The incidence of cybercrime in Australia and its impact on consumers

AIIA response to House of Representative Committee on Communications

Inquiry into the incidence and impact of cybercrime on consumers and the Australian economy.

June 2009

Background – About AIIA

The Australian Information Industry Association (AIIA) is Australia's peak information and communications technology industry body. AIIA's role is to lead and represent the ICT industry in Australia to maximise the potential of the Australian economy and society. AIIA's membership encompasses all sectors of the ICT sector including hardware, software, services and telecommunications. It has almost 500 member companies, from individual consultants, small to medium enterprises to the world's leading multinational corporations. AIIA member companies employ over 100,000 Australians, generate combined annual revenues of more than $40 billion (approximately 5% of GDP) and export more than $2 billion in goods and services each year.

AIIA is acutely aware of the cyber-security risks to ongoing safe use and exploitation of digital infrastructure, and the possible loss of confidence by users if those risks are not appropriately managed. Members participate in all relevant government programs aimed at user education and awareness, information sharing among critical infrastructure owners and real-time cyber-safety exercises involving cross-jurisdictional and international stakeholders.

Overview

"It is safe to anticipate that in all aspects of society the use of and reliance on information and communication technologies (ICT) will be more pervasive in the future. It is also reasonable to expect that today's ICT technologies will continue to evolve into a model that more critically depends on "services" hosted on the internet using interconnected technologies. The pervasiveness and advancements in mobile technology and the demands of consumers will dictate that almost every new electronic device will have some form of 'anywhere access' capacity".[1]

AIIA is pleased to provide industry comment on the House of Representatives Committee on Communications' review into cybercrime. Safe and confident use of digital infrastructure poses one of the most serious economic and security challenges for modern governments. The genesis of digital infrastructure architecture was born out of considerations of interoperability and efficiency, not security. Increased productivity growth and related economic advantages across sectors are now well accepted by

[1] Microsoft Australia, "E-Security Review 2008", page 4.

commentators. [2] So the secure and safe use of all the potential benefits delivered by digital infrastructure must be assured by governments concerned with enhancing their nations' GDP for the benefit of citizens. This frequently involves a fine balance between maintaining an eco-environment for digital activities that promotes safety, security, privacy and liberties, while meeting increasing consumer demands for innovative service delivery, efficiency, prosperity and fast, free commercial intercourse.

AIIA commends the government and other stakeholders for taking an ongoing and vigilant approach to all these issues. That said, it must be acknowledged that cybercrime knows no borders and detection of perpetrators is notoriously difficult; the nature of many platforms used by criminals in the digital space facilitates anonymity. Criminologists have long argued that certainty of detection, not severity of punishment, is the true deterrent for would-be criminals. So any efforts to send clear signals to cybercriminals that the national and international community is working seriously towards reducing opportunities for nefarious activities will assist.

In this regard AIIA urges the Government to develop and *adopt a clear definition of cybercrime* so that victims of cyber attacks understand that a crime has in fact been committed and encourage them to report that crime to appropriate authorities. Data from the Australian Institute of Criminology indicates that under-reporting of cyber incidents is a major obstacle to useful data collection and better understanding of the nature of the problem.

Further, AIIA recommends that the *act of identity theft in its own right, be made an offence* under the Model Criminal Code. Currently, identity theft alone is not a crime; it must be accompanied by a subsequent crime such as fraud or forgery to be actionable.

Thirdly, AIIA urges the Government to *sign and ratify the Council of Europe Convention on Cybercrime,* a model legal instrument that has been ratified by the US, Japan and Canada among others of our major trading partners.

Definitions – What is 'Cybercrime'?

Information and communications technologies (ICT) have become an integral part of almost every facet of modern, developed economies, underpinning their civil infrastructure, public safety, energy supply and management, financial networks and

[2] Access Economics, "The Economic Benefits of Intelligent Technologies", April 2009. Commissioned by IBM Australia

national security. This development has led to productivity increases and enhanced efficiencies across many economic sectors such as the financial, manufacturing and retail sectors.

But it has also resulted in opportunities for existing crimes such as fraud, forgery and impersonation to be carried out by the ill-intentioned in new and more detection-proof ways. A new lexicon has entered the public discourse reflecting the myriad models of behaviour now open to those intent on crime: cyberstalking, cyberbullying, phishing and spamming to name a few. If the undoubted benefits of online and digital economic transactions are to be further realised, all users must have confidence that information is secure, commerce is not compromised and critical infrastructure is not infiltrated. This confidence will only be assured through constant political vigilance, enhanced governance, application of technologies, education and changes to certain laws.

Cybercrime can be understood by reference to its eco-environment, cyberspace. The US has defined cyberspace as "the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people."[3] By this definition, cyberspace is *not just the internet*; so cybercrime can occur in a much wider environment than the internet.

