes so they become unrecognisable to antivirus programs.

Intellectual property infringement

Intellectual property (IP) as defined by the World Intellectual Property Organization (WIPO 2006) comprises:

- **industrial property** that includes patents, trademarks, industrial designs, and geographic indications of source
- **copyright** that includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, holographs and sculptures, and architectural designs.

In today's knowledge-based economy, managing and protecting IP, the principal economic asset and sustainable corporate competitive advantage, has become the cornerstone of corporate strategy. Enhanced capacity of ICT systems will enable electronic products (e.g. songs and movies) to be copied and reverse engineered more quickly and easily than at present, thus giving rise to increased risk of counterfeiting and piracy. In May 2007, NSW

Police reportedly seized more than 5000 optical disks during a raid in Ballina. It was alleged that the two persons arrested produced counterfeit copies of Microsoft Windows and Office software, games and music, reselling them on the internet (Rossi 2007).

Electronic properties, including video-on-demand; knowledge and information, such as patents, copyrights and trademarks; and identity devices, such as biometric smartcards, will be the assets of interest for future criminals. Besides being another source of data leakage, blogs and online sharing websites (for example, YouTube), will be abused by criminals to facilitate dissemination of copyright materials, such as MP3 blogs and video clips featuring copyright protected tracks and movies, without the express consent of the copyright owner. For example, in the case of *Universal Music Australia Pty Ltd v Cooper* [2005] FCA 972 (14 July 2005), the Federal Court found that there had been an infringement of copyright by Stephen Cooper (MP3s4free.net), ISP E-Talk Communications (trading as ComCen Internet Services), Liam Francis Bal (director of E-Talk/Com-Cen), and Chris Takoushis (employee of E-Talk/Com-Cen) for creating hyperlinks to third-party websites that had infringing sound recordings. In this particular case, the respondents neither stored nor distributed any infringing sound recordings.

A secure legal environment is vital for protecting IP rights. It is, therefore, not surprising that transfer of technology to countries with different notions of property rights or weaker protection of IP rights as part of investment and outsourcing projects will increase the risk of counterfeiting, piracy, illegal transfer of technology and facilitation of industrial espionage. For example, companies outsourcing their vital business process operations to countries such as China could potentially face difficulties in protecting their IP rights and enforcing foreign court judgments. China, one of the market leaders in hosting outsourced operations, is infamous for its high IP piracy rate (Yang 2007) and Kennedy and Clark have noted that:

> China has enacted IP laws that provide, on paper, the full protection one would expect in a Western country. China has patent, trademark, and copyright laws, as well as laws making the misappropriation of trade secrets both a civil and criminal wrong. The key issue in China is the enforcement of laws. In particular, Chinese civil procedure law makes it very difficult to protect high technology patents and trade secrets (Kennedy & Clark 2006: 251).

In 2007 the International Intellectual Property Alliance reported that the estimated losses due to infringements of software and music copyright in 2006 were between US$30 and US$35 billion (IIPA 2007). In the same report, the International Intellectual Property Alliance rated China and Russia as the two countries that are of the greatest concern to the copyright industries, contributing to US$2.207 billion and US$2.18 billion losses in revenues respectively. A more recent IDC Global Software Piracy Study released in May 2007 reported that a 10 percent drop in China's piracy rate over three years since 2003 resulted in a savings of US$864 million in losses (Business Software Alliance 2007). A seven percent drop in Russia's piracy rate over the same period was also recorded.

Increased use of open source or public domain software, in which the source code upon which the software is based is freely available so that users may access, change and re-distribute it, may reduce the incidence of copyright infringement, as may the use of freeware and shareware. For the near future, however, infringement of IP rights will remain of interest to law enforcement.

Industrial espionage

As digitisation continues to infiltrate all aspects of corporate life, a growing number of opportunities will arise for the commission of industrial espionage (see, generally, Nasheri 2005). Such attacks may use electronic surveillance and data capture technologies to steal commercial-in-confidence information, or may be directed at electronic IP such as trademarks or patents held electronically. Enhanced reverse engineering techniques (stripping down and analysing competitors' products) will also facilitate unauthorised accessing and exploitation of IP.

Criminals, competitors and foreign intelligence agents can also exploit commercial joint ventures and offshore outsourcing relationships for industrial espionage. For example, in outsourcing IT operations offshore, employees of outsourced vendors are likely to be placed in close proximity to protected programs. Malicious insiders (e.g. employees of outsourced vendors) could exploit such a situation to facilitate illegal technology transfer. In 2006 the United States-based Defense Security Service Counterintelligence reported a related example (US DSS 2006: 21) that underscored the risks inherent in joint overseas ventures between foreign organisations and defence contractors, where the former have opportunities to exploit the relationship. Recent cases include the following:

- In October 2006, Chi Mak, a former engineer with Navy contractor Power Paragon, was charged with collecting technical information about the Navy's current and future warship technologies with the intent to supply this military technology information to the People's Republic of China (US DoJ 2006b).
- In December 2006, Xiaodong Sheldon Meng was charged with stealing military combat and commercial simulation software and other materials from his former employer Quantum3D, a company based in San Jose, California with the intent to sell them to foreign governments of China, Thailand, and Malaysia (US DoJ 2006c).

Risks of industrial espionage may also arise where confidential contractual negotiations are carried out using email and wireless communications that have not been encrypted or otherwise carried out over secure networks.

Child exploitation and offensive content

Affordable technology (e.g. websites, web cameras and powerful editing multimedia software) has greatly reduced the barrier to entry for the production and distribution of child pornography. TopTenREVIEWS™ has estimated that child pornography generates approximately US$3 billion annually worldwide (Ropelato 2007). Although the level of knowledge of and measures to combat dissemination of child pornography and involvement of children in sexual offending has increased, individual and groups of criminals will continue to use ICT to carry out such crimes. In January 2007 the FBI arrested several individuals on charges involving possession and distribution of child pornography in connection with the North American Man Girl Love Association (www.namgla.net) website investigation (FBI 2007b). The use of ICT to carry out other related sexual abuses involving child victims (e.g. promoting child sexual tourism and trafficking children) are also likely to continue in the near future.

Offenders will continue to use cryptographic technologies to prevent detection and to enable images to be shared securely. Such cryptographic technologies include steganography, encrypted peer-to-peer networking and encrypted storage media (e.g. PGP Corporation Whole Disk Encryption 9.5 that uses the enhanced-strength advanced encryption scheme 256 encryption algorithm). Instant messaging programs and social networking sites will also continue to be used for child grooming and procuring children for sexual gratification. The enhanced capacity of systems and data transmission capabilities will result in a move from pornographic still images to motion pictures involving children. This will increase the need for law enforcement to enhance its cryptanalysis, steganalysis, and data analysis and storage capabilities.

It can also be expected that child exploitation will continue to involve the highly disturbing practice of live child sexual abuse videos being streamed to internet chat rooms, with the actual perpetrator responding in real time to commands from other participants who can see the images. Using the doctrine of constructive presence, it may be possible for such co-offenders to be prosecuted not only in relation to child pornography distribution, but also as accomplices in sexual assault.

With the enactment of new federal offences dealing with child pornography and grooming, it is to be expected that a proportion of future prosecutions will rely on these offences rather than state and territory laws. For example, Richard Gerard Meehan was charged with one count of using a carriage service to transmit communications to a person under 16 years of age with the intention of procuring that person to engage in sexual activity, contrary to ss474.26(1) of the *Criminal Code Act 1995* (Cth). On 21 July 2006, Meehan was sentenced in the Victorian County Court to 24 months' imprisonment, to be released after serving three months of that term (AAP 2006, Australia Commonwealth Director of Public Prosecutions 2006).

Law enforcement authorities have, to date, been particularly focused on websites and ISPs based in Australia that carry child pornography and child abuse material, although arrests for public order offences have also targeted the use of mobile phones and SMS to incite confrontations in public places. This type of act can fall within the broad offence of using a carriage service to menace, harass or cause offence, where offensiveness of material is to be assessed by ‘the standards of morality, decency and propriety generally accepted by reasonable adults’ (s474.17 of the *Criminal Code Act 1995* (Cth)). This provision may extend to offensive website content such as racial vilification material. It is to be expected that the future will see an increased number of prosecutions for these various forms of content-related offences.

Exploitation of younger people

As increasingly younger people (the ‘digital generation’) make use of personal computers and mobile devices, risks may arise where inadequate security measures are in place. Theft of laptops, USB drives, MP3 players and mobile phones from schools and entertainment venues will continue to create problems, not only in terms of replacement costs but also in relation to stolen personal information. Stolen personal and sensitive information will be used to facilitate other crimes, such as identity theft and extortion. Online scams are likely to target young users who may be less vigilant in detecting fraud than are adult users.

In recent years, a new form of bullying, including harassment targeting young users, has emerged which makes use of communication technologies such as email, text messaging, chat rooms, mobile phones, mobile phone cameras and social networking sites. Cyberbullying can also include online fights, denigration, impersonation, trickery, and cyberstalking.

> The anonymity provided by the internet introduces a new element: The victim may have no way to identify the bully. Neither parents nor school officials may know how to intervene to stop the harassment. Children may be reluctant to report incidents, for fear their computer privileges will be curtailed (Thomas 2006: 1015).

Findings from the second youth internet safety survey (a national telephone survey of a random sample of 1500 internet users between the ages of 10 and 17 years conducted between March and June 2005) indicated that there had been a significant increase in the prevalence of internet harassment since 2000 (Ybarra et al. 2006). Another study commissioned by the National Crime Prevention Council (2007) reported similar concerns. In the study conducted between 2 to 15 February 2006, approximately 46 percent of a nationally representative sample of 824 middle and high school students aged 13 through 17 in the United States reported that they had experienced some form of cyberbullying in the last year.

Cyberbullying will continue to be a problem. Victims may feel socially ineffective and consequently, experience greater interpersonal difficulties and exhibit lower academic performance. The consequences of cyberbullying can also shift from cyberspace to a physical location. For example, in June 2004, an 11-year-old girl fatally stabbed a classmate at an elementary school in Sasebo, Japan after an intense online argument (Nakamura 2004).

Transnational organised crime and terrorism

There are many examples of criminal elements (known colloquially as ‘super-empowered criminals’) operating in the online environment as obtainers and disseminators of identity and identity-related information. Operation Firewall, for example, in 2004 in the United States and Canada culminated in the arrest of 28 people from six countries for, inter alia, the buying and selling of 1.7 million credit card numbers. It is not clear, at this stage, whether there are ‘traditional’ organised crime groups operating within the technology-enabled crime environment, or whether there are simply criminal groups who happen to be organised. It seems likely, however, that traditional transnational organised crime groups will not shy away from using the technology-enabled crime environment to facilitate the operation, or to disguise the illicit proceeds, of real world based crimes. The use, for example, of denial-of-service attacks to pursue extortion or of online banking to transfer laundered funds is likely to continue to develop. The movement by traditional transnational organised crime groups into fully-fledged technology-enabled crime involvement will be determined as much by the diminished profitability, or increased risk, of real world criminal activities as it will by the innate attractiveness and relatively low risk of technology-enabled crimes. Certainly, therefore, each of the future risk areas may provide attractive targets not only for established organised crime groups based in Europe and North America but also for new groups based in the Asia–Pacific region. Organised operations that make use of conventional technology-enabled crime methodologies, such as financial scams or piracy, will also increase as the use of networked computers for criminal purposes develops.

Computers and computer networks will continue to be both the objects of terrorist attacks and the conduit through which terrorists and other criminals communicate in order to plan and carry out their destructive activities. Threats from (cyber) terrorism will carry serious economic and societal implications. Because many computer networks transcend international borders, it will increasingly become necessary for all countries to have adequate substantive and procedural laws, and to cooperate successfully to investigate, prevent and to punish terrorist and other criminal activities perpetuated with the aid of computers and computer networks.

Threats to national information infrastructure

Australia's national information infrastructure comprises computerised control systems that support critical infrastructure in both the public and private sectors. These are vital to our national security, economic development, and national public health and safety. They comprise:

> those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security (TISN 2006a).

Definitions of critical infrastructure differ between countries. In Australia, there are nine defined sectors; namely, banking and finance, emergency services, energy and utilities, food, health care, IT and communications, mass gatherings, transportation, and water (see Table 6).

Table 6: Summary of Australia's key critical infrastructure sectors

Key sectors	Examples of services within the sectors	Sector-specific government agencies
Banking and finance	Banking, securities and investment	Attorney-General's Department
Emergency services	Chemical, biological, radiological and nuclear safety, hazardous materials, search and rescue, and dams	Emergency Management Australia, a divison of the Attorney-General's Department
Energy and utilities	Electrical power, natural gas, oil production, transmission systems, and in future nuclear power production	Department of Industry, Tourism and Resources
Food	Safety, supply and distribution, agriculture and food industry	Department of Agriculture, Fisheries and Forestry
Health care	Hospitals, health care and blood supply facilities, laboratories and pharmaceuticals	Department of Health and Ageing
Information technology and communications	Telecommunications, broadcasting systems, international submarine cable and postal, software, hardware, and networks/the internet	Department of Communications, Information Technology and the Arts
Mass gatherings	Built environment, event spaces, and public spaces including key national sites and monuments	Attorney-General's Department
Transportation	Aviation, maritime and rail	Department of Transport and Regional Services
Water	Fresh drinking water and wastewater management	Attorney-General's Department

Source: Adapted from TISN (2006a)

Threats to critical infrastructure could arise from natural disasters (e.g. the earthquake in Taiwan on 26 December 2006 that disrupted telephone and internet services throughout Asia) and malicious attacks not directed at any particular critical infrastructure. In September 2001, computer networks at the Port of Houston in Texas were among an unknown number of intermediary servers affected by denial-of-service attacks against an unrelated third party (OUT-LAW 2005). Consequently, pilots navigating the Port of Houston were denied information on tide, water depth and weather.

National critical infrastructure faces a variety of threats from high tech criminals, including terrorists motivated by political or religious beliefs, aiming to disrupt one or more combinations of the following security notions:

- data confidentiality – designed to ensure that data are available only to authorised parties
- data integrity which ensures that data have not been tampered with or modified
- data availability which ensures that data continue to be available at the minimal operational level in situations ranging from normal to disastrous.

Examples of key cyberthreats to Australia's critical infrastructure, similar to key threats identified in other countries, notably the United States (US GAO 2004, US NSTC 2006), are outlined in Table 7.

Table 7: Sources of cybercrime threats to Australia's critical infrastructure

Identity fraudsters	Individual criminals and organised groups alike are offered more opportunities to commit economic crimes with fewer risks as advances in modern technologies allow them to easily hide their true identities or use spoofed identities. Deloitte Touche Tohmatsu's 2006 survey findings indicate that identity theft is fast replacing major viruses and worms as the principal threat to business. However, the PricewaterhouseCoopers survey (PwC 2006) indicated that United Kingdom businesses are ill placed to counter such threats.
Information thieves	Foreign intelligence services and industrial spies attempt to obtain information through clandestine entry into computer systems and networks as part of their information gathering, information warfare or espionage activities. They are usually interested in obtaining information relevant to vital national interests, with more sensitive information and data being exchanged electronically. In October 2006, Chinese hackers reportedly launched a concerted attack against the web systems of the United States Department of Commerce, attempting to gain clandestine access to sensitive and confidential data (Leyden 2006a).
Terrorists	Independent research has indicated that terrorists and terrorist groups have obtained information on and acquired chemical, biological, radiological materials via the internet or used global telecommunications technologies to mount attacks against key critical infrastructures. This is, perhaps, not surprising since authorities have known that members of terrorist groups include engineers and computer scientists (US NSTC 2006: 7) and the Al Qaeda terrorist group has been known to use the internet as a medium for propaganda.

Table 7: Sources of cybercrime threats to Australia's critical infrastructure (continued)

Malicious cybercriminals	Malicious hackers, code writers, and botnet operators often create malicious code to exploit the vulnerabilities in commercial off-the-shelf software or hardware products that are used in our critical infrastructure and control systems. Several surveys (AusCERT 2006, CSI 2006, Ernst and Young 2005) have shown 'threats from major viruses and worms' as ranking among the top three concerns of respondents from public sector and private sector organisations in different countries. The 2006 report by Arbor Networks indicated that distributed denial-of-service attacks are still the most significant security threat to ISPs in North America, Europe and Asia (Arbor Networks 2006). Distributed denial-of-service attacks on a key communication component could result in delay or interruption to communications between and within industries and sectors.
Hackivists	Hackivists have been known to carry out politically motivated hacking (hacktivism) and bringing down government agencies' websites. Such incidents include the 2006 defacing of Danish websites by Islamic hackers protesting controversial cartoons mocking the Prophet Muhammad (Ward 2006) and the denial-of-service attacks on Estonia websites (Kirk 2007).
Insiders (including disgruntled or corrupt employees)	In the AusCERT (2006) survey, malicious exploitation by insiders ranked second among the various concerns voiced by survey respondents from the public and private sector organisations surveyed. One of several infamous security breaches involving 'trusted' insiders is the Maroochydore incident in 2000, in which a disgruntled employee of a company used the internet, a wireless radio, and stolen control software to access a sewage management system to release up to 1 million litres of sewage into public areas of Maroochydore causing significant environmental damage *(R v Boden* [2002] QCA 164 10 May 2002).

