TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 341 July 2007

The future of technology-enabled crime in Australia

Kim-Kwang Raymond Choo, Russell G Smith
and Rob McCusker

As our use of information and communication technologies increases and evolves, incidents of technology-enabled crime are likely to continue. Based on what we know today, this paper summarises a range of potential challenges that regulators and law enforcement agencies need to bear in mind. Key areas identified include infrastructure risks, the use of wireless and mobile technologies, more sophisticated malware, new identification and payment systems, computer-facilitated fraud, exploitation of younger persons, intellectual property infringement, and industrial espionage. Successful prosecution and appropriate sentencing for these crimes will require coordinated policing and on-going legislative reform.

Toni Makkai
Director

As ICT continues to advance, there will be increasing opportunities for criminals to act unlawfully. Serious and justifiable concerns exist about the ways in which new technologies are likely to be misused in the years to come. Technology-enabled crime already ranges across a wide spectrum of activities. These include crimes that involve breaches of personal or corporate privacy, crimes committed by individuals that deliberately alter data within corporations or government agencies for profit, personal or political objectives, and crimes that involve attempts to disrupt the operation of the internet. These, and other areas, are likely to pose considerable challenges for regulators and law enforcement over the coming period, particularly the next two years. In which areas, then, are risks of technology-enabled crime most likely to occur?

Infrastructure risks

Developments in ICT now greatly facilitate commerce between developed countries and newly emerging economies such as India and China. Although these economies are developing quickly, their information security, and legal and ICT policy environments are often less well developed. In this environment technology-enabled crime attacks on Australian organisations could emanate from, or make use of, security weaknesses in those countries. Threats to ICT infrastructure could also arise from natural disasters and other accidental causes. A recent example was the earthquake in Taiwan on 26 December 2006 that disrupted telephone and internet services throughout Asia. The expansion of broadband services also creates risks arising from the fact that connections are open continually – making it easier for malware attacks such as botnets to occur against insecure computers, often used from home.

ISSN 0817-8542

ISBN 978 1 921185 48 9

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9272
Fax: 02 6260 9293

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

Disclaimer:
This research paper does not necessarily reflect the policy position of the Australian Government.

Project no. 0074a

<AHTCC>

Threats to critical infrastructure

Tight couplings between different areas of critical infrastructure (CI) – information technology and communications, banking and finance, water, energy and utilities, transportation, mass gatherings, food, and emergency services – may result in rapid escalation of seemingly modest disruptions from within one sector to others. If insecure sectors are compromised, they can then be used as launching pads to attack other CI sectors. Private companies responsible for the majority of CI are a major vector for cyberterrorism and crime, although growing concern exists over networked computers in other contexts such as households and educational institutions, which may be the targets of network-oriented malware.

A successful attack on ICT infrastructure that supports many areas of CI may disrupt supply chain systems, financial sector networks or power grids. Consequences of these attacks could reverberate after the immediate damage is done, as cross-sector interdependencies are of primary importance. Specific examples of cyberterrorism are rare at present in Australia and internationally, although any instance of technology-enabled crime that exposes vulnerabilities in CI security indicates a potential for a cyberterrorist attack.

A further area of risk concerns planning of terrorist attacks that involve the use of ICT. Terrorists, for example, could simply use open-source geospatial information to plan attacks on military forces stationed overseas. For example, it was recently reported that terrorists might have used information obtained from Google Earth™ to facilitate their planning of physical attacks against British troops in Iraq. (Harding 2007). Terrorists could also use social networking sites, such as those used by extremist and supremacist groups, as vehicles to reach an international audience, solicit funding, recruit new members, and distribute propaganda.

Outsourcing risks

The growing acceptance of the internet as a communication tool and the trend for corporations to locate their operations in developing countries to benefit from lower labour costs 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 US jobs are likely to be located offshore by the end of 2015 (McDougall 2004).