Usefully, the Australian Institute of Criminology (AIC) suggests the following stratification as an attempt to understand what cybercrime is; "cybercrimes can be characterised according to whether they are 'computer-assisted' or 'computer-focused'",[4] that is, whether the crime is enabled by a computer (making it easier to commit an offence) or enhanced by a computer (where the computer is essential for the commission). While this distinction is an aid to understanding, it has little relevance in the detection of cybercrimes or the enforcement of penalties. It also limits the environment to a 'computer' when in fact cybercrimes occur in the broad environs of the entire digital infrastructure. Cybercrime can also include offences directed at computing technologies themselves, not the data thereon. Cybercrime (or e-crime) is perhaps best

[3] Cyberspace Policy Review, www.whitehouse.gov/assets/documents/cyberspace_policy_refview.final/pdf
[4] AIC Report No. 102, www.aic.gov.au

understood as any unauthorised use, damage, theft, attack or monitoring of data stored in any digital environment. The crucial element is that the data use is *unauthorised.*

Identity and Identification

A critical pre-requisite of certain cybercrimes is identity theft. Identity crime can involve fictitious identity (fabricated), alteration of own identity (manipulation) or assumption of pre-existing identity (theft). More than 88% of identity fraud in the US involves fictitious or fabricated identities, not stolen or assumed identities.[5] Identity-related crimes are more commonly a constituent part of more serious criminal offences and not a primary focus of identity thieves. Studies have indicated that only a small number of identity fraud acts take place over the internet – most involve traditional offline channels.[6]

Methods of obtaining identities vary; Victoria Police warn homeowners that names and addresses can be stolen from letterboxes (or garbage bins) and used to commence a process of obtaining 'valid' identification documents such as birth certificates, which can in turn be used to obtain further identification documents to carry out a fraud or similar criminal act. More sophisticated methods involve phishing email attacks, key logging devices or infiltration of organisations storing large amounts of personal data (financial institutions, payments processors, government agencies).

Various definitions of identity crimes exist. COAG adopted the following definitions in 2007:

> **Identity crime** is a generic term to describe activities/offences in which a perpetrator uses a fabricated identity, a manipulated identity, or a stolen/assumed identity to facilitate the commission of crime.
>
> **Identity fraud** is the gaining of money, goods, services or other benefits or the avoidance of obligations through the use of a fabricated identity, a manipulated identity, or a stolen/assumed identity.
>
> **Identity theft** is the theft or assumption of a pre-existing identity (or a significant part thereof), with or without consent, and whether, in the case of an individual, the person is living or deceased.

---

[5] Final Report Identity Crime, Model Criminal Law Officers' Committee, page 4. www.agd.gov.au

[6] Ibid: page 10

The OECD uses the following definition; "ID theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes".

Clear definitions of cybercrime, identity theft and identity crimes are crucial if detection and enforcement of penalties for these 'victimless' crimes is to be enhanced.

In this regard it is noteworthy that apart from South Australia and Queensland, it is not currently an offence in Australia to assume or steal another person's identity except in very limited circumstances (such as concealing an identity under the Taxation Administration Act 1953). What is later *done with* the assumed identity attracts law enforcement attention; another associated criminal act like fraud or forgery will trigger legal mechanisms. **There is no single offence that comprehensively criminalises identity theft in its own right.**[7]

The Terms of Reference

Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans

Credible data on the nature and prevalence of e-security risks and subsequent cybercrimes is notoriously difficult to obtain, due to a variety of reasons, including under-reporting. Victims of cybercrime under-report either through ignorance (as to what 'crime' has occurred) or desire not to signal their organisation's poor security and so reduce their customers' confidence. Banks are generally thought to fall into this group of under-reporters. Under-reporting also occurs in cases of phishing and financial scams because 'victims' do not wish to appear ignorant or gullible.

In relation to theft of personal information (identity data), it is equally difficult to be definitive about nature and prevalence because in many cases victims do not know their personal data has been assumed or stolen until a subsequent crime is perpetrated against them, such as credit card fraud or some other financial incident.

---

[7] Final Report - Identity Crime. Model Criminal law Officers' Committee of the Standing Committee of Attorneys-General. March 2008. www.agd.gov.au.

In relation to malware infection rates, Australian rates are much lower than the *worldwide average of 1 out of every 123 computers infected* with malware. The malware infection rates in Australia are comparable to those observed in Denmark and Nigeria, and slightly higher than those in Malaysia (1:216) or New Zealand (1:264).

Consistent with the global trend observed in 2007, there has been a large increase in the detection of Trojan Downloaders and Trojans in Australia. Criminals use Trojan Downloaders to install other malicious files on the infected system either by downloading them from a remote computer or by dropping them directly from a copy contained in its own code.