Possible threats

Tight couplings between different areas of critical infrastructure may result in rapid escalation of seemingly modest disruptions within one sector to others. If unsecured sectors are compromised, these sectors can be used as launching pads to attack other critical infrastructure sectors. A successful attack on the information technologies and communications infrastructure that supports many of the other critical infrastructures could disrupt supply chain management systems, financial sector networks or power grids. Consequences of these attacks could continue to have a reverberating impact well after the immediate damage is done, such as adversely affecting tourism that accounts for 3.9 percent of Australia's gross domestic product (ABS 2006a). Cross-sector interdependencies are of primary importance in securing critical infrastructure. Specific examples of cyberterrorism activities are rare at present in Australia and internationally, although any instance of technology-enabled crime that exposes vulnerabilities in critical infrastructure security indicates the potential for a cyberterrorist attack.

A further area of risk concerns aspects of terrorist planning or preparation that involve use of ICT. In July 2006, Faheem Khalid Lodhi was convicted of offences including plotting in October 2003 to bomb Australia's national electricity grid in the cause of violent jihad (Wallace 2006b). Part of the prosecution case was that he had downloaded information, including electricity grid maps, from the internet. Lodhi was sentenced to 20 years in prison on 23 August 2006 (*Regina v Lodhi* [2006] NSWSC 691 23 August 2006). In 2007 it was reported that terrorists might have used information obtained from Google Earth™ to facilitate their planning of (physical) attacks against British troops in Iraq.

> Documents seized during raids on the homes of insurgents last week uncovered printouts from photographs taken from Google™. The satellite photographs show in detail the buildings inside the bases and vulnerable areas such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked (Harding 2007).

In another technology-enabled example, it was reported that:

> from approximately 1997 through at least August 2004, British nationals Babar Ahmad, Syed Talha Ahsan, and others, through an organization based in London called Azzam Publications, are alleged to have conspired to provide material support and resources to persons engaged in acts of terrorism through the creation and use of various internet Web sites, e-mail communications, and other means. One of the means Ahmad and his co-conspirators are alleged to have used in this effort was the management of various Azzam Publications websites, principally www.azzam.com <file:///\\www.azzam.com> [sic], which, along with associated administrative email accounts, were hosted for a period of time on the servers of a Web hosting company located in the state of Connecticut (US DoJ 2007g).

Similar concerns about publicly available information (including geospatial information) about the water industry that could help terrorist prepare for and plan a terrorist act have also been raised in Australia (AGD 2006). The continuing use of online resources to support such terrorist incidents is an area of concern that is unlikely to diminish in the future.

The possible risks to critical information infrastructure that are intimately involved with ICT and that may also provide a cover for criminal and terrorist activities in attacking an ICT system include:

- Changes in the weather patterns that can create changes in the upper atmosphere and affect the reliability of high frequency and satellite communications. Thunderstorms may provide legitimate disruptions from lightning strikes and power surges that isolate users from part of the power-grid.

- The electro magnetic pulse (EMP) was regarded as something only found within the military domain. Small equipment (briefcase size) is available that can cause a localised pulse into a company's property. Swedish Army tests created EMP guns from openly available materials that could permanently damage cars at 30 metres and stop their engines at 90 metres (Clark 2002).
- The failure of third-party dependence perhaps due to industrial unrest, a support company (a service supplier) going into liquidation, changes in government legislation, unavailability of raw materials, political pressure, and export/import embargoes, may all affect information operations.
- Incompatibility issues in hardware and software, along with incomplete testing of information systems have lead to some dramatic accidents. An air show display for the European Airbus provided a situation that was untested during flight trials. As the Airbus made a low pass, the pilots pulled up the plane's nose to climb away under full power; the onboard computer stated that no additional power was available as they were in the landing configuration on final touchdown. This software fault resulted in loss of two test pilots and the Airbus.
- Internal errors to an organisation such as employees' mistakes, accidents and misuse or abuse of ICT assets. Changes in the core values and attributes of generations X and Y may lead to less due care and attention leading to an increase in risks in the way ICT assets are used.
- Over-loading and over-extending existing piggybacked ICT systems causing severe interference to other services. The new developments of Broadband over Powerlines (BPL), is already documented as causing severe interference to other telecommunications services (Linton 2006). There is also potential to interfere with other supervisory control and data acquisition and similar services.

Displacement risks

As methods of user authentication are enhanced, risks of crime displacement will increase. The use of multi-factor card authentication and biometrically enabled systems will result in offenders employing a range of alternative strategies to obtain access to computers and funds. The use of violence, duress, bribery and corruption are the likely areas of concern for the future as criminals seek to circumvent digital identification systems (Smith et al. 2003). As information security increases, risks of insiders collaborating with external offenders, or becoming offenders themselves are likely to increase. This will require organisations to use more extensive and intensive (and perhaps intrusive) personnel checks to monitor the activities of existing staff and to verify the credentials and backgrounds of new staff.

Summary

The next wave of technology-enabled security threats will be targeted attacks aimed at specific organisations or individuals within enterprises. A particular household (or consumer) may be targeted as a vector to support intrusions of more valuable targets. Criminals and malware authors are also targeting remote client machines as a means of attack vector (Kerr 2007). Thus prevention at both the consumer and business levels remains of equal importance. In addition to existing threats, new attacks will come from people, not just with programming experience but also with business and systems (process) and legal experience. There is a significant shift, therefore, in offender focus with more attacks targeting specific businesses and specific systems internal to those businesses. Cyber criminals will probe for weak and poorly guarded or unsecured computer networks within commercial organisations whose ability to detect and respond to fraud or other thefts is slow, imprecise and limited.

The next generation of threats will move from client to server vulnerabilities with offenders moving away from mass distributed attacks that assault any computer connected to the internet to attacks against single corporate networks which are more profitable for cybercriminals. One of the driving forces behind the increase in targeted attacks has been the commitment from major software vendors like Microsoft to develop more secure applications (e.g. trusted platforms such as Microsoft Vista) and release update patches more frequently. This has significantly decreased the success rate of many mass distributed denial-of-service attacks that were thwarted at the applications vulnerabilities level. As traditional cybercrime techniques evolve and are combined, targeted attacks on specific industries or businesses will increase considerably.

The incidence of commercially oriented technology-enabled crime will continue to increase, with traditional threats now being used to obtain funds through theft or extortion. Organisations in the financial services industries will be targeted more heavily than others, with financial gain being the ultimate goal. The reasons for commercially motivated technology-enabled crime will also change from greed and cupidity to politically or ideologically motivated activities. Terrorist financing through the use of technology-enabled crime will develop as an important area of risk.

Legal and evidentiary implications

While transnational crime predates the digital age, continuing development of new technologies and new applications for existing technologies present significant challenges for investigators and prosecutors involved in technology-enabled crime cases. For example, the global nature of cyberspace makes it possible to invade and exploit another's privacy in ways that would not have been possible before. One important characteristic that tends to distinguish technology-enabled crime from 'terrestrial crime' is the matter of jurisdiction. The offending activity (whether it involves sending illicit images of children, malicious code, or fraudulent stock tips) can transit numerous sovereign nations rapidly on the way to the target.

Which, among these nations, can prosecute such cases: the jurisdiction where the activity was initiated, where it had its effect (that is, where the loss or damage was sustained), or where the offending communication may have transited on its path from origin to destination?

The traditional mechanisms of international cooperation, including letters rogatory, mutual assistance and other formalities with roots in the 19th century and earlier, are ill-suited to an era in which offences can be, and are, committed from across the world in real time. The transnational dimension of cyber crime poses formidable challenges for prosecutors, especially those who may be involved upstream in investigations.

Existing legislation

Many of the wide-ranging activities and consequences resulting from technology-enabled crime attacks constitute offences under existing criminal laws in Australia. For example, activities and consequences resulting from botnet attacks constitute offences under *Criminal Code Act 1995* (Cth). The relevant sections of the Act are:

- Section 477.1: Unauthorised access, modification or impairment with intent to commit a serious offence
- Section 477.2: Unauthorised modification to cause impairment
- Section 477.3: Unauthorised impairment of electronic communication
- Section 478.1: Unauthorised access to, or modification of, restricted data
- Section 478.2: Unauthorised impairment of data held on a computer disk, etc.
- Section 478.3: Possession or control of data with intent to commit a computer offence
- Section 478.4: Producing, supplying or obtaining data with intent to commit a computer offence
- Section 480.4: Dishonestly obtaining or dealing in personal financial information
- Section 480.5: Possession or control of thing with intent to dishonestly obtain or deal in personal financial information.

A number of offences under state and territory legislation may also apply to botnet attacks. Using botnets to disseminate spyware (including adware) may also result in a breach of the *Privacy Act 1988* (Cth), the *Telecommunications Act 1997* (Cth), and the *Telecommunications (Interception) Act 1979* (Cth) as personal financial information is harvested and collected without the victims' consent.

In March 2006, the Australian High Tech Crime Centre (AHTCC) reported that a Melbourne man had been charged with botnet-related activities after a joint investigation by the AHTCC, the Australian Federal Police, and NSW and Victoria Police. Initial information was provided by the Belgian Federal Computer Crime Unit following a series of distributed denial of service attacks on IRC servers in Australia, which also affected the United States, Singapore and Austria. The suspect, a 22-year-old male, faces charges under s474.14 of the *Criminal Code Act 1995* (Cth), which creates an offence of using a telecommunications network (such as the internet) with intention to commit a serious offence (AHTCC 2006).

Examples of successful prosecutions of technology-enabled crimes in Australia include:

- In 2007, Takuya Muto, a Japanese student in Australia, was sentenced to two months imprisonment for taking inappropriate pictures of women using a digital video camera (ABC 2007a).
- In 2005, two Australian companies – Global Racing Group Pty Ltd and Australian SMS Pty Ltd – were fined $11,000 and $2,200 respectively for sending unsolicited commercial SMS messages, breaching the *Spam Act 2003* (Cth) (ACMA 2005).

Several other countries have laws that criminalise technology-enabled crime activities (see Table 8). For example, in January 2007, a teenager in Singapore was sentenced to 18 months' probation under the Computer Misuse Act after being found guilty of encroaching upon someone else's internet connection (leeching) (Ng 2007).

Table 8: Countries with technology-enabled crime statutes

Country	Law
Australia	*Crimes Act 1914* (Part VIA), Sections 76B, 76D
Austria	*Privacy Act 2000* (effective as of 1 January 2000)
Belgium	Belgian Parliament in November 2000 adopted new articles in Criminal Code (effective from 13 February 2001) Article 550(b)
Brazil	Law no. 9,983 of 14 July 2000 Art. 313-A & B
Canada	Canadian Criminal Code Section 342.1
Chile	*Law on Automated Data Processing Crimes* no. 19.223, published 7 June 1993
People's Republic of China	Decree No. 147 of State Council of the Peoples Republic of China, 18 February 1994. Computer Information Network and Internet Security, Protection and Management Regulations, (approved by State Council 11 December 1997, and published 30 December 1997)
Hong Kong	Telecommunication Ordinance

Table 8: Countries with technology-enabled crime statutes (continued)

Country	Law
Denmark	Penal Code (Section 263)
Estonia	Estonian Criminal Code (Sections 269 to 273)
Finland	Penal Code Chapter 38 (Section 8)
France	New Penal Code, in effect since 1 March 1993 Chapter III (Articles 323-1 to 323-4)
Germany	Penal Code (Section 202a, 303a, 303b)
Greece	Criminal Code Article 370C§2
Hungary	Penal Code (Section 300 C)
Ireland	*Criminal Damage Act 1991*
Iceland	Penal Code (§228 Section 1)
India	*Information Technology Act 2000* (No. 21 of 2000)
Israel	*The Computer Law* of 1995
Italy	Penal Code (Article 615)
Japan	*Unauthorized Computer Access Law* No. 128 of 1999 (in effect from 3 February 2000)
Latvia	The Criminal Law (Section 241)
Luxembourg	The Act of July 15th, 1993, relating to the reinforcement of the fight against financial crime and computer crime
Malaysia	*Computer Crimes Act 1997*
Malta	*Electronic Commerce Act* (Sections 337 (C) (1) to 337 (F) (1)
Mauritius	The *Information Technology (Miscellaneous Provision) Act 1998* (Act No. 18 of 1998) Penal Code (Section 369A)
Mexico	Penal Code Part 9 (Chapter II)
The Netherlands	Criminal Code (Article 138a)
New Zealand	Crimes Amendment (No 6) Bill (Section 305ZE & 305ZF)
Norway	Penal Code (§145, 151 b, §261 & §291)
Pakistan	Electronic Transactions Ordinance 2002
Poland	Penal Code (Article 267 to 269)
Portugal	*Criminal Information Law* of 17 August 1991
Philippines	*Republic Act* No. 8792 or the E-commerce Law
Singapore	*Computer Misuse Act*
South Africa	South African Law Commission published a discussion paper on computer-related crime
Sweden	The *Data Act 1973* (amendments in 1986 and 1990)
Switzerland	Penal Code (Article 143bis)
Turkey	Penal Code (Section 525/a)
United Kingdom	*Computer Misuse Act 1990*
United States	Federal legislation (updated 15 April 2002) US Code: Title 18
Venezuela	Special Statute against Computer Related Crimes (Published in *Official Gazette of Bolivarian Republic of Venezuela*, 30 October 2001)

Source: Quimbo (2006)

Legislative reforms

In Australia, the growing body of federal law relating to computer technology, particularly telecommunications systems, is likely to increase. These laws operate alongside general criminal laws, and other legislation dealing with such matters as IP rights, classification of publications, terrorism and national security which are also likely to be subject to amendment over the next two years to deal with new technological developments and threats. For example, to ensure that crimes involving the criminal misuse of identity can be prosecuted in each jurisdiction, the Australian Government is considering the introduction of legislation that will criminalise activities associated with identity crime (e.g. identity theft and fraud), on-selling of identity data, and possessing equipment to create identification information (Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General 2007). Currently, only Queensland and South Australia have provisions that specifically criminalise such crime.

Section 408D of the *Criminal Code Act 1899* (Qld) makes it an offence to obtain or deal with another entity's identification information for the purpose of committing, or facilitating the commission of, an indictable offence; punishable by a maximum of three years imprisonment.

The following provisions in Part 5A of the *Criminal Law Consolidation Act 1935* (SA) criminalise the following conduct:

- Section 144B makes it an offence to assume a false identity (including falsely pretending to have a particular qualification or have, or be entitled to act in, a particular capacity) with the intent to commit, or facilitate the commission of, a serious criminal offence; punishable by a penalty appropriate to an attempt to commit the serious criminal offence.
- Section 144C makes it an offence to misuse personal identification information with the intent to commit, or facilitate the commission of, a serious criminal offence; punishable by a penalty appropriate to an attempt to commit the serious criminal offence.
- Subsection 144D(1) makes it an offence to produce or has possession of prohibited material, with the intent to use the material, or to enable another person to use the material, for a criminal purpose; punishable by a maximum of three years imprisonment.
- Subsection 144D(2) makes it an offence to sell (or offer for sale) or give (or offer to give) prohibited material to another person, knowing that the other person is likely to use the material for a criminal purpose; punishable by a maximum of three years imprisonment.
- Subsection 144D(3) makes it an offence to has possession of equipment for making prohibited material intending to use it to commit an offence; punishable by a maximum of three years imprisonment.

The following provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) could also be applied to identity crime:

- s137 makes it an offence for a person to provide false or misleading documents; punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.
- ss138(1) makes it an offence for a person to make a false document with the intention that the person or another will produce the false document in the course of an applicable customer identification procedure and the applicable customer identification procedure is under this Act; punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.
- ss138(3) makes it an offence for a person to knowingly possess a false document with the intention that the person or another will produce it in the course of an applicable customer identification procedure; and the applicable customer identification procedure is under this Act; punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.
- ss138(5) makes it an offence for a person to possess equipment for making a false document knowing that a device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and has the device, material or thing in his or her possession with the intention that the person or another person will use it to commit an offence against ss138(1); punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.
- ss138(6) makes it an offence for a person to make or adapt a device, material or other thing; and knows that the device, material or other thing is designed or adapted for the making of a false document (whether or not the device, material or thing is designed or adapted for another purpose); and makes or adapts the device, material or thing with the intention that the person or another person will use it to commit an offence against ss138(1); punishable by a maximum of ten years imprisonment or 10,000 penalty units, or both.

Examples of recent amendments of criminal law in other countries include:

- In the United Kingdom, new computer misuse provisions were introduced in the *Police and Justice Act 2006* by way of amendment to the *Computer Misuse Act 1990* on December 2006 to deal with emerging cyberthreats.
- The *Spam Control Act 2007* passed in the Parliament of Singapore on 12 February 2007 (Singapore Infocomm Development Authority 2007; Singapore Parliament 2007) to deal with emerging risks associated with spam (e.g. the use of address harvesting software designed to collect, compile and acquire electronic addresses by searching the internet will be illegal under the proposed Act).

Although the process of harmonisation of cybercrime legislation throughout Australia has been consistent, the need for uniformity will become more pronounced as the number of technology-enabled crimes continues to increase. Existing legislation may not be suitable or adequate within the context of developments in using new and emerging technologies to commit technology-enabled crimes. In addition, existing offences, although technically adequate, may be practically impossible to use, such as occurs in the case of botnet prosecutions where evidence would need to be obtained concerning the thousands of computers that have been compromised. New offences of creating a network for illegal purposes and selling established botnets might need to be developed to deal with such emerging threats.