Outsourcing involves the transfer of a significant amount of management control to offshore vendors and this usually results in diminished control over security arrangements. There is also a possibility for vulnerabilities to be clandestinely introduced into software developed offshore and for loss or misappropriation of intellectual property to occur, particularly in countries with inadequate legal systems for protecting such rights.

Data storage and dissemination

Future technological innovations and the declining price of electronic data storage devices will continue to lower entry barriers for digitisation of information. The size and capability of data storage devices will continue to be enhanced by advances in technology.

With increased digitisation of information, the future will see the increased likelihood of digital content being a source of disputes or forming part of underlying evidence in judicial proceedings.

Better educated criminals are likely to explore alternatives to hiding data over the internet such as storing data on compromised machines, password-protected file-sharing websites, email accounts and less reputable content providers hosted in countries with lax cybercrime legislation. They are also likely to leverage the use of anti-forensic tools and information hiding tools including steganography to further impede the collection of evidence.

Developments in data storage and dissemination technologies such as proprietary storage media and 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 possibly be compromised during extraction or conversion from incompatible proprietary formats. An in-depth understanding of how different technologies and applications operate is crucial in collecting digital evidence.

It can reasonably be anticipated that technology-enabled crime prosecutions involving multiple jurisdictions will continue to occur as legislation dealing with such matters is subject to amendment over the next two years to deal with new technological developments and threats.

Wireless and mobile technologies

Mobility is an enduring characteristic of today's knowledge-based society. As businesses continue to engage in e-commerce and m-commerce, they will become increasingly global and interconnected. This will increase the risks of identity-related financial crime committed through the use of modern technologies. The following wireless and mobile technologies are examples of possible threats in the next two years.

Mobile devices: The increasing use of mobile devices, with ever-increasing storage capacities, constitutes a key threat for the future. Moreover, the ease with which erased data on such devices (which might contain passwords and account details) can be recovered increases their attractiveness to criminals. Advances in 3G and 4G wireless telephony and the widespread dissemination of Bluetooth-enabled mobile phones will increase the popularity of multimedia services such as multimedia messaging services (MMS). MMS could be exploited by criminals and malware writers in various ways, as demonstrated by Mulliner and Vigna (2006).

Instant messaging (IM): The proliferation of IM programs constitutes another threat for the future. Malware authors will continue to target IM programs with malicious code (e.g. W32.heartworm which installs files on victims' computers recording personal and financial information). Botnets, one of the internet's biggest threats, will also target IM and other peer-to-peer networks for command and control (C&C) of infected systems. This will allow C&C servers to be arranged in a distributed structure to limit traceability by law enforcement.

Wireless networks: Key among the vulnerabilities created by wireless networks is that networks and their data can be accessed without physical access being required. This facility assists both the user and the criminal. Enhanced methods of exploiting wireless vulnerabilities include drive-by subversion of wireless home routers through unauthorised access by mobile WiFi clients and other forms of attacks. These include eavesdropping and sniffing of voice over internet protocol (VoIP) calls, man-in-the-middle attacks, denial of service attacks, and making 'free' calls on VoIP networks built over wireless local area networks.

Evolution of malware

The trend to exploit social vulnerabilities and prey upon the public interest by using breaking news events to disseminate malware is likely to continue in the next two years. So too will the trend of designing malware for facilitating blended attacks (e.g. spy-phishing – phishing attacks that involve the use of malicious applications to perpetrate online information theft). The availability of a market in which to sell malware provides criminals with 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 and selling W32/Fujacks to other internet hackers for more than 100,000 yuan (Dao 2007).

Malware authors will continue to explore ways to deny victims access to information regarding the source or nature of malware infection. The future will also see the continued development of malware employing self-modifying code and code obfuscations to elude detection by anti-virus and anti-malware products. Other stealth techniques to hide files, processes or registry values belonging to the malware, including the installation of an application program interface (API) that hooks into running processes or changes system APIs, will continue to be enhanced.