Evidence from Australia and other countries suggests that Trojans have become the tool of choice among criminals in targeting victims around the world and in Australia. These approaches represent an evolution of an expanding toolset supported by sophisticated software engineering techniques and processes used by criminals to compromise users' digital devices which increasingly include mobile and gaming variants.

Because Trojans, by definition, are primarily carriers or vectors for any desired form of software code, they have the capacity to place multiple agents on a user's device that work in concert at the behest of a remote entity. This sets the conditions for an extremely wide range of cyber-based exploits not yet experienced but fully possible.[8]

The most recent and credible data available on nature and prevalence is from the AIC. The data related to small, medium and large businesses. In brief, the AIC findings are:

- 14% of all businesses experienced computer security incidents during the survey year
- the most common incidents were malware code and virus attack
- the most common outcome was software corruption
- total financial loss was estimated to be up to $649million
- most businesses dealt with the incident internally

[8] Microsoft Australia, E-Security Review 2008.

- only 8% of victims reported breaches to a law enforcement authority
- total cost of protection for business was estimated to be up to $1.95billion
- the most common tool used to defeat breaches was anti-virus software

These findings throw up certain implications relevant to this review. The data indicate that law enforcement agencies do not feature as part of the solution to cybercrime; this may be due to the fact that most victims feel the cyber incident is not important enough to report to police or are unsure if it is a crime. Specific sectors may choose not to report serious attacks to avoid negative publicity (banks etc). The AIC survey also indicates that the types of cyber attacks experienced by participants could lead to more serious crimes such as fraud and forgery through the use of assumed personal identity data.

The AIC notes that cyber criminals appear to be "mostly opportunistic offenders" not organised crime gangs. Their cyber attacks were indiscriminate, not planned. This is in line with data from other jurisdictions such as the US.

The implications of these risks on the wider economy, including the growing economic and security impact of botnets

The implications and effect of cybercrime across the wider economy is difficult to ascertain because there is no reliable method of measuring losses from downtime, or quantifying the dollar value of stolen data. Estimates from various reports indicate that financial losses for business in Australia could be as high as $1.1billion per annum.[9] In the UK, the impact of cybercrime (defined as identity theft) is estimated at 1.7billion pounds over three years.

Curiously, some commentary indicates that over-zealous anti-fraud policies have resulted in lost online orders for some internet retailers. This development, combined with the more natural human response to curtail online trading because of the perceived risk, has had a negative impact on online commercial transactions. Consumers have apparently reduced (by up to one third) their online retail activity, or confined it to large well-known retailers, which will have a consequential impact on smaller businesses

[9] Model Criminal Law Officers' Committee, page 6

trying to digitise their activities. In any deliberations by government on appropriate policy settings, a balance must be struck between facilitating protection against cybercrime and ensuring regulation does not become rampant or over-zealous.

As importantly as the financial impact, there is the possible loss of confidence by consumers and business in using a digital infrastructure to conduct their activities. The consequential failure to exploit the potential of that digital world will have even greater negative impacts on economic efficiencies and productivity growth.

Australia's critical infrastructure may also be compromised if risk-threats are not appropriately managed. The critical infrastructure includes physical facilities, supply chains, ICT networks etc that support the efficient operation of social and public life. If destroyed or degraded for extended periods, its loss would detrimentally impact the economic and social wellbeing of citizens, and/or affect Australia's capacity to ensure national safety and security. See www.tisn.gov.au. Successful cyber attacks against critical infrastructure could affect water supply, health services delivery, national communications, energy distribution, financial and banking services and transport.

Level of understanding and awareness of e-security risks within the Australian community

The AIC data has shown that 85% of survey participants used some type of security tool or method to protect their business data online, so it can be assumed that at least in the business community, awareness of cybercrime risk is relatively high. Whether that awareness extends to complete understanding of the implications of serious cybercrime is not known. So far as private users are concerned, increasing government efforts to raise awareness and understanding through various education programs and policies have raised the profile of the issue beyond where it was, say, five years ago. E-security Week, online education and information programs managed through the Department of Broadband Communications and Digital Economy continue to assist. Business efforts to educate customers have also had a salutary impact. Banks are especially adept at bringing to customer notice the very real potential of financial loss unless appropriate care is taken. The IT industry likewise is focussing on customer education and awareness; suppliers such as Microsoft, Cisco, MacAfee and Verizon publish articles and learned papers setting out latest developments from the e-security environment. But given that there will continue to be ill-intentioned individuals with access to increasingly sophisticated analysis and attack tools, it is not practical or possible to prevent all types

of cybercrime at all times and in all circumstances, just as it is similarly impossible with more 'traditional' crimes.