With the addition of Part 10.6 to the *Criminal Code Act 1995* (Cth) that contains offences prohibiting the misuse of telecommunications networks for a range of illicit purposes, it can be expected that section 474.14 will largely displace the need to use previously enacted unauthorised access offences, such as those in section 477.1. With these new telecommunications offences, it is likely that Australian government agencies will assume a more dominant role in the investigation and prosecution of technology-enabled crime offences, than was previously the case. Other offences in Part 10.6 are also capable of application to a range of conduct not previously covered by federal criminal law, such as child pornography, grooming, and racial vilification.

Although existing Australian laws cover spyware-related malicious activities, installing programs that collect and send back information about usage (‘spyware’) is not currently criminalised. The enactment of legislation to proscribe the usage of spyware has been proposed (DCITA 2005) and its application will need to be monitored to ensure it achieves its objective. In view of these changes, the need for additional resources for federal policing and prosecution agencies will become more pressing over the next two years.

Criminal complicity

The years ahead will see an increase in instances of individuals acting jointly in the commission of technology-enabled crime. Examples of potential accessories to such crimes include:

- members of the public recruited to receive funds into their bank accounts before transferring the money overseas using wire transfer services, minus a certain commission payment and thereby facilitating money laundering – money mules
- business employees who disclose passwords, security codes or database details to others and thereby intentionally or recklessly facilitate unauthorised access
- members of hacker communities sharing security information that allows others to obtain unauthorised access to computers or data
- members of hacker communities building their own encrypted programs (e.g. CarderIM) to establish secure encrypted communication that facilitates them to sell confidential information (e.g. credit-card numbers and email addresses), part of an underground economy dealing in financial data

- software 'crackers' who strip business or entertainment computer programs of their copyright and information management protections and distribute these through 'warez' websites
- providers of illegal signal decoding hardware or similar circumvention devices that allow users to obtain unauthorised free access to subscription services, such as pay-TV
- creators and manipulators of malware, such as viruses, worms, bots and spyware that can be used to steal confidential information or hijack computer functions in furtherance of financial or other crimes
- users of card skimming or similar devices that can surreptitiously capture personal and financial details and facilitate identity fraud and financial crimes
- experts in encryption, steganography or anti-forensics techniques that can help conceal criminal activities or remove evidence that may incriminate offenders.

The implications of these trends are that investigations and prosecutions are likely to become more complex and lengthy than at present, with the need for investigators to take coordinated and timely action against multiple suspects contemporaneously. Again, this will entail resourcing implications for law enforcement in terms of time and resources throughout the country, and internationally.

Jurisdictional issues

Traditionally, courts have accepted jurisdiction if a person against whom legal proceedings are brought is physically present in the geographical territory (i.e. country or state) in which the court operates, or is a citizen of the territory, or if there is some other sufficient 'territorial nexus'. Such a connection might arise if the alleged victim of a crime is in the territory, or some other effect of the crime, sufficient to exercise jurisdiction, is present. For crimes involving physical acts, rules of jurisdiction have largely been relatively easy to apply, but the situation is more complicated for online activity.

> One of the most important characteristics that tend to distinguish computer-related crime from 'terrestrial crime' is the matter of jurisdiction. The global nature of cyberspace makes it much easier than ever before for a person sitting on one side of the world to commit a crime on the other side (Smith et al. 2004).

It can reasonably be anticipated that technology-enabled crime prosecutions involving multiple jurisdictions will continue to arise in the years ahead. Tracking the fragile and ephemeral digital trails often requires swift action. Because online offending transcends borders so easily, numerous territories can simultaneously assert jurisdiction, particularly when an attack transits multiple jurisdictions with different regimes for preserving evidence. Timely access to evidence located in one or more foreign countries may be difficult or impossible, as it would normally require the assistance of authorities in the foreign country (or countries) that for various reasons may be unwilling or unable to assist. When the suspect is located abroad, these difficulties are compounded. This leads to the need to chose the most appropriate forum for proceedings, with the choice having important consequences due to the different legal systems and penalties that apply in different countries. Conflict in the laws and jurisdictional issues are likely to compromise the effectiveness of legislation and hamper investigation and prosecution of cross-border crimes. It will be necessary for the international community to urgently address problems of multiple jurisdictions.

Identifying and determining the physical location of the perpetrator will continue to be a challenge in an environment where a skilled offender can exploit technologies of anonymity and methods of stealing electronic identities to great advantage. The networked environment of cyberspace compounds this difficulty, as offences that appear to originate in far-flung countries may in fact have been launched from across town. Conversely, apparently 'local' offences may have originated on the other side of the planet.

Issues relating to extradition are also likely to arise. Although to date, there are no examples of Australians having been extradited overseas, or foreign nationals being extradited to Australia, in relation to offences that could be characterised as technology-enabled crimes, a British national living in Australia, Hew Raymond Griffiths, has been extradited from Australia to the United States to face criminal charges in connection with operating the internet software piracy group, "DrinkOrDie" (US DoJ 2007h). He was extradited from Australia to the United States in February 2007 and pleaded guilty in April 2007 before United States District Judge Claude M. Hilton to one count of conspiracy to commit criminal copyright infringement and one count of criminal copyright infringement (US DoJ 2007d). If convicted on both counts, Griffiths could receive a maximum sentence of ten years in prison and a US$500,000 fine.

Decisions on whether to seek extradition of the offender to deal with them under one's own law will be heavily dependent on the financial cost involved and the existing formal arrangements between countries. There will continue to be demands placed on Australian law enforcement to work collaboratively with overseas law enforcement agencies in identifying and investigating cases suitable for extradition.

Criminal defences

As cases involving technology-enabled crime continue to come before the courts, those accused will develop new and sophisticated defences to charges (see generally, Smith et al. 2004). It may be expected, for example, that 'public benefit' defences to child pornography charges will increasingly be relied upon, and that self-defence may be used to resist charges relating to 'reverse hacking' (e.g. victims resorting to illegal hacking-back remedies).

Other defence arguments specific to technology-enabled crimes will continue to arise, such as challenges to the admissibility of electronic evidence, assertions that computers were under the control of other parties (the 'unknown hacker' defence) and computers were compromised by browser hijacking programs (making it as if the defendant had surfed to pornographic websites), and claims that online behaviour was merely role-playing. Defendants might also challenge the 'presumption of reliability' (presuming that computer forensic software such as EnCase reliably yields accurate digital evidence) particularly if open source forensic tools that have not been cross validated (cross-checking the results of one software tool against the results of another based on industrial baselines) were used to extract the digital evidence.

> The reliability of a particular computer system or process can be difficult to assess. Programmers are fallible and can unintentionally or purposefully embed errors in their applications. Also, complex systems can have unforeseen operating errors, occasionally resulting in data corruption or catastrophic crashes. Possibly because of these complexities, courts are not closely examining the reliability of computer systems or processes and are evaluating the reliability of digital evidence without considering error rates or uncertainty (Casey 2002).

Defendants charged with technology-enabled crimes such as denial-of-service attacks may also argue that their computer was infected with malware that made it perform functions beyond their control and knowledge. To further substantiate their arguments, it is also likely that criminals will infect their computers with malware before committing the crimes. Similar arguments have sometimes been raised when child pornography is discovered on personal computers. It can be expected that such arguments will continue to be advanced in the years ahead.

Novel defence arguments raised in response to child pornography or child grooming prosecutions will continue to include the 'fantasy defence' according to which the sender of messages to underage children claims to have really believed that the person with whom they were dealing was an adult, and that all concerned were merely role-playing or engaging in sexual fantasies. Of course, in some cases such a belief would be accurate, as a number of successful investigations in Australia and overseas have involved law enforcement officers posing as children online and engaging in chat room conversations with predators. In some jurisdictions, the defence of entrapment might succeed in such situations if it can be argued that the defendant did not seek to engage in criminal activity but was merely enticed into doing so by a sting operation. Although in some jurisdictions, the defence of entrapment might succeed in such situations if it can be argued that the defendant did not seek to engage in criminal activity but was merely enticed into doing so by a sting operation, the court might have little sympathy for the accused person as illustrated in the case of *R v Ferguson* [2006] 3 DCLR (NSW)

70 (9 March 2006). Ferguson responded to an advertisement on the internet selling child pornography magazines posted by an undercover officer, offering to make videos with his stepdaughter, and writing scripts for the same activity. Although no children were ever likely to be victimised in this case, Ferguson was sentenced to a term of two years and two months imprisonment with a non-parole period of one year and four months.

Some defendants have also argued, usually unsuccessfully, that engaging in such behaviour was ‘therapeutic’ or was part of a research project.

> Issues commonly introduced by the defense in undercover cases, such as entrapment, role-playing or fantasy, and the crime as a factual or legal impossibility, are common but seem to be ineffective (Mitchell et al. 2005).

For example, on 4 December 2006, Christopher Rajlal of Santa Clarita, California was arrested by the FBI after Rajlal corresponded with an undercover agent whom he believed was a 7th Grade minor. Rajlal was subsequently indicted on attempted use of a facility of interstate commerce to induce a minor to engage in criminal sexual activity, and distribution and possession of child pornography (FBI 2007c).

Denial of improper purpose has also been a feature of some unauthorised access cases, where it is claimed that the defendant was merely pursuing the altruistic aim of exposing the vulnerabilities of computer systems and databases.

Procedural and evidentiary powers

Authorities expect that those charged with technology-enabled crimes will continue to challenge the legality of electronic searches conducted by law enforcement officers who seek to obtain evidence of technology-enabled crime. Difficulties will continue to arise in determining ‘reasonable suspicion’ of the existence of evidentiary material relevant to the crime before private premises can be searched. Difficulties will also arise owing to search warrants being insufficiently precise or insufficiently related to the purposes for which the warrant was issued.

The need for law enforcement to be able to obtain evidence legally through remote access to computers located in other jurisdictions will become increasingly important, as will the need to obtain access codes to facilitate access to encrypted or otherwise protected data through use of Trojan programs. The ability to obtain evidence in this way needs legislative clarification, as does the use of digital evidence obtained covertly in court proceedings.

Section 3LA of the *Crimes Act 1914* (Cth) provides a power to compel, by order of a Magistrate, any person suspected of having committed offences to which the warrant relates, or the owner or lessee of the computer or an employee of such a person, to provide assistance that is reasonable and necessary to allow the officer to do one or more of the following:

- Access data held in, or accessible from, a computer that is on warrant premises.
- Copy the data to a data storage device.
- Convert the data into documentary form.

Failure to comply with such an order is punishable by 6 months imprisonment. This provision, though seldom if ever used thus far, created a degree of apprehension among legal and computer professionals after its introduction (James 2004). It is likely that this provision will be used more often in the future in order to facilitate access to encrypted or password-protected data. Arguably, the maximum penalty may need increasing in view of the importance of the provision.

Although some memoranda of understanding have been negotiated with private sector organisations, it will become increasingly important to have the cooperation of ISPs and other organisations to facilitate access to data. It will also be likely that ISPs may, themselves, be subject to prosecution for failing to cooperate with law enforcement. There are now provisions that impose obligations on ISPs and internet content hosts to alert police to suspected online child pornography and child abuse material (*Criminal Code Act 1995* (Cth), Section 474.25), and enforcement powers to compel people with knowledge of passwords or computer security protections to assist investigators (*Crimes Act 1914* (Cth), Section 3LA and *Customs Act 1901* (Cth), Section 201A). As organised crime groups move to greater use of the internet and other computer-related technologies, particularly in committing fraud and financial crimes, it can be expected that computer experts who assist by providing their tools of trade will face accessorial liability in relation to these activities.

Delays in the use of conventional mutual legal assistance applications will continue to make their use problematic in technology-enabled crime investigations where cooperation needs to be provided within hours rather than years. On the other hand, however, technology clearly facilitates surveillance and detection enabling law enforcement to follow electronic data trails. The use of data mining and database analysis tools, currently used by financial institutions to detect payment card transaction anomalies, will increase in importance in the future and may lead to reduction of some types of technology-enabled crime.

Tighter regulatory controls may also need to be introduced to control private sector investigators. For example, at present the use of data surveillance devices by public police is regulated in most jurisdictions. Legislation does not, however, regulate data surveillance by private investigators that use technologies for keyword searching and blocking of email, surveillance of internet usage and keylogging.

Computer forensic evidence

With increased digitisation of information, the future will see the increased likelihood of digital content being a source of dispute or form part of underlying evidence to support or refute a dispute in judicial proceedings.

Digital evidence, typically the first step in any computer forensic process, can be broadly defined as any relevant information or data in electronic storage used to support or prove a fact at issue in judicial proceedings. The three broad ways in which digital evidence can be categorised are:

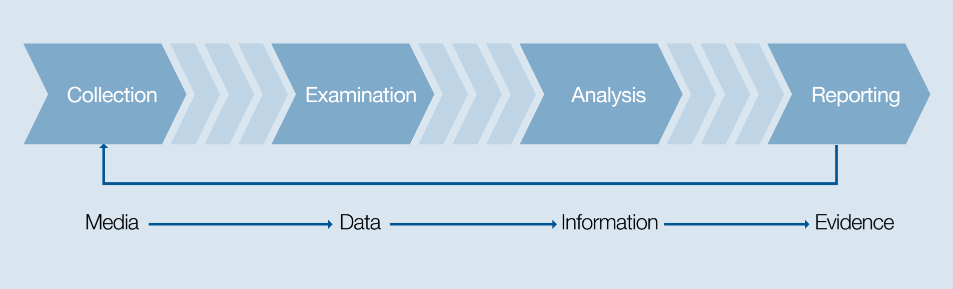
- **records that are computer-stored:** examples include email messages, word processing files, digital images and digital videos
- **records that are computer-generated:** examples include log files generated by web servers
- **records that are partially computer-stored and partially computer-generated:** examples include Excel spreadsheets that contain both human statements and computer processing (Standards Australia International 2003).

Digital evidence differs from traditional evidence. The former is intangible and often transient in nature, and can easily be duplicated, copied, shared, disseminated, modified and damaged. In order to ensure all elements of a proper (digital) evidentiary foundation are correctly established, an understanding of fundamental characteristics underlying digital evidence is crucial in addition to traditional evidential procedures (e.g. thorough documentation to ensure chain of custody). For example, volatile storage media such as hard drives should be stored in static-free bags and recorded. They should be marked as evidence and should not be stored near anything, particularly magnets that could damage evidence on the device.

To address the specific and articulated needs of law enforcement and to ensure (digital) evidentiary admissibility, forensic researchers and practitioners have developed various models for the computer forensic process. Computer forensics can be defined as the science of identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data (NIST 2006a).

Although models for the computer forensic process differ primarily in how granular each phase of the process is and in the terms used for specific phases, they reflect the same basic principles and the same overall methodology (NIST 2006c) particularly proper documentations for the chain of custody. The basic model the National Institute of Standards and Technology has adopted is shown in Figure 3.

Figure 3: Forensic process



Source: NIST (2006c): 3–1

The process consists of:

- **Collection:** Identification of digital evidence is typically the first step in the forensic processes for computer forensic models. Knowing what evidence is present, where it is stored and how it is stored is vital to determining which processes are to be employed to facilitate its recovery. Computer forensic examiners must be able to identify the type of information stored in a device and the format in which it is stored so that the appropriate technology can be used to extract it.
- **Examination:** Given the likelihood of judicial scrutiny in a court of law, it is imperative that any examination of the electronically stored data be carried out in the least intrusive manner. There are circumstances where changes to data are unavoidable, but it is important that the least amount of change occurs. In situations where change is inevitable it is essential that the nature of, and reason for, the change can be explained.
- **Analysis:** Analysis of digital evidence includes extraction, processing and interpretation of digital data. This is generally regarded as the main element of forensic computing. Analyses should be performed on the evidence copy and care taken not to alter the original copy of the evidence. Once extracted, digital evidence usually requires processing before people can read it.
- **Reporting:** Presentation of digital evidence: involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

Possible threats to legislative solutions

Possible threats to legislative solutions to detecting and successfully prosecuting technology-enabled crime are the level of education of cybercriminals and the constant developments in data storage and dissemination technologies.

Better educated criminals

Technology-enabled crime is getting more sophisticated and organised (Seger 2005), perhaps because profiles of cybercriminals differ significantly from those of traditional criminals. Ease of communication by like-minded individuals, who know each other only online, is probably a major factor in this as the internet makes it easy to 'meet' and plan activities, including crime. For example, a 2006 case involved David Beavan, Alan Hedgcock and Robert Mayers who had never met in person and knew each other only online. All three were convicted at London's Southwark Crown Court of a conspiracy to rape a girl under 16 years of age, based on a discussion in an internet chat room (GB CPS 2006).

These better-educated criminals are likely to explore alternatives to hiding data using the internet. This includes storing data on password-protected file sharing websites, email accounts and less reputable content providers hosted by countries with lax cybercrime legislation. They are also likely to leverage the use of anti-forensic tools to further impede collection of evidence. Anti-forensic tools, such as trail obfuscation tools and wiping/zero-footprinting tools (e.g. evidence eliminator or window wiping/scrub software), and information-hiding tools, including steganography, can be used to destroy, hide, manipulate and counterfeit evidence (Harris 2006, Peron & Legary 2005) are freely available on the internet (e.g. http://www.securitywizardry.com/foranti.htm).