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

Kernel-mode malware: Kernel-mode malware, which is executable as part of a computer's operating system and has full access to the computer's resources, is hard to detect. Several working prototypes of kernel-mode malware and hypervisor (e.g. Blue Pill) have been identified as a risk. Although kernel-mode malware has yet to become popular, threats from such malware are likely to increase.

Ransomware: The application of cryptographic tools and techniques to enhance new malware attacks will also increase. This includes ransomware programs designed to search for data on compromised systems and encrypt these data (e.g. Win32.Gpcode.ag ransomware). This activity, also known as cryptovirology or denial of resources attacks, has yet to become widespread, although it is very likely that ransomware attacks will become more targeted, for example, against certain organisations and industries. They will also use more complex encryption functionality.

Internet browsers and web services: These will be of interest to criminals and malware authors. For example, users' computers can be infected by malware when they visit compromised websites (by exploiting vulnerabilities in web servers or operating systems) that host malicious programs.

Existing security measures such as network-based firewalls may not be able to defend against threats of unauthorised access to a web service. Di Paola and Fedon (2006) demonstrated how Asynchronous JavaScript and extensible markup language can be exploited to facilitate attacks against web services. Future probable exploitation of internet browsers and web services to disseminate malware includes designing malware to hide browser attack codes and circumvent existing anti-malware products, and mix known exploit codes so that they become unrecognisable to anti-virus programs.

Unauthorised access

Threats from outsiders: Semantic attacks committed through social engineering will continue to be employed by criminals to gain access to computers and networks. Social engineering is the use of psychological tricks to manipulate human behaviour often through deception on unsuspecting users to gain access information. Once access to the system has been gained, they are able to manipulate the information to suit the needs of their attack. For example, information from unauthorised intrusions into systems that process or store information related to customer transactions can facilitate illicit financial transactions.

Threats from insiders: 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), and 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. Corrupt insiders could deliberately introduce vulnerabilities during the coding of inhouse software used to manage sensitive military or intelligence networks. This could allow terrorists or foreign intelligence agents to exploit vulnerabilities and surreptitiously enter systems, gain control, and launch attacks via and against compromised systems.

There will also be more avenues for insiders to leak sensitive documents or information. An example is the website http://wikileaks.org/ designed for whistleblowers in authoritarian countries to post sensitive documents on the internet without being traced. The anonymity feature is provided with the use of an anonymising protocol that allows data to be routed through a network of servers. Cryptography is used to further obscure the data path and make it untraceable.

Identification systems

Although the Australian national health and social services access card is not designed to be a generalised government identity card, the biometrically-enabled card will have widespread use and applications, making it a likely target for criminals. Areas of risk will relate to the dishonest initial enrolment of users as well as data security, with respect to the card's computer chip and supporting databases. Threats might also arise from criminal groups which seek to compromise the system's computer infrastructure, or others who seek to obtain personal information for use in identity-related crimes.

Radio frequency identification (RFID) enabled biometric passports are designed to provide strong authentication that unequivocally identifies their bearers. 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 (to circumvent the use of Faraday cages). A recent study by Rieback et al. (2006) on the design principles for RFID malware together with proof-of-concept examples underscores the feasibility of RFID devices being abused to be exploited in attacks against biometric passports.

New payment systems

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 many electronic currency transactions are not captured by regulators, and that internet IFTIs may assist in the money laundering process.

The following electronic payment technologies are examples of possible threats in the next two years (AIC 2007).

Prepaid cards: The anonymity offered by pre-paid cards continues to act as a vehicle for facilitating illicit financial transactions and money laundering, particularly as value limits increase. A recent report (NDIC 2006) emphasises similar concerns.

Smart cards: 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 smartcards. In a recent study of 20 different RFID-enabled credit cards issued in the United States by Visa, Master Card and American Express, Heydt-Benjamin et al. (forthcoming) presented proof-of-concept prototypes and attacks. The study suggested that RFID-enabled credit cards are susceptible in various degrees to a range of other traditional RFID attacks such as skimming.