Measures currently deployed to mitigate e-security risks faced by Australian consumers

i) Education initiatives

AIIA commends the government on its continuing efforts to develop and manage education and awareness programs and policies[10] through relevant agencies and media. AIIA members have in the past participated in E-Security Week events and the development of the strategies behind such programs. AIIA would urge government to continue these programs with the engagement of industry in the rollout. At this stage AIIA does not see the need to increase the frequency of those programs. Clearly, content and coverage of the programs needs to be regularly upgraded as anti-cybercrime technology develops, and as more users move online. This will especially be the case when small business is more actively encouraged to conduct their business digitally, as occurred in the recent Budget with positive assistance initiatives to assist those businesses to go online.

ii) Legislative and regulatory initiatives

As noted earlier in this paper, identity theft is not a crime in Australia, apart from two state jurisdictions. The Model Criminal Law Officers' Committee recommends in its March 2008 report that a specific identity theft crime offence be created using definitions that would comprehensively cover identity fraud and identity theft. AIIA supports this recommendation and urges the Government to adopt this approach. The model offences proposed are:

- dealing in identification information
- possession of identification information (with the intention of committing or facilitating commission of indictable offences);
- possession of equipment to create identification information

While there are some issues associated with these proposals (mere possession of a printer may be an offence unless the circumstances of possession are circumscribed by lack of relevant intent), AIIA believes that progression towards a consistent legal

[10] These include cybersafety outreach for schools, youth advisory groups, research into new technologies to defeat cybercrime, "Don't Take the Bait" programs against phishing, Scam Watch, and Stay Smart Online.

framework which provides certainty to users about what amounts to a cybercrime will enhance user confidence and allow victim compensation to be more equitably managed. In this regard AIIA commends the paper by the Australasian Centre for Policing Research[11] to the Committee.

iii) Cross-portfolio and inter-jurisdictional coordination

The best example of cross-portfolio and inter-jurisdictional coordination is TISN and Cyber Storm I, II and III. AIIA supports these activities and AIIA members have participated in Cyber Storm activities. AIIA commends the Cyber Storm II report to the Committee as it spells out failures in communications and cooperation which should be addressed. In this regard AIIA notes that Australia appears to be leading the US in preparedness, vigilance and content. The most recent report from the White House (Cyberspace Policy Review) states that the US digital infrastructure is not secure or resilient. Although Cyber Storm I and II threw up significant challenges for infrastructure providers and managers in Australia, lessons learned indicate that Australia is addressing the gaps identified by the US research.

iv) International co-operation

Cybercrime is a borderless phenomenon. Because cyber-attacks can be launched from any geographic domain, detection and enforcement processes are notoriously difficult. This makes it ever more critical that nations cooperate in developing consistent legislation and regulation in the international community to send to cyber criminals the message that where possible, nation-states will act against cybercriminal activity. It also signals to Australia's trading and diplomatic partners that we are committed to addressing cybercrime. The Council of Europe Convention on Cybercrime has been ratified by 21 nation-states, including the US, the UK, Japan and Canada. The Convention sets out some of the substantive criminal law offences that should be enacted at the national level of signatories. It also deals with illegal access to computer data, illegal interception of data and data interference. System interference, misuse of devices, computer related fraud and forgery are also covered. The Convention is attached for reference.

Australia is neither a signatory nor a ratifying member of the Convention. Dealing successfully with the global aspect of cybercrime hinges on effective and efficient

[11] Review of the legal status and rights of victims of ID theft in Australasia. 2006.

international cooperation; AIIA strongly urges the Government to commence proceedings to ratify the Council of Europe Convention without delay.

Future initiatives that will further mitigate the e-security risks to Australian internet users

Cyber Storm III in October 2010 will provide further useful input to systems, communications plans, strategic coordination and agency interdependencies through an exercise aimed at assessing and improving crisis management arrangements for the protection of critical infrastructure. AIIA commends the government for pursuing these no-fault exercises with national and international partners. AIIA members will continue to participate in this important activity.

Ongoing efforts to adopt a model criminal code covering a specific identity theft offence are also supported by AIIA.

Industry and government cooperation in TISN activities has also produced positive outcomes through sectoral infrastructure assurance advisory groups; information shared and lessons learned through joint exercises means that tailored security response measures will be more likely in the case of real-time cyber crises.

Emerging technologies to combat these risks.

All suppliers active in the data/network protection market are constantly developing new technologies and systems to enhance customer safety online and in cyberspace. These include perimeter protection, device and physical security, smartcards and tokens, biometrics, software-based protection, intrusion detection and encryption. AIIA would be pleased to prepare specific information from members for the Committee should that be required.