Developments in data storage and dissemination technologies

Given the likelihood of judicial scrutiny in a court of law, it is imperative that any examination of the electronically stored data be carried out in the least intrusive manner. Data examination involves assessing and extracting the relevant pieces of information from the collected data. The latter is by no means easy due to increased data storage capacities. For example, an acquired storage medium is likely to contain hundreds of thousands of data files. Identification of data files containing information of interest is both time consuming and daunting. Moreover, identified data files (of interest) may contain extraneous information that needs to be filtered.

With the advent of more complex data storage and dissemination technologies, forensic investigators face an increasingly difficult task. These developments (in data storage and dissemination technologies) can impede forensic investigators and prevent police from acquiring digital evidence and analysing digital content forensically in terms of time and resources. Examples include:

- **Different formats and platforms used to store digital content:** The constantly evolving formats are independently developed by different vendors and according to different standards. The proprietary storage media (e.g. iPod, flash memory and USB memory sticks) and proprietary cryptographic algorithms used (e.g. encryption) could be incompatible (with one another) and compromise the integrity of the data during extraction or converting from incompatible proprietary formats. Therefore, an in-depth understanding of how different technologies and applications operate is crucial in collecting digital evidence. Moreover in response to changing contexts, various computer forensic tools and techniques have to be re-designed and re-engineered.
- **Increased data storage capacities:** The best form of immediate backup to make is a binary disk image (also referred to as bit stream backup or mirror image backup). Enhanced data storage capacities (e.g. large volume data sets) and more complicated data accessibility (e.g. networks of interconnected computers located in different locations) will impede bit stream backup in terms of time and resources.

The amended Federal Rules of Civil Procedure in the United States that took effect on 1 December 2006 (http://www.uscourts.gov/rules/congress0406.html) will result in organisations having to produce a wider range of electronically stored information in court proceedings.

This would require forensic investigators and incident handlers to have in-depth knowledge of forensic principles, guidelines, procedures, tools, and techniques, as well as anti-forensic tools and techniques. Conversely, forensic investigators and incident handlers can also make use of searching utilities such as Google Desktop™ application to reduce the time and resources required in searching file systems for keywords.

> The Google Personal Desktop Search™ is remarkably interesting for its caching of certain file types such as text, that continue to exist after the original item has been deleted. This may continue indefinitely, and the result is not easily removed. Microsoft Office files, even password protected ones, are indexed once opened in the local system, and saved in plain text within the Google Desktop Index™ (Turnbull et al. 2006).

Other organisations, such as ISPs, may also record information, such as logs of network activity and computers and email servers located in other countries. In botnet-related cases, evidence is likely to be stored on hundreds or thousands of compromised computers and various ISPs located in various jurisdictions. It can reasonably be anticipated that technology-enabled crime prosecutions involving multiple jurisdictions will continue to arise in the years ahead. Because online offending transcends borders so easily, numerous territories can simultaneously assert jurisdiction. This leads to the necessity of choosing the most appropriate forum for proceedings, with the choice having important consequences due to the different legal systems and penalties that apply in different countries. It will be necessary for the international community to urgently address problems of multiple jurisdictions.

Technology-enabled crime in the courts

Criminal courts hearing cases involving technology-enabled crime, or other cases involving electronic evidence, face particular issues which will continue to arise in the future. Difficulties concern the presentation of complex and technical evidence, the heavy reliance on expert opinion in technology-enabled crime cases, the use of complex and novel arguments relating to admissibility of evidence or the exercise of discretions, difficulties of juror comprehension of offence elements and evidence, the use of novel defences and defence arguments, and devising appropriate sentences for convicted offenders. For example Sprague (2006) suggested that

> [c]omputer crime prosecutions very often are, or can be forced into being, a form of "complex litigation," chock full of confusing technological terms and concepts. The average juror is generally ignorant of both the theory and practice of computer science. Even "computer savvy" jurors are unlikely to have the training or experience to comprehend complex issues involving networking, security theory and practice, computer architecture, operating systems, system administration, or programming. A conscientious juror may well (and should) have a problem concluding that all reasonable doubt has been eliminated by evidence that he or she does not fully understand (Sprague 2006: 145).

The judge in the Federal Court of Australia case of *Kabushiki Kaisha Sony Computer Entertainment v Stevens* [2002] FCA 906 (26 July 2002) also indicated that '[t]he Court should not be left in a position where it has to guess as to the operation of technological processes and how those processes might satisfy the statutory language'. Such (technical) information that needs to be communicated to the judiciary by the security experts includes:

- the possibility of a wide variety of evidence being extracted from an increasing diversity in sources of computer or electronic exhibits (e.g. GPS devices, engine management systems, CCTV systems, digital cameras and mobile phones).
- the use of mathematical hash algorithms in computer forensics as a means of evidence authentication to be able to trust the hash values that uniquely identify electronic evidence.

- the use of filtering to reduce data volumes including the use of hash sets or targeted searching as their use or non-use may have significant impact on processing time, and accuracy of the results.
- the ability to visualise the ‘actual size’ of digital data. It has been noted that in a number of court cases, judges, prosecutors and unassisted defence lawyers have asked for all data on a computer exhibit to be printed out. In many technology-enabled cases, a printout of all data produced as a result of an examination would be practically impossible. For example, the amount of information gathered during the investigation in Operation Firewall by the United States Secret Service is estimated to be approximately two terabytes – the equivalent of an average university’s academic library (US SS 2004). Moreover, hardcopy printout of an electronic document does not necessarily include all the information stored in the computer or electronic exhibit (e.g. data held in memory) (see *Armstrong v Executive Office of the President* 1 F 3d 1274 (DC Cir 1993)).

Much of the legislation governing technology-enabled crime has only recently been introduced in Australia and is awaiting judicial interpretation. It can be anticipated that difficulties will arise as untested provisions are relied on in prosecutions.

There will continue to be a need to enhance the skill base of lawyers, judges, juries, and court officials when dealing with cases involving computer forensic issues through initiatives such as training materials exploring both legal and technical aspects of technology-enabled crime. This will ensure that judges with appropriate experience and financial and IT skills are available to hear these trials. Continuing training in the presentation of complex technological information to courts and juries for witnesses, particularly computer forensic expert witnesses, will also need to be provided. In addition, the use of networked and electronically enabled courtrooms that can display electronic evidence in a clear and accessible way to court officials and participants in proceedings will need to be extended. Information protection standards including best practice guidelines for managing electronic records will also need to be developed to ensure effective use of technology and to maintain the confidence demanded of our courtroom systems. A summary of available courtroom technology in Australia’s higher courts is described in Table 9.

Table 9: Summary of available courtroom technology in Australia's Supreme Courts

Supreme Court	Document camera	Projector and screen	Digital audio facilities	Computers /laptops	Internet	Plasma/ LCD monitors	Individual monitors for jury and/or witness
Cth	✓	✓	✓		✓	✓	✓
ACT		✓					✓
NSW	✓	✓	✓	✓	✓	✓	✓
NT			✓			✓	
Qld	✓	✓	✓	✓	✓	✓	✓
SA	✓	✓	✓			✓	✓
Tas[a]	✓	✓	✓	Available to judges only		✓	
Vic	✓	✓	✓		✓	✓	
WA	✓	✓	✓			✓	✓

a: Personal communication, Dorothy Shea (Librarian of the Supreme Court of Tasmania) to Australian Institute of Criminology (2 May 2007)

Source: Adapted from De Wilde (2006): 325–326. Information was correct as at January 2006

Sentencing and punishment

Sentencing practices in cases of technology-enabled crime are continuing to develop and arguably some sentences may seem overly lenient in view of the fact that technology-enabled crime is seen as a novel phenomenon with some types of conduct only recently having been proscribed. The future will see the need to harmonise legislation concerning punishments for technology-enabled crimes throughout Australia, and, ideally, across the globe. Achieving some measure of uniformity will help minimise the risk of jurisdiction shopping by offenders who seek countries from which to base their activities that have the least severe punishments.

In sentencing hearings, it is likely that offenders will raise a range of new mitigating considerations. In view of the ever-expanding use of personal computers, it is likely that 'computer addiction' (or 'internet addiction disorder') will be raised more often as a mitigating factor, or even as a defence vitiating intent.

The future will also see courts continuing to experiment with new punishments such as forfeiture of computers and restriction-of-use orders. Restricting access to computers or the internet can have potentially profound consequences, making punishments of this kind arguably more severe than traditional conditional orders. The simple prohibition on the use of a computer could deprive a person of the ability to find employment in today's inter-connected world. Consequently, this could reduce, not enhance, the possibility of rehabilitation.

Rather than seeking to impose restrictions on the use of computers as a means of punishment, courts could perhaps adopt the alternative approach of requiring offenders to use their computer skills or knowledge for constructive purposes. This could include orders that require offenders to deliver lectures to the public or to schools about the dangers of computer crime, and discouraging others from engaging in similar conduct, and performing supervised community service in the technology-enabled field. Care, however, has to be taken to ensure that offenders do not profit from their crimes (e.g. profiting from the sales of autobiography or rights to a movie).

Summary

The prosecution and judicial disposition of cases involving technology-enabled crime (particularly arising from the global nature of much technology-enabled crime) will continue to raise certain considerations that make these cases different from cases involving conventional crime. These key issues faced by law enforcement and prosecution include the need for legislative reforms due to new offences, criminal complicity, jurisdictional issues (whether jurisdiction exists and the problem of concurrent jurisdiction); complex and novel arguments relating to admissibility of evidence or the exercise of discretions, novel defences and defence arguments (including in sentencing proceedings); and imposing appropriate sentences on convicted offenders.

Policing and preventive strategies

The threat of technology-enabled crime has given rise to a growing demand for devising new strategies of response. These include the need to reduce the opportunities for technology-enabled crime to occur, to make technology-enabled crime more difficult to commit, to increase the risks of detection and punishment associated with committing technology-enabled crime, and showing that there are fewer benefits to be gained from committing such crimes.

There is no single all-encompassing answer to responding to technology-enabled crime. In fact, countering these risks is a multi-dimensional challenge. It requires effective coordination and collaborative efforts on the part of a wide range of government and private sector entities that can occur at various levels, as described in this chapter.

The role of the information and communications technologies security industry

Poorly designed, executed and maintained security protocols, programs, processes and devices leave computer networks open to attack. In 2007 IBM reported that the number of detected security vulnerabilities had increased by almost 40 percent from 2005 to a total of 7247 in 2006 (IBM 2007). Examples include:

- A case involving the Extended Copy Protection and the MediaMax CD-3 programs embedded in Sony BMG music CDs designed to protect copyright materials. In 2005, a security researcher discovered that both the Extended Copy Protection program introduced system vulnerabilities enabling both programs to covertly transmit usage information back to the vendor and the music label. As a result, a number of lawsuits were filed against Sony BMG; the company recalled all affected CDs and released a software utility to remove the rootkit component (Halderman & Felten 2006). Shortly after the existence of both programs became public, a variety of malware exploiting the programs to avoid detection appeared (e.g. Stinx-E Trojan).
- A case involving the GO-910 satellite navigation devices manufactured by TomTom between September and November 2006. In January 2007 TomTom reported that some of their GO-910 models might be infected with the win32.Perlovga.A and TR/Drop.Small.qp Trojans (TomTom 2007).
- In February 2007 Trend Micro announced that vulnerability had been discovered in their antivirus scan engine (versions 8.0 and 8.3) that might allow attackers to execute malicious code and take control of the system (Trend Micro 2007).
- In May 2007, Cisco Systems announced that multiple vulnerabilities that can result in a denial of service (DoS) condition, improper verification of user credentials, and the ability to retrieve or write any file from the device filesystem had been discovered in their IOS FTP Server (Cisco Systems 2007).

Many such risks can be minimised by the industry developing more secure hardware and software. It would, however, be insufficient to reduce software vulnerabilities and the overall defect content in software and hardware components. Security should also be integrated into the software and system development life cycle, as retrofitting security implementations to a released system typically require significant architectural or coding changes. Making late changes can be technically challenging and costly. Although several international standards have been designed to facilitate and ease the secure development of applications (also known as SDA), there does not appear to be widespread adoption of SDA (by software and hardware vendors). This could, perhaps, be attributed to competitive market forces dictating that software and hardware products with sophisticated functionalities have to be delivered at accelerated speeds (Viega et al. 2001). Consequently, less thorough code reviews and vulnerability testing are conducted resulting in less robust software and hardware applications that contain security flaws and bugs.

Industry has been making efforts to integrate security within the software and system development life cycle, in particular during early requirement analyses. Several industry initiatives aiming to design more trustworthy systems and to provide security mechanisms at the device interface have been established. For example, the Trusted Computing Group was formed to develop and promote open, vendor-neutral industry specifications and industry-wide codes of conduct for trusted computing. The Trusted Computing Group also plays a significant role in promoting best practice. Manufacturers need to be made aware that they could achieve marketing and competitive advantages if they produced new products with higher levels and more innovative types of security that would help combat technology-enabled crime. Organisations actively seeking to go beyond mere compliance with existing legislation would generate greater consumer trust and confidence in the new world of informed consumers. Moreover, vendors of secure software and hardware would spend less time and resources on fixing and releasing patches for vulnerabilities. Law enforcement and security researchers could contribute to a stronger technology security environment by notifying manufacturers and vendors of weaknesses discovered in technologies to enable fixes to be formulated, by publicising weaknesses discovered during investigations and research, and by working with industry to identify potential new and emerging risk areas.

Public–private sector partnerships

Government has driven much of the response to technology-enabled crime but the private sector plays a crucial role. The latter includes its contribution to training and research. An example is the International Centre for Missing & Exploited Children training of police officers and prosecutors around the world to combat online child abuse and child pornography. Under this joint initiative, Microsoft and the International Centre for Missing & Exploited Children (http://www.icmec.org/) have linked with over 30 financial institutions worldwide, including credit card companies, to develop a system that will monitor and report online commercial transactions involving crimes against children. Another recent initiative includes the following action plan to support the United States-based Financial Coalition Against Child Pornography announced by the Association of Banks in Singapore on January 2007 that

> its 9 merchant acquiring and credit card issuing member banks (ABN AMRO Bank NV, Bank of China Limited, Citibank Singapore Limited, DBS Bank Ltd, The Hongkong and Shanghai Banking Corporation Limited, Maybank, OCBC Bank, Standard Chartered Bank and United Overseas Bank Limited) have banded together to work with the major payment card providers in Singapore (including American Express, JCB, MasterCard and Visa) to help combat child pornography on the Internet (Association of Banks in Singapore 2007).

Government, industry and higher educational institutes could create strategic partnerships to equip technology-enabled crime investigators with the appropriate universal standards of competence as in other professions. Government agencies could play a major supporting role in assisting software and hardware vendors in developing secure software and hardware components. For example, the United States National Security Agency helped Microsoft develop their Vista operating system to ensure it met United States Department of Defense requirements (McMillan 2007b). An example of a cross-institutional partnership is the fraud prevention early warning systems jointly established by a number of retail banks in the United States – Bank of America, BB&T Corporation, JPMorgan Chase, Wachovia, and Wells Fargo – to bring together fraud prevention expertise to better fight fraud (Early Warning 2006).

Many of the critical infrastructure sectors are privately owned and therefore, instituting an effective coordination with private sector organisations including public–private crisis management plays a pivotal role in critical infrastructure protection within and between countries. Partnerships between public sector police and private agencies will also form strategic alliances outside national borders for risk management and continue to be a guiding principle of technology-enabled crime policing in the future. The perceived benefits of such alliances include:

- increased reporting to police
- more timely sharing of information
- shared equipment for processing digital evidence
- better preservation of evidence
- avoidance of duplicated efforts
- reduced costs
- bi-directional training of investigators.

For the private sector, partnerships will also result in commercial opportunities and, perhaps, more effective, policing avenues for their clients. Such partnerships may also prepare businesses for pandemics and natural disasters.

Public–private sector partnerships may not be easy to establish or manage given the range of technical, legal and political issues and the economic complexity of cyberspace infrastructure. Investigations by law enforcement agencies and private investigators will continue to be hindered by the global distribution and increasingly corporate ownership of internet and cyberspace infrastructure and services. Trails of evidence may pass through innumerable hosts, each requiring legal authority to access evidence, while gambling at each step on evidence retention versus business demands for data storage. Both sectors face difficulties establishing identity from online identifiers. The potential sources of digital evidence have multiplied and are increasingly wireless, miniature and encrypted. By virtue of global organisations spanning international and interstate jurisdictions, corporate investigators will continue to face the difficulties of having to deal with many police forces and inconsistent local laws. Civil search and seizure powers available to private investigators, such as Anton Piller orders and Mareva injunctions, are more restrictive than police warrants. Other impediments in relation to transnational policing of technology-enabled crime include deciding jurisdiction, negotiating mutual assistance and extradition, and logistical issues such as navigating time zones and languages.