Online gaming and gambling

In the virtual multiplayer online games (MMOG) worlds (e.g. Second Life), players are able to purchase virtual properties, accommodation and merchandise, and inflate their virtual status using physical cash. For example, it was reported on LindeX, the official Second Life currency exchange, 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 in virtual goods trading provides criminals with financial incentives to offend. Organised criminal rings and hackers target MMOG 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.

Risks of money laundering will also increase as MMOG sites emerge as a potential vehicle for online money laundering. For example, money launderers could purchase virtual currency using illicit cash and exchange the virtual currency back into cash.

Existing avenues of money laundering such as online gambling, a multibillion dollar industry, will continue to be used. 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 money mules' accounts to obfuscate the money trail.

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. Computer-facilitated frauds include advanced fee scams (e.g. Nigerian scams) and online auction frauds. Major drivers with an impact on computer-facilitated frauds include the rapid expansion of new and emerging technologies and the apparent ease of committing consumer fraud.

Click frauds: Several search engines such as Google™ and Yahoo™ and online sites are supported either in part or in full by pay-per-click advertising revenue models. In such models, advertisers are charged based on the click-through rate of an advertisement. However, such a revenue mechanism could be abused by malicious hosting sites. Click frauds have been identified as an emerging threat to e-commerce (Delaney 2005).

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 the w32.KMeth worm that can 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 and storefront to buy and sell a wide range of merchandise through competitive bidding. Crimes associated with online auctions, particularly online auction frauds, are likely to increase. Criminals and malware authors will continue to design malware to circumvent existing anti-fraud measures for illicit financial gains.

Phishing and spam: Phishing attacks will become more sophisticated and the number of such attacks will increase. Dissemination of spam will be facilitated not only through the use of botnets, but also VoIP –Vishing – and mobile phones (via SMS) – SMiShing – which will be used to overcome existing spam prevention and detection filtering software. The future will see an increase in persistent attacks using redirection or the use of malware techniques that trap even astute internet users. The development of technical attacks poses 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 which lead to malicious sites. Some sites may contain code that allows the phishers to retrieve contextual information such as details of sites visited from the browser's cache. The contextual information obtained can then be used to facilitate 'context aware phishing'.

It is also likely that automated tools (e.g. Universal Man-in-the-Middle Phishing Kit) will be further enhanced to include more sophisticated capabilities targeting two-factor authentication mechanisms such as subversion of token-based logons, and acquisition of and reuse of 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.

Exploitation of younger persons

As young people increasingly make use of personal computers and mobile devices, risks will arise where inadequate security measures are in place. Online scams are likely to target young users, who may be less vigilant in detecting scams than adult users. In recent years, a new form of bullying, including harassment targeting young users, has emerged which makes use of communication technologies.

Child exploitation and offensive content

Although the level of knowledge of and measures to combat the dissemination of child pornography and involvement of children in sexual offending have increased, individuals and groups of criminals will continue to use ICT to carry out such crimes.

The use of cryptographic technologies will continue to be used by offenders to enable images to be shared securely. In addition, it can be expected that involvement in child exploitation will include the highly disturbing practice of live child sexual abuse videos being streamed to internet chatrooms, with the actual perpetrator responding in real time to commands from other participants who are able to see the images.

Intellectual property infringement and industrial espionage

The enhanced capacity of ICT systems will enable electronic products to be copied and reverse engineered (stripping down and analysing competitors' products) more quickly and easily than at present. The transfer of technology to countries with different notions of property rights, or weaker protection of 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 business process operations to other countries could face difficulties in protecting their intellectual property rights and enforcing foreign court judgments. A recent report (IIPA 2007) suggested that China and Russia are rated as the countries of greatest concern to the copyright industries, contributing to losses in revenue of US$2.207 billion and US$2.18 billion respectively (see also Kennedy & Clark 2006; Gross 2007; Yang 2007).

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 intellectual property held electronically. Enhanced reverse engineering techniques will also facilitate unauthorised access and exploitation of intellectual property. Criminals, competitors and foreign intelligence agents could also exploit commercial joint venture and offshore outsourcing relationships for commercial 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 are otherwise carried out over insecure networks.