Other likely risks associated with public–private investigative partnerships include the inadvertent creation of opportunities for corruption, mishandling of investigations, misinterpretation or planting of digital evidence, and copying of seized, illicit materials. The potential to constrain public police in commercial-in-confidence situations may reduce transparency, and possibilities may arise for cases to be referred to 'for-fee' private investigators that may result in incidents not being investigated if victims cannot or decide not to pay.

Information sharing

The emergence of international networks of Computer Emergency Response Teams (e.g. CERT, AusCERT, APCERT and SingCERT), 24/7 law enforcement contact points (e.g. Australian High Tech Crime Centre) and other public/user interest groups underscores the intrinsic importance of information sharing in fighting crime. As at 30 June 2006, the Australian Security Intelligence Organisation had established international partnerships with 268 agencies in 113 countries, which facilitates the sharing of knowledge and capabilities (Ferguson 2007). Examples of arrests resulting from information sharing and joint investigations include:

- In January 2007, information supplied by Swiss authorities led to the arrest of a Melbourne man for using a carriage service for child pornography and possession of child pornography obtained through a carriage service (AAP 2007c).

- In late 2005, the collaborative efforts of the FBI, Turkish and Moroccan law enforcement agencies resulted in the swift arrest of the Turkish and Moroccan authors of the Zotob worm (Lemos 2005, FBI 2006a).

Public–private sector partnerships could improve industry trust and confidence when the industry shares sensitive information, and could provide the following assistance:

- Build resilient systems (e.g. supply chains) and also cybersecurity protection.
- Provide training and enhance security awareness of the industry, in particularly small and micro businesses. Examples of training guidelines include the United States National Institute of Standards and Technology documents (e.g. NIST SP 800-12, 16, 50).
- Identify risks that could help develop effective measures and mitigation controls. Controls required to mitigate individual risk might vary among different types of systems. For example, requirements for critical control systems usually differ from typical IT systems on aspects such as performance, availability, and risk management.
- Share information and improve the speed of information dissemination that would help post information disclosure controls, such as development of secure real-time information sharing networks. For example, the Australian Security Intelligence Organisation Business Liaison Unit was established in 2005 to provide an interface between Australian businesses and Australian intelligence agencies.

Many advanced countries have now produced comprehensive critical information infrastructure protection planning processes and best practices. The TCRN Critical Information Infrastructure Protection Handbook and the situation reports of the Swiss agency Reporting and Analysis Centre for Information Assurance (MELANI at http://www.melani.admin.ch/index.html?lang=en) are good examples of the work being done. MELANI's January–June 2006 report addresses the international situation under the key headings of threats and risks, general trends, current lists of crimes and breakdowns, prevention software and hardware developments, current activities by international and national agencies, and legal developments. MELANI also undertakes surveys of information security among corporations and thus provides some assessment of the industry's readiness to respond the challenges of critical information infrastructure protection. The relevant Australian agencies would benefit significantly by adopting and adding value to these forms of current situational reporting.

Law enforcement will require resources for ongoing research and development in technology-enabled crime and for sharing information and intelligence between investigative, intelligence and forensic units. Such information sharing must, however, be carried out in a safe and secure manner. A responsive information distribution mechanism will be needed to enable effective responses to technology-enabled crime to be implemented in a timely manner. Harnessing open source private sector resources, such as 'Intellipedia' currently used by the United States intelligence community to disseminate and share intelligence amongst 16 United States intelligence agencies may assist. Such (confidential) information sharing channels will be the target of malicious attacks by criminals and terrorists. Information leaked from these channels could potentially result in the compromise of national security.

The role of task forces

Law enforcement agencies, particularly in ICT advanced countries, have recognised the increased interdependence of global markets and have responded to the general risks of technology-enabled crimes by establishing task forces dedicated to investigating technology-enabled crime cases. The task forces need to have adequately trained personnel capable of undertaking the operational demands of the comprehensive role envisaged by public policing agencies. The organisational capacity of law enforcement and other agencies within and across national borders to deal with increasingly complex technology-enabled crime will continue to be constrained. The use of task forces to respond to particularly complex technology-enabled crimes will continue to be beneficial, although this may have the effect of reducing resources for investigating more mundane, low-value computer crimes. The need for task forces to be established quickly also creates difficulties for investigation of new types of technology-enabled crime, where immediate response is invariably needed. Standing investigatory units may, therefore, offer greater benefits than those units convened in response to a specific identified crime.

Training and educational needs

Technological expertise, computer forensic capabilities, and sufficient investigative powers within government agencies are important. A focus on training a few experts no longer suffices: both generic and specialist training with common standards are now demanded. The need for training in technology-enabled crime legislation, particularly concerning evidence and procedure, will increase as countries enact new legislation to deal with emerging threats. In fact, it was identified that:

> [i]ncreased funding for law enforcement, including training in cyber forensics, improved vehicles for international cooperation (like the efforts in the G-8 to create national points of contact for cybercrime), and effective national laws (modeled on the Council of Europe Cybercrime Treaty) will also help narrow the opportunities for cybercriminals (McAfee 2005: 17).

Such training should be targeted towards IT professionals, legal professionals and juries, computer forensics professionals and law enforcement officers, as well as end-users and the computer-using public.

Training for information technology professionals

IT professionals are becoming more actively involved in the investigation and prosecution of technology-enabled crimes. For example, IT professionals may be called upon to help facilitate compliance with legal obligations, developing and operating secure computer systems to ensure the privacy of protected information is not compromised. Training would equip IT professionals with a working knowledge of key legal challenges and issues they are likely to encounter in the course of professional activities.

Training for legal professionals and juries

Training targeted towards lawyers, prosecutors, judges and juries involved in technology-enabled crime cases, will help them understand technical terminologies crucial to the case. Such terminology would include spyware, adware, encryption, slack space, file allocation table and date/time stamps.

> Crime involving technology is now part of everyday policing and has an effect on all types of crime. A comprehensive training program that reaches the widest audience is therefore essential … Any crime scene could be an electronic crime scene and the correct handling of this type of evidence can positively affect an investigation. However, detections, disruptions, prosecutions and crime reduction/prevention can only be achieved with properly trained personnel who are appropriately equipped to investigate the various aspects of computer-enabled criminality that they encounter in their daily duties (Jones 2005).

Training for computer forensics professionals and law enforcement officers

Developments in network vulnerabilities will require ongoing training in computer forensics. Although establishment of computer forensics accreditation programs (e.g. Certified Forensic Computer Examiner offered by the International Association of Computer Investigative Specialists) will ensure that standards of training are maintained, problems will arise in ensuring adequate staffing levels of accredited investigators. Use of private sector contractors will continue to be necessary, although risk management will be needed to ensure trained personnel do not misuse their skills for non-policing work. A recent example concerns a 'so-called' computer forensics expert hired to testify at two child pornography court cases in the United States who 'pleaded guilty to federal perjury charges for falsifying his resume and lying in open court, presumably about his credentials' (Goodin 2007b, US DoJ 2007a). The indictment alleged that '[a]t the time he worked on the child porn cases, he had already been qualified as an expert witness in computers and submitted court testimony in several jurisdictions, including federal court in California, and in courts in at least two California counties'.

Creation of resources, such as the 'Handbook of Legal Procedures of Computer and Network Misuse in European Union Countries', for police and legal practitioners will continue to be necessary. Australia is well placed to guide training in technology-enabled laws and procedures across the Asia–Pacific region, although any initiatives should be harmonised with activities in Europe and North America.

Increasingly, forensic analysis of computers for law enforcement purposes is being undertaken by well-organised groups of forensic examiners working in government facilities or private sector workplaces. Such groups include leading accounting firms such as KPMG, Deloitte, Ernst & Young and PricewaterhouseCoopers. An emerging issue is the desirability of accreditation both for individual examiners and for forensic laboratories, along with validation of forensic analysis tools. Over the next two years, developments will be needed to ensure that standards of forensic computing are being maintained nationally and internationally.

Technical assistance to less capable (or less ICT advanced) jurisdictions will also be essential as the widespread provision of training will allow the leading ICT advanced countries to manage if not prevent many of the cross-border problems (e.g. rendition of fugitives) now so evident in the delivery of phishing, denial-of-service attacks and other technology-enabled crime.

Training for end-users and the computer-using public

Although Kerr (2007) has suggested that 'user education was no longer applicable because nothing could be done to prevent infection', information security awareness training courses do help reinforce organisations' information security policies. As Rothke (2007) suggested:

> [b]y all means, we need to run the safest operating system we can, fortify our networks and police the whole thing. But once we've done all that, we're left with one unalterable fact: Users will still make errors galore. Training can help.

Information security awareness training courses inform end-users about their accountability for ensuring the integrity, confidentiality, privacy and availability of IT assets within the organisations. For example, in 2007 Microsoft investigated targeted attacks against Microsoft Word using a vulnerability in Microsoft Office 2000 and Office XP that allowed remote code execution when users opened an infected document (Microsoft TechNet 2007).

> It is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. The 'people factor' – not technology – is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this 'asset'.

> A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them (NIST 2003).

Information security awareness training courses will also equip employees with the capacity to recognise basic security breaches or threats and respond to a perceived breach or threat (e.g. to whom and how suspicious occurrences should be reported). Although there is growing awareness among end-users of the need for basic security online, constant and ongoing promotion of a culture of security for information systems and networks among end-users is essential to ensure employees (and also the public) are kept abreast of technology-enabled crime developments and how new security measures can be used to their advantage.

The 2006 AusCERT survey (AusCERT 2006) indicated that 53 percent of respondents ranked inadequate staff training and education in security practices and procedures as one of the most common weaknesses within organisations and one they believed contributed to electronic attacks. The escalating complexities of the end-user environments underline the need for continuing training requirements. The Australian Bureau of Statistics estimated that, as at 30 June 2006, approximately 43.8 percent of the population in Australia was aged 40 and above (ABS 2006b). This particular group might not be as IT literate as the younger generation and hence, might be an easier target for criminals. Constant and ongoing training programs are essential in educating this ageing population about the transnational nature of technology-enabled crime.

There is, therefore, a need for coordinated action by government agencies to ensure the most effective crime prevention advice is provided to the community. User education through dissemination of media releases by authoritative institutions, such as the Internet Crime Complaint Center, would enable users to maintain current knowledge of the latest scams and the best fraud prevention measures available.

Costs of training

The complexity of the task of providing training and educational programs in the context of the transnational nature of technology-enabled crime will continue to be challenging and costly. A survey the Computer Security Institute conducted in 2006 indicated that the reported average security awareness training expenditures per employee ranged from US$18 per employee to US$318 per employee (CSI 2006: 7). This amount is, however, insufficient particularly in light of AusCERT's survey in which 65 percent of the respondents indicated that their organisations needed to improve on the level of qualifications and training for their IT security staff (AusCERT 2006). Moreover, Gartner Research (Fiering & Kirwin

2006) pointed out that an untrained or under-trained desktop user would cost five times more to support than a well-trained worker.

Costs of training depend on various factors, such as:

- whether the training is conducted in-house or outsourced
- the media used in conducting training courses – for example:
  - web-based training that can be undertaken at the organisation's premises
  - classroom-based training courses that take the employees out of the office to outsourced trainers
  - onsite instructor-led training courses that involve no additional travelling for employees
- the type of training courses – training for key security personnel, system administrators and network administrators will be more costly than general security training for those in the organisation performing non-security specific functions (NIST 2003); for example, the cost of the 'SEC 508: System Forensics, Investigation & Response' course conducted in Brisbane on 19–23 February 2007 was approximately $3735 per trainee (SANS Institute 2007)
- opportunity costs such as lost wages and productivity when employees attend training costs
- costs for hosting onsite courses (e.g. training rooms, teleconferencing facility and computer equipment).

Policing and technology-enabled crime prevention through deterrence

Law enforcement operates at three broad levels: crime prevention, investigation and prosecution. Public agencies have a limited role in preventing technology-enabled crime. This is in part due to the design of the personal computer and the global adoption of the internet being largely in the hands of private sector forces that are less focused on security than on functionality. Thus the burden of protection against misuse of the technology has fallen to individual users. There is a flourishing industry of computer security products and services, such as antivirus software, intrusion detection devices and encryption tools, servicing the increasing desire of individuals and businesses to protect themselves against computer-related threats.

Clearly, there is limited capacity in law enforcement to investigate a high volume of technology-enabled crimes, and the future of security will remain largely with system administrators and software developers. Nonetheless, the threat of prosecution and punishment will continue to be a powerful deterrent in this environment, particularly where substantial penalties can be imposed. There will be an ongoing need for effective publicity to be given to the results of successful prosecutions, particularly in new areas of risk. The use of international task force operations should also be widely publicised as indicative of the ability of law enforcement to carry out investigations against individuals located in multiple countries.

Intelligence and the anticipation of future technology-enabled crime

Centralised sharing of information and intelligence across jurisdictional borders, both within Australia and internationally needs to be an ongoing priority. New technology-enabled crime methodologies will continue to emerge and disseminate rapidly thus requiring the immediate sharing of intelligence and newly developed response strategies. Resources also need to be allocated to mapping trends in technology-enabled crime to help anticipate new areas of risk and to determine when previous types of crimes have dissipated. One of the keys to staying abreast of the latest technologies lies in understanding both the hardware and software characteristics of the technologies in question.

Knowledge about offender and victim behaviour, as it applies in the online environment, needs to be enhanced. Some of the information gaps are being addressed but further development, based on a clear and functional classification of computer crimes, is essential. To guide training and research, a number of cross-disciplinary applied and theoretical approaches will need to be tested. Along with these essential processes must be a greater willingness to test and re-test software and hardware defences as well as the best forms of general and specific forms of public–private partnerships in preventing technology-enabled crime.

Summary

The rapid uptake of information communications technologies and its convergence with the internet poses new challenges in the formulation of policing and preventative strategies. It is also likely that the incidence of technology-enabled crime will continue to increase over the next two years, with the number of large-scale, organised attacks taking prominence.

Over the past decade, considerable progress has been made within and between countries to develop the capacity of law enforcement agencies to respond to technology-enabled crime and there is now growing awareness amongst computer users of the need for basic security online. The saying ‘think globally act locally’ is especially pertinent in the control of technology-enabled crime given that the pace of technological change will continue unabated, and cybercriminals will continue to adapt (Broadhurst 2006). As reporting of incidents increases among businesses and consumers, the capacity of law enforcement to respond in a timely manner will diminish unless additional resources are made available. The issue of retaining specialist forensic computing staff in the law enforcement sector will also continue to present a significant challenge, particularly due to the high demand for computer forensic experts in the highly paid private sector. Therefore, harnessing expertise of computer forensics in the private sector may be an important way in which the future investigatory caseload could be managed.

The key to future success in controlling technology-enabled crime is the continued development of partnerships between the various stakeholders including industry, academia, government and law enforcement.

Conclusion

As the internet and other ICT continue to advance, the risks and opportunities for criminals to commit unlawful activities will increase. It is possible to gauge the nature of such threats by examining the kind of technological developments likely to occur and associated community and social changes. With an appreciation of these developments it is possible to predict how criminals in the next two years might act.

Technology-enabled crime ranges across a wide spectrum of activities and behaviours. At one end of the spectrum are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital repositories and use of illegally obtained digital information to blackmail individuals or to extort funds from organisations. A related threat is the growing crime of identity theft. Midway along the spectrum are transaction-based crimes such as fraud, trafficking in child pornography, money laundering, and counterfeiting. Another aspect of this type of crime involves individuals within corporations or government agencies who deliberately alter data for profit, personal or political objectives. At the other end of the spectrum are crimes that involve attempts to disrupt the actual workings of the internet. These range from spamming, hacking, and denial-of-service attacks against specific sites to acts of cyber-terrorism.

Serious concerns have been expressed about the ways in which new technologies might be used for illegal enterprises. The discussion earlier in this report provides some clues to the ways in which emerging technological changes may be exploited to commit technology-enabled crime. The principal risks relate to the following areas:

- ICT take-up in developing countries, particularly in Asia, that could create an environment in which technology-enabled crime attacks on Australian organisations may emanate from or make use of security weaknesses in organisations in developing countries with which Australian organisations and individuals deal.
- New ways of exploiting advances in wireless and mobile technologies to facilitate the commission of technology-enabled crimes.
- The digitisation of information resulting in increased data holding and dissemination capabilities, new ways of accessing and sharing information, new payment methods that might facilitate crimes such as money laundering, internet-driven radicalisation and possible threats to the acquisition and preservation of digital evidence.
- Developments in government access cards and biometric passports that could be exploited by organised criminal groups that seek to compromise the underlying infrastructure, or others who seek to obtain personal information for use in identity-related crimes.
- Outsourced operations offshore that could introduce risks such as vulnerabilities in software developed offshore by corrupt offshore employees or foreign intelligence agents, and loss or misappropriation of IP.

- Computer-facilitated fraud, such as click frauds, online auction frauds, phishing and spam, targeting businesses and consumers.
- Unauthorised access to networks that makes use of advances in communications technologies to leak or to steal sensitive documents or information.
- Blended attacks and the evolution of malware, such as bot malware and zombies, kernel-mode malware, ransomware, and exploitation of internet browsers and web services. The trends in malware that can be expected to develop within the next two years are:
  - The continued development of malware such as viruses, worms and Trojans that will employ self-modifying or self-mutating code. This may allow malware to inject random pieces of code into malware automatically such as Trojan program code before compilation and compression, thus creating separate variants. Code-obfuscation may also arise in order to elude detection by antivirus and anti-malware products.
  - Continuing availability of a market for the sale of malware such as password stealers (e.g. W32/Fujacks) and related Trojans and file infectors, such as password-stealing websites using fake sign-in pages.
  - Other stealth techniques to hide files, processes or registry values belonging to the malware such as installation of Application Program Interface that hooks into running processes or changes system Application Program Interfaces.
- Infringement of IP rights including illegal transfer of technology to other countries and companies.
- Industrial espionage facilitated by enhanced reverse engineering, electronic surveillance and data capture technologies and by exploiting commercial joint venture and offshore outsourcing relationships.
- Child exploitation and offensive content-related crimes using affordable technology (e.g. web cameras and powerful editing multimedia software).
- Exploitation of younger persons to facilitate crimes such as identity theft, extortion, online scams and cyberbullying.
- Transnational organised crime and terrorism perpetrated with the aid of computers and computer networks.
- Threats to Australia's national information infrastructure perpetuated with the aid of advances in internet and other technologies, such as geospatial technologies. Tight couplings between different areas of critical infrastructure may also result in rapid escalation of seemingly modest disruptions within one sector to others.

- Displacement risks such as the transition from white collar crime to violent crime in situations where user authentication is undertaken with biometrics that can only be compromised through duress or threats of violence to users.

The pace of technological change, the rapid uptake of ICT and their convergence with the internet are such that law and policy are required to be continually monitored and adapted. A multi-dimensional response to technology-enabled crime, as recommended in the chapter on Legal and evidentiary implications, is likely to offer the greatest benefits focusing on effective coordination and collaborative activities between public and private sector agencies and organisations.

The following recommendations on possible policing and preventative strategies were presented in the previous chapter:

- engaging the ICT security industry in the design of secure software and hardware components
- establishing public–private sector partnerships and information sharing initiatives
- establishing task forces dedicated to investigating and prosecuting technology-enabled crime cases
- enhancing the training and educational capabilities of law enforcement, prosecutors, judges, and IT professionals. Technical assistance to less capable, or less ICT advanced, jurisdictions will also be essential as the widespread provision of training will allow the leading ICT advanced countries to manage if not prevent many of the cross-border problems
- policing and technology-enabled crime prevention through deterrence
- developing intelligence and anticipating future technology-enabled crime.

Although technology has the potential to spur economic growth, it can also retard development through creation of crime risks. The evolution of problems and challenges resulting from technology-enabled crime is likely to expand in the immediate future, creating a need for a comprehensive strategy based on sound evidence-based policy. There is no single all-encompassing answer to technology-enabled crime. Countering the risks is a multi-dimensional challenge and requires effective coordination and collaborative efforts on the part of a wide range of government and private sector entities. Possible directions for action include:

- the engagement of the ICT security industry in the design of secure software and hardware
- the creation of public–private sector partnerships and information sharing initiatives
- the establishment of task forces dedicated to the investigation and prosecution of technology-enabled crime cases
- the enhancement of training and educational capabilities of police, prosecutors, judges and IT professionals.

Technical assistance to less capable or less ICT-advanced jurisdictions will also be essential as the widespread provision of training will allow leading ICT-advanced countries to manage if not to prevent many cross-border problems from emerging.

Only three years ago Smith et al. (2004: 156) observed when discussing crime in the digital environment that ‘those who fail to anticipate the future are in for a rude shock when it arrives’. Hopefully, the present report will be of assistance in preventing such a situation from arising over the next two years.

References

References

All URLs were correct on 18 May 2007

Aboud J, Lyndon J & Yaneza M 2006. Spy-phishing: a new breed of blended threats. Paper to Virus Bulletin Conference, Montreal, 2006.
http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/spyphishing_102006.pdf

Ahmad R 2007. Slashing through the Web of terror. *Todayonline* 3 March.
http://www.todayonline.com/articles/175137.asp

Ames B 2007. Online spending tops US$100 billion. *Computerworld.com* 5 January.
http://www.computerworld.com.au/index.php?id=732481904&eid=-180

AOL/NCSA 2005. Online safety study. December.
http://www.staysafeonline.info/pdf/safety_study_2005.pdf

Arbor Networks 2006. *Worldwide infrastructure security report*.
http://www.arbornetworks.com/sp_security_report.php

Associated Press (AP) 2007. China cracks down on 'virtual money'. *Sydney morning herald* 8 March.
http://www.smh.com.au/news/games/china-cracks-down-on-virtual-money/2007/03/08/1173166819859.html

Associated Press (AP) 2006. China's internet population boom. *Sydney morning herald* 31 December.
http://www.smh.com.au/news/web/chinas-internet-population-boom/2006/12/29/1166895509752.html

Association of Banks in Singapore 2007. Singapore banks join global battle against child pornography. *Media release* 17 January.
http://www.abs.org.sg/pdf_files/Final%20Media%20Release%20on%20Singapore%20Banks'%20Battle%20Against%20Child%20Pornography.pdf

AusCERT 2006. *Computer crime and security survey*.
http://www.auscert.org.au/images/ACCSS2006.pdf

Australia. Attorney-General's Department (AGD) 2006. Water industry risk context statement. March.
http://pandora.nla.gov.au/pan/39423/20070416/www.ag.gov.au/agd/www/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)_water.pdf/$file/water.pdf

Australia. Commonwealth Director of Public Prosecutions 2006. *2005–2006 Annual report*.
http://www.cdpp.gov.au/AboutUs/AnnualReports/

Australia. Department of Communications, Information Technology, and the Arts (DCITA) 2005. *Outcome of the review of the legislative framework on spyware.*
http://www.dcita.gov.au/communications_for_consumers/security/spyware/outcome_of_review

Australian Associated Press (AAP) 2007a. Smartcard not ID card: minister. *Sydney morning herald* 7 February. http://www.smh.com.au/news/national/smartcard-not-id-card-minister/2007/02/07/1170524137064.html

Australian Associated Press (AAP) 2007b. Sweden plans embassy in Second Life. *Sydney morning herald* 29 January http://www.smh.com.au/news/games/sweden-plans-embassy-in-second-life/2007/01/27/1169788744103.html

Australian Associated Press (AAP) 2007c. Swiss authorities raise porn alarm. *News.com.au* 22 January. http://www.news.com.au/story/0,10117,21100393-1243,00.html?from=public_rss

Australian Associated Press (AAP) 2006. Man jailed in landmark internet sex case. *Sydney morning herald* 21 June. http://www.smh.com.au/news/technology/man-jailed-in-landmark-internet-sex-case/2006/07/21/1153166569887.html

Australian Bureau of Statistics (ABS) 2005. *Internet activity*. ABS cat. no. 8153.0. http://www.abs.gov.au/ausstats/abs@.nsf/cat/8153.0

Australian Bureau of Statistics (ABS) 2006a. *Australian economic indicators*. ABS cat. no. 1350.0. http://www.abs.gov.au/ausstats/abs@.nsf/cat/1350.0

Australian Bureau of Statistics (ABS) 2006b. *Population by age and sex, Australian states and territories*. ABS cat. no. 3201.0. http://www.abs.gov.au/ausstats/abs@.nsf/cat/3201.0

Australian Broadcasting Corporation (ABC) 2006. Centrelink staff sacked for privacy breaches. *ABC.net.au* 23 August. http://www.abc.net.au/news/newsitems/200608/s1721505.htm

Australian Broadcasting Corporation (ABC) 2007a. Man jailed for Open ‘upskirting’. *ABC.net* 25 January. http://www.abc.net.au/news/items/200701/1833683.htm?victoria

Australian Broadcasting Corporation (ABC) 2007b. Ex-policeman gets suspended sentence for info breaches. *ABC.net* 9 February. http://www.abc.net.au/news/items/200702/1844467.htm?wa

Australian Communications and Media Authority (ACMA) 2006. Research shows rapid uptake in free-to-air digital television. *Media release* MR 146/2006 23 November. http://www.acma.gov.au/ACMAINTER.1572992:STANDARD::pc=PC_100962

Australian Communications and Media Authority (ACMA) 2005. Racing tips company fined for breach of Spam Act. *Media release* 17 August.
http://www.acma.gov.au/WEB/STANDARD//pc=PC_100121

Australian High Tech Crime Centre (AHTCC) 2006. International internet investigation nets arrest. *Media release* 22 March.
http://www.ahtcc.gov.au/__data/assets/pdf_file/7961/nat_060322internetarrest.pdf

Australian Institute of Criminology (AIC) 2007a. New methods of transferring value electronically. *High tech crime brief* 14.
http://www.aic.gov.au/publications/htcb/htcb014.html

Australian Institute of Criminology (AIC) 2007b. Underground markets in stolen digital information. *Crime facts info* 148.
http://www.aic.gov.au/publications/cfi/cfi148.html

Australian Payments Clearing Association (APCA) 2005. *Annual report 2005*.
http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/PUB_AnnualReport

Australian Law Reform Commission (ALRC) 2006. *Review of privacy*. Issues paper 31.
http://www.austlii.edu.au/au/other/alrc/publications/issues/31/

Baker J 2007. YouTube led police to suspects. *Sydney morning herald* 7 February.
http://www.smh.com.au/news/technology/youtube-led-police-to-suspects/2007/02/06/1170524096380.html

Bandura A 1999. Social cognitive theory of personality. *Asian journal of social psychology* 2(1): 21–41

Berkman O & Ostrovsky OM 2006. *The unbearable lightness of PIN cracking*.
http://www.arx.com/documents/The_Unbearable_Lightness_of_PIN_Cracking.pdf

BlackHat 2003. *BlackHat briefings*.
http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-hackercourt.pdf

Business Software Alliance 2007. *Fourth annual BSA and IDC global software piracy study*.
http://www.bsa.org/customcf/popuphitbox.cfm?doc_url=http://www.bsa.org/globalstudy/upload/2007-Global-Piracy-Study-EN.pdf

Burns S 2006. Korea to ban online game currency trading. *PCauthority.com.au* 27 November.
http://www.pcauthority.com.au/news.aspx?CIaNID=42740

Broadhurst R 2006. Developments in the global law enforcement of cyber-crime. *International journal of police strategies & management* 29(3): 408–433

Broadhurst R & Chantler C 2006. Cybercrime update: trends and developments.
Draft submission to the UNODC expert group meeting on the virtual forum against cybercrime. Brisbane: Queensland University of Technology.
http://eprints.qut.edu.au/archive/00004690/01/4690.pdf

Broersma M 2007a. IDefense puts up $50,000 for Microsoft bugs.
Computerworld.com 12 January.
http://www.computerworld.com.au/index.php?id=1678507864&eid=-180

Broersma M 2007b. Spam shows sudden slide. *Computerworld.com* 10 January.
http://www.computerworld.com.au/index.php?id=1059931122&eid=-255

Cappelli D et al. 2006. *Common sense guide to prevention and detection of insider threats*.
http://www.us-cert.gov/reading_room/prevent_detect_insiderthreat0504.pdf

Casey E 2002. Error, uncertainty, and loss in digital evidence.
International journal of digital evidence 1(2).
http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf

Chau M & Xu J 2007. Mining communities and their relationships in blogs: A study of online hate groups. *International journal of human-computer studies* 65(1): 57–70

Chaum D 1982. Blind signatures for untraceable payments, in *Advances in cryptology: proceedings of CRYPTO 82*. New York NY: Plenum Press, 199–203

Chen YC et al. 2004. Online gaming crime and security issue: cases and countermeasures from Taiwan. Paper to Second Annual Conference on Privacy, Security and Trust, University of New Brunswick, October 2004.
http://dev.hil.unb.ca/Texts/PST/pdf/chen.pdf

China tops 20m bloggers 2007. *AustralianIT* 12 January.
http://australianit.news.com.au/articles/
0,7204,21047806%5E15322%5E%5Enbv%5E15306,00.html

Choo KKR 2006. Issue report on business adoption of Microsoft Passport.
Information management & computer security 14(3): 218–234

Choo KKR 2007. Zombies and botnets. *Trends & issues in crime and criminal justice* no. 333.
http://www.aic.gov.au/publications/tandi2/tandi333.html

Cisco Systems 2007. Cisco security advisory: multiple vulnerabilities in the IOS FTP server.
Media release 9 May.
http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml

Clark JA 2002. *Pervasive computing: sensors galore, information warfare and death in IKEA*. York: University of York, Department of Computer Science. http://www-users.cs.york.ac.uk/~jac/PublishedPapers/Presentations/PervasiveYork.ppt

Clark W 2006. *Definition of mobile workforce*. Stamford CT: Gartner

Coates J 1998. *21st century technologies: promises and perils of a dynamic future*. Paris: OECD

Colwill C & Gray A 2007. Creating an effective security risk model for outsourcing decisions. *BT technology journal* 25(1): 79–87

Computer Security Institute (CSI) 2006. *2006 CSI/FBI computer crime and security survey*. http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf

Conroy V 2006. *UK leads Europe in e-payments*. London: Electronic Payments International

Cooke E, Jahanian F & McPherson D 2005. The zombie roundup: understanding, detecting, and disrupting botnets, in *Proceedings of SRUTI 2005*. Berkeley CA: USENIX Association: 35–44

Council of Europe 2004. *Organised crime situation report 2004: focus on the threat of cybercrime* http://www.coe.int/T/E/Legal_Affairs/Legal_co-operation/Combating_economic_crime/8_Organised_crime/Documents/Organised%20Crime%20Situation%20Report%202004.pdf

Crandall J et al. 2006. Temporal search: detecting hidden malware timebombs with virtual machines, in Mukherjee S & McKinley KS (eds), Proceedings of the 11th International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS 2004, Boston, MA, USA, October 7–13, 2004. New York NY: ACM 2004: 25–36

Crawford M & Pauli D 2006. Industry act to contain offshore scandal. *Computerworld.com* 16 October. http://www.computerworld.com.au/index.php?id=1135495204&eid=-257

Dao C 2007. 8 arrests in computer virus case. *China daily*. 13 February. http://www.chinadaily.com.cn/china/2007-02/13/content_807823.htm

Davis R & Pease K 2000. Crime, technology and the future. *Security journal* 13(2): 59

De Wilde F 2006. Courtroom technology in Australian courts: an exploration into its availability, use and acceptance. *Queensland lawyer* 26: 303–328

Deloitte Touche Tohmatsu 2006. *Eye to the future: how TMT advances could change the way we live in 2010*. http://www.deloitte.com/dtt/cda/doc/content/UK_TMT_Eyetothefuture_06.pdf

De Young R 2001. The internet's place in the banking industry. *Chicago Fed letter* no. 163. http://www.chicagofed.org/publications/fedletter/2001/cflmar2001_163.pdf

Dhamija R, Tygar JD & Hearst M 2006. *Why phishing works*.
http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf#search=%22why%20phising%20works%22

Di Paola S & Fedon G 2006. *Subverting AJAX: next generation vulnerabilities in 2.0 web applications*.
http://events.ccc.de/congress/2006/Fahrplan/events/1602.en.html

Dulaney K & Hafner B 2006. *Predicts 2007: Mobile devices and applications reflect key changes at work and home*. Stamford CT: Gartner

Dunn JE 2007. Malware now hiding in search results. *Computerworld.com* 11 January.
http://www.computerworld.com.au/index.php?id=1543993617&eid=-255

Duo charged in credit card fraud scam 2006. *North country gazette* 1 November.
http://www.northcountrygazette.org/articles/110106CreditCardFraud.html

Early Warning Services 2006. Financial services industry leaders join together to fight fraud. *Media release* 22 May.
http://www.early-warning.com/news/financial_services_industry_leaders_join_together_to_fight_fraud.asp

eBay 2006. *2005 Annual report*.
http://investor.ebay.com/annuals.cfm

Economist Intelligence Unit 2006. *The 2006 e-readiness rankings*.
http://graphics.eiu.com/files/ad_pdfs/2006Ereadiness_Ranking_WP.pdf

Electronic Frontier Foundation (EFF) 2007. Surveillance of soldiers' blogs sparks EFF lawsuit. *Media release* 31 January.
http://www.eff.org/news/archives/2007_01.php#005103

Erber G & Sayed-Ahmed A 2006. Offshore outsourcing. *Intereconomics* 40(2): 100–112

Ernst and Young 2006. Global information security survey 2006. *Media release*.
http://www.ey.com/Global/download.nsf/International/TSRS_-_GISS_2006/$file/EY_GISS2006.pdf

Ernst and Young 2005. Global information security survey 2005. *Media release*.
http://www.ey.com/global/content.nsf/International/Press_Release_-_2005_Global_Information_Security_Survey

Evers J & McCullagh D 2006. Researchers: e-passports pose security risk. *CNET News.com* 5 August.
http://news.com.com/Researchers+E-passports+pose+security+risk/2100-7349_3-6102608.html

FBI 2007a. Cracking the code: Online IP theft is not a game. *Media release* 1 February.
http://www.fbi.gov/page2/feb07/iptheft020107.htm

FBI 2007b. Los Angeles task force announces arrests involving federal charges of possession and distribution of child pornography and state charges of child molestation; public's help sought in identifying victims. *Media release* 12 January.
http://losangeles.fbi.gov/pressrel/2007/la011207.htm