Targets of attacks

The next wave of 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. As a result, prevention at both the consumer and business levels will remain of high importance. In addition to existing threats, new attacks will come from people, not just with programming experience, but with business, systems and legal experience. There will be a significant shift in offender focus with more attacks targeting specific businesses and specific systems within those businesses. Cybercriminals will probe for weak or unguarded computer networks within commercial organisations whose ability to detect and to respond to fraud or other thefts may be slow, imprecise or 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. Traditional transnational organised crime groups are unlikely to shy away from using the technology-enabled crime environment to facilitate the operation and/or to disguise the illicit proceeds of real world based crimes. Organised operations which make use of conventional technology-enabled crime methodologies will also increase as the use of networked computers for criminal purposes develops. Organisations in the financial services industries are likely to be targeted more frequently than others, with financial gain the ultimate goal. Terrorist financing through the use of technology-enabled crime will also develop as an important risk area.

Conclusions

The prosecution and judicial disposition of cases involving technology-enabled crime will continue to raise key issues faced by police and prosecutors. These include the need for legislative reforms as a result of the emergence of 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 discretion, novel defences and defence arguments and appropriate sentences for convicted offenders.

There is no single all-encompassing answer to responding to technology-enabled crime. Countering these 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:

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

Technical assistance to less ICT-advanced jurisdictions will also be essential. This will help not only to minimise the development of technology-enabled crime within these locations, but also to enable assistance to be provided for the investigation of increasingly cross-jurisdictional technology-enabled crimes. Developing a culture of security for information systems and networks is of primary importance, and this can be achieved through coordinated efforts by both government and private sector organisations. If these efforts are successful, the development of new forms of technology-enabled crime in the future will be minimised.

Related report

This paper is based on *Future directions in technology-enabled crime: 2007–09*. http://www.aic.gov.au/publications/rrp/78/index.html

References

Australian Institute of Criminology (AIC) 2007. New methods of transferring value electronically. *High tech crime brief* no. 14

Dao C 2007. 8 arrests in computer virus case. *China daily* 13 February

Di Paola S & Fedon G 2006. Subverting AJAX – next generation vulnerabilities in 2.0 web applications. Presented at 23rd Chaos Communications Congress, Berlin

Delaney KJ 2005. In ‘click fraud’, web outfits have a costly problem. *Wall street journal* 6 April: A1

Gross G 2007. U.S. to file trade complaint against China. *PCworld.com* 9 April

Harding T 2007. Terrorists use Google maps to hit UK troops. *Telegraph.co.uk* 13 January

Heydt-Benjamin TS et al. forthcoming. Vulnerabilities in first-generation RFID-enabled credit cards. Proceedings of Financial Cryptography and Data Security 2007 *Lecture notes in computer science*

International Intellectual Property Alliance (IIPA) 2007. *Copyright industries in the U.S. economy: the 2006 report.* Washington, DC

Kennedy G & Clark D 2006. Outsourcing to China: risks and benefits. *Computer law & security report 22(3):* 250–253

McDougall P 2004. There’s no stopping the offshore-outsourcing train. *Information week* 24 May

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

Rieback M et al. 2006. RFID malware: design principles and examples. *Pervasive and mobile computing 2(4):* 405–426

United States. National Drug Intelligence Center (NDIC) 2006. *National drug threat assessment 2007: drug money laundering.* Washington, DC: NDIC

Yang D 2007. The impact of business environments on software piracy. *Technology in society* 29(1): 121–141

Dr Kim-Kwang Raymond Choo and Rob McCusker are research analysts at the Australian Institute of Criminology. Dr Russell G Smith is Principal Criminologist at the Australian Institute of Criminology.

**General editor, *Trends & issues in crime and criminal justice* series:
Dr Toni Makkai, Director,
Australian Institute of Criminology,
GPO Box 2944 Canberra ACT 2601
Note: *Trends & issues in crime and criminal justice* papers are peer reviewed.**

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*.