FBI 2007c. Santa Clarita man indicted today for using internet to entice minor into sex. *Media release* 3 January.
http://losangeles.fbi.gov/pressrel/2007/la010307.htm

FBI 2006a. FBI cyber action teams: Traveling the world to catch cyber criminals. *Media release* 6 March.
http://www.fbi.gov/page2/march06/cats030606.htm

FBI 2006b. Lebanese credit card fraudster sentenced to four years in prison. *Media release* n.d.
http://losangeles.fbi.gov/dojpressrel/pressrel06/la092606usa.htm

FBI 2006c. Romanian nationals indicted for running internet scam that purported to benefit hurricane Katrina victims. *Media release* 6 October.
http://www.usdoj.gov/katrina/Katrina_Fraud/pr/press_releases/2006/oct/10-06-06tworomaniansindict.pdf

FBI 2006d. San Diego computer expert pleads guilty to hacking into USC computer system containing student applications. *Media release* 5 September.
http://losangeles.fbi.gov/dojpressrel/pressrel06/la090506usa.htm

Ferguson G 2007. Persistent and pervasive terrorism threat. *Australian national security magazine* February: 10–12

Fiering L & Kirwin B 2006. Untrained users cost more to support than trained users. Stamford CT: Gartner

Financial Action Task Force (FATF) 2006. *Report on new payment methods.* FATF Publication 13.
http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf

Federal Reserve System (FRS) 2004. *The 2004 federal reserve payments study*.
http://www.frbservices.org/Retail/pdf/2004PaymentResearchReport.pdf

Fortinet 2007. *Malicious code appears on Blogger.com*.
http://www.fortiguardcenter.com/advisory/FGA-2007-04.html

Gallaire H 1998. Faster, connected, smarter, in OECD, *21st century technologies: promises and perils of a dynamic future*. Paris: OECD 47–76

Gaudin S 2007. Second hack at university exposes info on 22,000 students. *InformationWeek* 9 May. http://www.informationweek.com/security/showArticle.jhtml;jsessionid=RGMTGULHG3PDGQSNDLPCKHSCJUNN2JVN?articleID=199500214&articleID=199500214

Gibson J & Creagh S 2007. Student confirms school link in race hate video on internet. *Sydney morning herald* 25 January. http://www.smh.com.au/news/national/student-confirms-school-link-in-race-hate-video-on-internet/2007/01/24/1169594362334.html

Glenbrook Partners 2006. Visa launches mobile Visa wave payment pilot in Malaysia. *PaymentsNews.com* 27 April. http://www.paymentsnews.com/2006/04/visa_launches_m.html

Global Reach 2007. *Global internet statistics (by language)*. http://www.glreach.com/globstats/index.php3

Gohring N 2006. Mobiles offer more than voice in developing markets. *Computerworld mobile and wireless.com* 13 December. http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005994

Goodin D 2007a. DDoSers bombard military root server (and more). *The register.com* 7 February. http://www.theregister.co.uk/2007/02/07/root_server_attack/

Goodin D 2007b. Man faces 10 years for fudging computer credentials. *The register.com* 9 May. http://www.theregister.co.uk/2007/05/09/computer_expert_pleads_guilty/

Goodin D 2007c. Six individuals suspected of using stolen TJX data. *The register.com* 21 March. http://www.theregister.co.uk/2007/03/21/tjx_info_arrests/

Gorbis M & Pescovitz D 2006. *Bursting tech bubbles before they balloon.* Institute for the Future/IEEE Spectrum future of science and technology survey. http://www.spectrum.ieee.org/print/4435

Grabosky & Smith 1998. *Crime in the digital age: controlling telecommunication and cyberspace illegalities*. New Brunswick NJ: Transaction Publishers

Great Britain. Crown Prosecution Service (GB CPS) 2006. Convictions for internet rape plan. *Media release* 1 December. http://www.cps.gov.uk/news/pressreleases/archive/2006/170_06.html

Greenleaf G 2007. Australia's proposed ID card: Still quacking like a duck. *Computer law & security report* 23(2): 156–66

Guardian News & Media 2007. Txt banking now a reality. *Sydney morning herald* 24 March. http://www.smh.com.au/news/technology/txt-banking-has-become-a-reality/2007/03/23/1174597882204.html

Gutberlet M 2006. *Mobile carriers should embrace internet-based instant messaging services*. Stamford CT: Gartner

Halderman JA & Felten EW 2006. Lessons from the Sony CD DRM Episode, in *Proceedings of 15th USENIX Security Symposium*. Berkeley CA: Usenix: 77–92

Harding T 2007. Terrorists 'use Google maps to hit UK troops'. *Telegraph.co.uk* 13 January. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/01/13/wgoogle13.xml

Harrington S 1996. The effects of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS quarterly* 20(3): 257–77

Harris R 2006. Arriving at an anti-forensics consensus: examining how to define and control the anti- forensics problem. *Digital investigations* 3(1): 44–49

Hart C 2007. Access Card scheme stalls. *Australian* 16 March. http://theaustralian.news.com.au/story/0,20867,21390636-2702,00.html?from=public_rss

Heydt-Benjamin TS et al. 2007. Vulnerabilities in first-generation RFID-enabled credit cards, in Proceedings of Financial Cryptography and Data Security 2007 *Lecture notes in computer science* (forthcoming).
http://www.cs.umass.edu/~tshb/FC07-heydt-benjamin.pdf

Hinchcliffe D 2006. Enterprise 2.0: ten predictions for 2007. *ZDNet* 27 December. http://blogs.zdnet.com/Hinchcliffe/?p=76

Hoare D 2006. Internet predator jailed under new laws. *ABC.net.au* 21 July. http://www.abc.net.au/pm/content/2006/s1693718.htm

Hoecht A & Trott P 2006. Outsourcing, information leakage and the risk of losing technology-based competencies. *European business review* 18(5): 395–412

Hutcheon S 2006. Second Life miscreants stage members-only attack. *Sydney morning herald* 21 December.
http://www.smh.com.au/news/web/second-life-miscreants-stage-membersonly-raid/2006/12/21/1166290662836.html

IBM 2007. IBM X-Force 2006 trend statistics report. IBM report, January. http://www.iss.net/documents/whitepapers/X_Force_Exec_Brief.pdf

IBM 2006a. IBM B2B Security Survey 2006. *Media release* 13 March. http://www-03.ibm.com/press/it/it/newsarticle/19373.wss

IBM 2006b. Surge in criminal-driven cyber attacks anticipated in 2006. *Media release* 23 January. http://www-03.ibm.com/industries/financialservices/doc/content/news/pressrelease/1500860103.html

IEEE 2006. News brief. *IEEE computer* 39(10): 26

International Intellectual Property Alliance (IIPA) 2007. *Copyright industries in the United States economy: the 2006 report*. http://www.iipa.com/pdf/2006SiwekSummary.pdf

Inter-Ministry Committee on Youth Crime (IMCYC) 2005. Game over. *Straits times* 11 February. H1

Internet Systems Consortium 2006. *ISC domain survey: number of internet hosts*. http://www.isc.org/index.pl?/ops/ds/host-count-history.php

Internet World Stats 2006. *Internet usage statistics: the big picture*. http://www.internetworldstats.com/stats.htm

Isobar & Yahoo 2006. *Fluid-lives highlights 2006*. http://www.fluid-lives.com/docs/fluid_lives_highlights.pdf

Jaques R 2006. Huge botnet swamps UK firms with 8 million phishing emails. *vnunet.com* 2 August. http://www.vnunet.com/vnunet/news/2161530/huge-botnet-swamps-uk-firms

Jagatic T et al. 2007. Social phishing. Communications of the ACM (forthcoming). http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

Jakobsson M & Stamm S 2006. Invasive browser sniffing and countermeasures, in *Proceedings of the 15th international Conference on World Wide Web, Edinburgh, 2006.* http://www2006.org/programme/item.php?id=3527

James NJ 2004. Handing over the keys: contingency, power and resistance in the context of section 3LA of the Australian Crimes Act 1914. *University of Queensland law journal* 23(1): 7–21

Jones N 2005. U.K. police plug in to high-tech know-how. *Royal Canadian Mounted Police gazette*. http://www.gazette.rcmp.gc.ca/article-en.html?&lang_id=1&article_id=152

Jones N 2006. *Europeans expect mobile technology to facilitate collaboration in 2009*. Stamford CT: Gartner

Josse M 2006. Prevalence of PE packers in email traffic, in Digital security: prevention to prosecution: *proceedings of AVAR 2006*: 168–91 [CD-ROM]

Kasslin K 2006. Kernel malware: The attack from within, in Digital security: prevention to prosecution: *proceedings of AVAR 2006*: 144–59 [CD-ROM]

Keizer G 2006. Newest ransomware threat: buy drugs or else. *ITNews.com.au* 2 June. http://www.itnews.com.au/newsstory.aspx?CIaNID=33259&eid=3&edate=20060602

Kennedy G & Clark D 2006. Outsourcing to China: risks and benefits. *Computer law & security report* 22(3): 250–53

Kerr J 2007. Cyber crime battle. *Australian national security magazine* February: 21–23

Kesar S & Rogerson S 1998. Developing ethical practices to minimize computer misuse. *Social science computer review* 16(3): 240–51

Kirk J 2007. Estonia recovers from massive denial-of-service attack. *InfoWorld* 17 May. http://www.infoworld.com/article/07/05/17/estonia-denial-of-service-attack_1.html

Knight W 2006. Click fraud is just another business tax. *Infosecurity today* 3(6): 29–31

Krebs B 2007. Super bowl site trojan aims to nab passwords. *Washingtonpost.com* 2 February. http://blog.washingtonpost.com/securityfix/2007/02/official_superbowl_site_pushin.html?nav=rss_blog

Lawton G 2006. Working today on tomorrow's storage technology. *IEEE computer* 39(12): 19–22

Lemos R 2007a. Fraud linked to TJX data heist spreads. *The register* 29 January. http://www.theregister.co.uk/2007/01/29/tjx_data_fraud/

Lemos R 2007b. Imperfect Storm aids spammers. *The register* 19 February. http://www.theregister.co.uk/2007/02/19/storm_worm_stockpatrol/

Lemos R 2005. Zotob suspects arrested in Turkey and Morocco. *SecurityFocus* 26 August. http://www.securityfocus.com/news/11297

Lemos R 2004. Alarm growing over bot software. *News.com* 30 April. http://news.com.com/2100-7349_3-5202236.html

Leyden J 2006a. Chinese crackers attack US.gov. *The register* 9 October. http://www.theregister.co.uk/2006/10/09/chinese_crackers_attack_us/

Leyden J 2006b. Wikipedia Blaster 'fix' points to malware. *The register* 3 November. http://www.theregister.co.uk/2006/11/03/wikipedia_blaster_attack/

Linton J 2006. BPL trial at Mt Beauty. *Amateur radio magazine* December: 22–24

Lyman P & Varian HR 2003. *How much information 2003*?
http://www.sims.berkeley.edu/how-much-info-2003

Marks P 2007. How to leak a secret and not get caught. *New scientist* 2586: 13

Mathieson SA 2006. Hot stocks to your inbox. *Infosecurity today*, September/October: 10–13

McAfee 2007. Backdoor-DKT. Alert, 2 February.
http://vil.nai.com/vil/content/v_141405.htm

McAfee 2006. *McAfee virtual criminology report 2006*. Santa Clara CA: McAfee

McAfee 2005. *McAfee virtual criminology report 2005*. Santa Clara CA: McAfee

McDougall P 2004. There's no stopping the offshore-outsourcing train. *Information week* 24 May.
http://www.informationweek.com/story/showArticle.jhtml?articleID=20900333

McKewan A 2006. Botnets: zombies get smarter. *Network security* 2006(6): 18–20

McMillan R 2007a. Hackers slow Internet root servers with attack. *Computerworld* 7 February.
http://www.computerworld.com.au/index.php?id=1160081859&eid=-6787

McMillan R 2007b. NSA helped Microsoft make Vista secure. CSO 10 January.
http://www.csoonline.com.au/index.php?id=2112787630&eid=-302

Me G & Verdone D 2006. An overview of some techniques to exploit VoIP over WLAN, in *Proceedings of IEEE ICDT 2006*. Washington DC: IEEE: 67

Microsoft TechNet 2007. Vulnerability in Microsoft Word could allow remote code execution. 14 February. *Microsoft security advisory*.
http://www.microsoft.com/technet/security/advisory/933052.mspx

Milburn R 2006. Will IT automate the financial supply chain? *Computerworld* 21 September.
http://www.computerworld.com.au/index.php/id;386241730

Miller R, Michalski W & Stevens B 1998. The promises and perils of 21st century technology: an overview of the issues, in OECD, *21st century technologies: promises and perils of a dynamic future*.
http://www.oecd.org/dataoecd/41/16/35391210.pdf

Millman R 2005. IT managers fail to protect mobile devices. *SC magazine*, 11 November.
http://www.scmagazine.com/asia/news/article/527520/it-managers-fail-protect-mobile-devices/

Mitchell KJ, Wolak J & Finkelhor D 2005. Police posing as juveniles online to catch sex offenders: is it working? *Sexual abuse* 17(3): 241–67

Mobile Payments World 2007a. M-banking gains traction in Latin America. *Mobile payments world* 93: 9

Mobile Payments World 2007b. Spending to reach $800m. *Mobile payments world 92*: 7

Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General 2007. *Discussion paper: identity crime*. http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf/$file/MCLOC-draft-identity-crime-discussion-paper-march+2007.pdf

Montalbano E 2006. Google faces another click-fraud suit. *Computerworld.com* 18 August. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9002585&source=rss_news50

Moore GE 1965. Cramming more components onto integrated circuits. *Electronics* 38(8): 114–117

Moore GE 1998. Cramming more components onto integrated circuits. *Proceedings of the IEEE* 86(1): 82–85.

Morris S 2004. *The future of netcrime now: part 1: threats and challenges*. Home Office online report 62/04. http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf

Mulliner C & Vigna G 2006. Vulnerability analysis of MMS user agents, in *Proceedings of IEEE ACSAC 2006*. Washington DC: IEEE: 77–88

Nakamura A 2004. Killing stokes fears over impact of net. *Japan times online* 5 June. http://search.japantimes.co.jp/cgi-bin/nn20040605a5.html

Nasheri H 2005. *Economic espionage and industrial spying*. Cambridge: Cambridge University Press

National Crime Prevention Council 2007. *Teens and cyberbullying*. http://vocuspr.vocus.com/VocusPR30/Temp/Sites/2623/57d586957e1d404ca0f0d5f6d0b18996/Cyberbullying-Exec%20Summary-FINAL.doc

National Cyber Security Alliance and Bank of America 2006. *Online fraud report: technical report*. http://www.staysafeonline.info/news/onlinefraudreportfinal.pdf

National Institute of Standards and Technology (NIST) 2006a. *Guide to computer security log management*. NIST computer security special publications SP800-92. Gaithersburg MD: NIST

National Institute of Standards and Technology (NIST) 2006b. *Guide to IEEE 802.11i: robust security networks.* NIST computer security draft special publication 800–97. Gaithersburg MD: NIST

National Institute of Standards and Technology (NIST) 2006c. *Guide to integrating forensic techniques into incident response*. NIST computer security special publications SP800-86. Gaithersburg MD: NIST

National Institute of Standards and Technology (NIST) 2003. *Building an information technology security awareness and training program*. NIST computer security publications SP800-50. Gaithersburg MD: NIST

National White Collar Crime Center and Federal Bureau of Investigation (NW3C/FBI) 2006. *2005 internet fraud crime report*.
http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf

National Science and Technology Council 2000. *National Nanotechnology Initiative: the initiative and its implementation plan*.
http://www.nano.gov/html/res/nni2.pdf

Naylor RT 2000. *Expert panel on emerging crimes*. Ottawa ON: Research and Statistics Division, Department of Justice.
http://www.justice.gc.ca/en/ps/rs/rep/2002/expertpanel.pdf

Newton EM & Lawrence Pfleeger S 2006. Information technology trends to 2020, in Silberglitt R et al. *The global technology revolution 2020: in-depth analyses*. Santa Monica CA: RAND: Appendix D.
http://www.rand.org/pubs/technical_reports/2006/RAND_TR303.pdf

Ng A 2007. Illegal wireless-network user sentenced to 18 months' probation. *Todayonline* 17 January.
http://www.todayonline.com/articles/166274.asp

Niccolai J 2007. Google nets search deal with China Mobile. *Computerworld* 5 January.
http://www.computerworld.com.au/index.php?id=2135592482&eid=-180

Optus to pour $800m into 3G network 2007. *Computer world magazine* 7 February: 8

OUT-LAW 2006. Google settles click fraud case for $90 million. News 31 July.
http://www.out-law.com/page-7150

OUT-LAW 2005. Denial. *OUT-LAW magazine* 12:10–12

Organisation for Economic Co-Operation and Development (OECD) 2006. Protecting consumers from cyberfraud. *Policy brief* October.
http://www.oecd.org/dataoecd/4/9/37577658.pdf

Ortega B 2006. NewsBrief. *IEEE Security & Privacy* 4(6): 6

Ortiz Jr S 2006. How secure is RFID? *IEEE computer* 39(7): 17–19

Palmers C 2007. Policing a virtual world. *Anti-money laundering magazine* 7:25–27

Parker J 2007. Myspace use comes with risks. *United States Air Force leader* 29(2): 18

Peron C & Legary M 2005. Digital anti-forensics: emerging trends in data transformation techniques, in *Proceedings of 2005 E-Crime and Computer Evidence Conference*. http://www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf

Perez JC 2007. NY teen hacks AOL, infects systems. *InfoWorld* 20 April. http://www.infoworld.com/article/07/04/26/HNteenhackaol_1.html

Power R & Forte D 2006. Thwart the insider threat: a proactive approach to personnel security. *Computer fraud & security* 2006(7): 10–15

PricewaterhouseCoopers (PwC) 2006. *DTI information security breaches survey 2006*. http://www.pwc.com/extweb/pwcpublications.nsf/docid/7FA80D2B30A116D7802570B9005C3D16

Quelin B & Duhamel F 2003. Bringing together strategic outsourcing and corporate strategy: outsourcing motives and risks. *European management journal* 21(5): 647–61

Quimbo R 2006. Cyber-crime and security policy issues. Paper to Workshops on Capacity Building in Public Policy Issues of Internet Use for Business Development in Asia and the Pacific. http://www.apdip.net/news/ESCAP-iGovSME-Workshop-Security.pdf

Reinventing the internet 2006. *Economist technology quarterly*. 11 March

Reuters 2007. Gates predicts internet will revolutionise TV. *Sydney morning herald* 29 January. http://www.smh.com.au/news/technology/gates-predicts-internet-will-revolutionise-tv/2007/01/29/1169919268351.html

Rieback M et al. 2006. RFID malware: design principles and examples. *Pervasive and mobile computing* 2(4): 405–26

Ropelato J 2007. Internet pornography statistics. *Internet filter review*. http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

Rosenbloom A 2004. The blogosphere. *Communications of the ACM* 47(12): 31–33

Rossi S 2007. 5000 discs seized in antipiracy sting. *Computerworld.com* 10 May. http://computerworld.idg.com.au/index.php?id=1473808560

Rothke B 2007. Security isn't just avoiding Microsoft. *Computerworld.com* 7 May. http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=291226

RSA Security 2007. New universal man-in-the-middle phishing kit discovered. *Media release* 10 January.
http://www.rsasecurity.com/press_release.asp?doc_id=7667

Rubin A 2005. Security and privacy in computing project [online assignment]. Johns Hopkins University Department of Computer Science.
http://www.cs.jhu.edu/~rubin/courses/sp05/assignment.2.txt

Rutkowska J 2006. Subverting Vista kernel for fun and profit. Paper to Black Hat USA 2006 conference, Las Vegas

Ryan E 2006. Mobile porn market set to explode. *The register* 28 November.
http://www.theregister.co.uk/2006/11/28/mobile_porn_to_increase/

SANS Institute 2007. SANS Brisbane 2007 [conference notice].
http://www.sans.org/brisbane07/description.php?tid=692&portal=355a20d907c8360583bb00a8e251ed6b

Schaffer GP 2006. Worms and viruses and botnets, oh my! *IEEE security & privacy* 4(3): 52–58

Schipka M 2006. Prevalence of PE packers in email traffic, in *Proceedings of AVAR 2006*: 44–53 [CD-ROM]

Schram J, Bulliet B & Gittens S 2007. Teen in AOL ‘hack attack’. *New York post* 26 April.
http://www.nypost.com/seven/04262007/news/regionalnews/teen_in_aol_hack_attack_regionalnews_jamie_schram_______mark_bulliet_and______hasani_gittens.htm

Seger A 2005. A letter from the Council of Europe: cybercrime and organised crime. *Crime prevention and community safety* 7(4): 59–64

Shrader K 2006. Over 3,600 intelligence professionals tapping into ‘Intellipedia’. *USA today* 2 November.
http://www.usatoday.com/tech/news/techinnovations/2006-11-02-intellipedia_x.htm

Silberglitt R et al. 2006. *The global technology revolution 2020: in-depth analyses*. Santa Monica CA: RAND.
http://www.rand.org/pubs/technical_reports/2006/RAND_TR303.pdf

Singapore. Infocomm Development Authority 2007. Singapore law to control spam. *Media release* 13 April.
http://www.ida.gov.sg/News%20and%20Events/20060919202026.aspx?getPagetype=20

Singapore. Parliament 2007. *Spam Control Bill*.
http://www.parliament.gov.sg/Publications/070006.pdf

Smith RG 2007. Consumer scams in Australia: an overview. *Trends & issues in crime and criminal justice* no. 331. http://www.aic.gov.au/publications/tandi2/tandi331.html

Smith RG 2006. Identification systems: a risk assessment framework. *Trends & issues in crime and criminal justice* no. 324. http://www.aic.gov.au/publications/tandi2/tandi324.html

Smith RG, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Cambridge: Cambridge University Press

Smith RG, Wolanin N & Worthington G 2003. e-crime solutions and crime displacement. *Trends & issues in crime and criminal justice* no. 243. http://www.aic.gov.au/publications/tandi/tandi243.html

Soat J 2004. IT confidential: offshore outsourcing, tax dollars, trouble. *Information week* 13 December. http://www.informationweek.com/story/showArticle.jhtml;jsessionid=JUHHKWUE15KJEQSNDLPSKH0CJUNN2JVN?articleID=55301201

Sophos 2007a. Did your PC try to bring down the internet last night? asks Sophos. *Media release* 7 February. http://www.sophos.com/pressoffice/news/articles/2007/02/dnsbackbone.html?pl_id=9&lang_id=1&lp_keyword=dnsattack

Sophos 2007b. Dorf malware storms the top ten chart. *Media release* 31 January. http://www.sophos.com/pressoffice/news/articles/2007/01/toptenjan07.html?pl_id=9&lang_id=1&lp_keyword=topjan07

Sophos 2007c. *Security threat report, 2007*. http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-2007_wsrus.pdf

Sophos 2006a. Hackers may get second chance to benefit from Second Life security breach. *Media release* 11 September. http://www.sophos.com/pressoffice/news/articles/2006/09/second-life.html

Sophos 2006b. *Stopping zombies, botnets, and other email-borne threats*. Sophos white paper. http://www.sophos.com/pressoffice/news/articles/2006/09/second-life.html

Sprague WE 2006. Uncharted waters: prosecuting phishing and online fraud cases. *Journal of digital forensic practice* 1:143–146

Standards Australia International 2003. *Guidelines for the management of IT evidence: handbook* HB 171-2003. Sydney: SAI

Stewart J 2006. *SpamThru trojan analysis*. http://www.secureworks.com/research/threats/spamthru/

Straub D 1986. Computer abuse and computer security: update on an empirical study. *Security, audit, and control review* 4(2): 21–31

Theoharidou et al. 2006. The insider threat to information systems and the effectiveness of ISO17799. *Computers & security* 24(6): 472–84

Thomas SP 2006. From the editor: the phenomenon of cyberbullying. *Issues in mental health nursing* 27(10): 1015–16

Banco Francs launches m-banking with Movistar 2007. *TMCnet news* 15 January. http://www.tmcnet.com/usubmit/2007/01/15/2245338.htm

TomTom 2007. Isolated number of TomTom GO 910s may be infected with a virus. *Media release* 29 January. http://www.tomtom.com/news/category.php?ID=2&NID=349&Language=1

Tsow A et al. 2006. Warkitting: the drive-by subversion of wireless home routers. *Journal of digital forensic practice* 1(3): 179–92

Turnbull B, Blundell B & Slay J 2006. Google Desktop as a source of digital evidence. *International journal of digital evidence* 5(1). http://www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf

Trend Micro 2007. Antivirus UPX parsing kernel buffer overflow vulnerability. *Vulnerability confirmation* 6 February. http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-1034289

Trusted Information Sharing Network (TISN) 2006a. *Critical infrastructure protection: whose responsibility is it?* http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~CI+Whose+Responsibility+Updated+6+6+06.pdf/$file/CI+Whose+Responsibility+Updated+6+6+06.pdf

Trusted Information Sharing Network (TISN) 2006b. *Wireless security: overview for CEOs*. http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(7A188806B7893EBA0402BC1472412E58)~Wireless+Security+-+Overview+CEOs.PDF/$file/Wireless+Security+-+Overview+CEOs.PDF

Trusted Information Sharing Network (TISN) 2006c. *Wireless security: overview for CIOs*. http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(7A188806B7893EBA0402BC1472412E58)~Wireless+Security+-+Overview+CIOs.PDF/$file/Wireless+Security+-+Overview+CIOs.PDF

United States. Army 2004. A*rmy knowledge management and information technology management*. Army regulation 25-1. http://www.army.mil/ciog6/references/webmaster/docs/WebPolicyExcerptAR25-183104.doc

United States. Defense Security Service (US DSS) 2006. *2006 technology collection trends in the United States defense industry*. http://www.fas.org/irp/threat/2006trends.pdf

United States. Department of Justice (US DoJ) 2007a. Bogus expert in computer forensics pleads guilty to perjury charges. *Media release* 4 May. http://www.usdoj.gov/usao/cae/press_releases/docs/2007/05-04-07EdmistonPlea.pdf

United States. Department of Justice (US DoJ) 2007b. Digital currency business e-gold indicted for money laundering and illegal money transmitting. *Media release* 27 April. http://www.usdoj.gov/opa/pr/2007/April/07_crm_301.html

United States. Department of Justice (US DoJ) 2007c. Electronic funds transfer fraud. *Media release* 8 May. http://cleveland.fbi.gov/dojpressrel/2007/fraud050807.htm

United States Department of Justice (US DoJ) 2007d. Extradited software piracy ringleader pleads guilty. *Media release* 20 April. http://washingtondc.fbi.gov/dojpressrel/pressrel07/wfo042007b.htm

United States. Department of Justice (US DoJ) 2007e. Four defendants arraigned in half-million dollar eBay fraud scheme. *Media release* 16 February. http://www.usdoj.gov/usao/gan/press/2007/02-16-07.pdf

United States. Department of Justice (US DoJ) 2007f. Four men convicted in online auction piracy initiative. *Media release* 26 April. http://milwaukee.fbi.gov/dojpressrel/pressrel07/auctionpiracy042607.htm

United States. Department of Justice (US DoJ) 2007g. Former member of the US navy indicted on terrorism and espionage charges. *Media release* 31 March. http://newhaven.fbi.gov/dojpressrel/2007/nh032107.htm

United States. Department of Justice (US DoJ) 2007h. Software piracy ringleader extradited from Australia. *Media release* 20 February.
http://www.usdoj.gov/criminal/cybercrime/griffithsExtradition.htm

United States. Department of Justice (US DoJ) 2006a. California man sentenced for 'botnet' attack that impacted millions. *Media release* 25 August.
http://seattle.fbi.gov/dojpressrel/2006/pr082506.htm

United States. Department of Justice (US DoJ) 2006b. Five family members face new charges of conspiring to export U.S. defense articles to China and lying to federal investigators. *Media release* 25 October.
http://www.usdoj.gov/usao/cac/news/pr2006/146.html

United States. Department of Justice (US DoJ) 2006c. Former Chinese national charged with stealing military application trade secrets from silicon valley firm to benefit governments of Thailand, Malaysia, and China. *Media release* 14 December.
http://www.usdoj.gov/criminal/cybercrime/mengCharge.htm

United States. Department of Justice (US DoJ) 2005. Six defendants plead guilty in internet identity theft and credit card fraud conspiracy. *Media release* 17 November.
http://www.cybercrime.gov/mantovaniPlea.htm

United States. Federal Trade Commission United States. General Accounting Office (US GAO) 2004. *Technology assessment: cybersecurity for critical infrastructure protection*. Technical report GAO-04-321.
http://www.gao.gov/new.items/d04321.pdf

United States. Immigration and Customs Enforcement (US ICE) 2005. ICE arrests 9 in Ohio fraud driver's license scheme. *News release* 24 February.
http://www.ice.gov/pi/news/newsreleases/articles/drivers022405.htm

United States. National Drug Intelligence Center (US NDIC) 2006. *National drug threat assessment 2007: drug money laundering*.
http://www.usdoj.gov/ndic/pubs21/21137/index.htm

United States. National Science and Technology Council (US NSTC) 2006. *Federal plan for cyber security and information assurance research and development: report by the Inter-agency Working Group on Cyber-security and Information Assurance*.
http://www.ostp.gov/nstc/html/Cyber%20Security%20and%20Information%20Assurance%20Report%20April%202006.pdf

United States. Office of Management and Budget (US OMB) 2006. Protection of sensitive agency information. *Memorandum* M–06–16. 23 June
http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf

United States. Secret Service (US SS) 2004. U.S. secret service's operation firewall nets 28 arrests. *Media release* 28 October.
http://www.secretservice.gov/press/pub2304.pdf

United States. Treasury Inspector General for Tax Administration (US TIGTA) 2007. *The Internal Revenue Service is not adequately protecting taxpayer data on laptop computers and other portable electronic media devices*. Audit report no. 2007–20–048.
http://www.treas.gov/tigta/auditreports/2007reports/200720048fr.pdf

University of California Los Angeles (UCLA) 2006. UCLA warns of unauthorized access to restricted database. *Media release* 12 December.
http://newsroom.ucla.edu/page.asp?RelNum=7571

University of Missouri-Columbia 2007. May 2007 security incident. *Media release* 10 May.
http://doit.missouri.edu/computersecurity/

Urbas G & Krone T 2006. Mobile and wireless technologies: security and risk factors. *Trends & issues in crime and criminal justice* no. 329.
http://www.aic.gov.au/publications/tandi2/tandi329.html

Viega J et al. 2001. Trust and mistrust in secure applications. *Communications of the ACM* 44 (2): 31–36

Visa Southeast Asia 2007. *Mobile Visa Wave*.
http://www.visa-asia.com/ap/sea/cardholders/cardsservices/visa_wave_mobile.shtml#1

Vodafone 2007. Safaricom and Vodafone launch M-PESA, a new mobile payment service. *Media release* 13 February
http://www.vodafone.com/start/media_relations/news/group_press_releases/2007/safaricom_and_vodafone.html

Vogelstein F et al. 2005. 10 tech trends to watch in 2005. *Fortune* 151(1): 43–55

Wall DS 2004. The internet as a conduit for criminal activity, in Patttavina A (ed), *Information technology and the criminal justice system*. Thousand Oaks CA: Sage: 77–98

Wallace M 2006a. A futuristic utopia for Duran Duran. *3pointD.com* 7 August.
http://www.3pointd.com/20060807/a-futuristic-utopia-for-duran-duran/

Wallace N 2006b. Lodhi guilty of terror plot. *Sydney morning herald* 19 June.
http://www.smh.com.au/news/national/lodhi-guilty-of-terror-plot/2006/06/19/1150569264287.html

Walton R 2006. Balancing the insider and outsider threat. *Computer fraud & security* 11: 8–11

Wang X & Wang SS 2006. Virtual money poses a real threat. *China.com* 12 December. http://english.china.com/zh_cn/business/news/11021613/20061226/13837346.html

Ward M 2006. Anti-cartoon protests go online. *BBC.co.uk* 8 February. http://news.bbc.co.uk/1/hi/technology/4692518.stm

Winton R & Hong P 2006. LAPD, FBI probe arrest on videotape. *TRB.com* 10 November. http://cw2.trb.com/news/nationworld/nation/la-me-beating10nov10,0,2844841.story?coll=kwgn-nation-1

World Intellectual Property Organization (WIPO) 2006. *WIPO guide to intellectual property worldwide*, 2nd ed. http://www.wipo.int/about-ip/en/ipworldwide/index.html

Yang D 2007. The impact of business environments on software piracy. *Technology in society* 29(1): 121–41

Ybarra ML et al. 2006. Harassment: findings from the second youth internet safety survey examining characteristics and associated distress related to Internet. *Pediatrics* 118(4): 1169–77

Yee N 2006. The demographics, motivations and derived experiences of users of massively-multiuser online graphical environments. *PRESENCE: Teleoperators and virtual environments* 15(3): 309–29

YouTube turned crime-fighter in Canada 2006. *Channelnewsasia* 19 December. http://www.channelnewsasia.com/stories/technologynews/view/248015/1/.html

Zhang F & Wang Y 2003. Security fundamentals, in Kou WD (ed), *Payment technologies for e-commerce*. New York NY: Springer: 7–38

Zhu L 2006. China nabs 44 suspects in biggest internet virtual property swindle. *China view* 15 December. http://news3.xinhuanet.com/english/2006-12/15/content_5492401.htm

Zovi DD 2006. Hardware virtualization based rootkits. Paper to Black Hat USA 2006 briefings, Las Vegas, 2–3 August

Research and Public Policy Series
No. 78

Over the next two years, Australians will use information and communications technologies at an ever-expanding rate. They will make use of computers and mobile devices to communicate, share information, and work and play with people across the globe. What opportunities for criminal exploitation of these new technologies will arise? This publication identifies the risks and considers their implications for policing, policy and law making. If we can understand the opportunities for crime and predict their likely trajectory, government and industry can develop effective responses before they are realised. Some will lie in developing more secure technologies. Others will require education of the public. Where prevention fails, police and the courts need to be well-equipped to take effective steps to bring criminals to justice. This report comprehensively examines the risks of technology-enabled crime and provides a workable platform for response.