NSW GOVERNMENT SUBMISSION TO THE HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON COMMUNICATIONS' INQUIRY INTO CYBER CRIME

Introduction

At the beginning of 2007, 5.67 million households in Australia had Internet access[1], and even more people were accessing the Internet at work or school. While cyberspace provides opportunities in the learning and working environments, it is also an effective tool for crime. It enables offenders to commit crimes all over the world and creates difficulties in detecting and investigating their crimes.

The term 'cyber crime' covers two types of situations. The first is when a computer or network is the victim of an attack. The second is when a computer or network is used in an attack. Cyber crime encapsulates traditional offences such as fraud, which may now be committed online, however it also entails new offences such as distributed denial of services attacks, and infections of databases. Australia, along with the international community, needs to increase the security of cyberspace, while still maintaining privacy, civil liberties and efficiency.

The Government of the United States of America has recently released its Cyberspace Policy Review[2], which was developed over many months with the input of many experts. In addition, the Council of Europe has developed a *Convention on Cyber Crime.*[3] It is important that Australia deals with this issue in a systematic and informed way, complementing the work of the international community. I therefore encourage this inquiry to become the beginning of an in depth policy review of how Australia is going to deal with this important and growing problem.

Outlined below are NSW comments against the Terms of Reference.

a. 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.

There are many different forms of cyber crime including fraud, online sexual exploitation of children, selling unclassified films and computer games online, selling spray cans for graffiti online and cyber bullying.

The NSW Police Fraud Squad Computer Crime Team has investigated a number of cyber crime incidents. They also provide investigation leadership to the joint Identity Security Strike Force. However, NSW Police do not record whether a crime was conducted through cyberspace. Therefore data on cyber crime

---

[1] *Australian Computer Crime and Security Survey* www.auscert.org.au/render.html.
[2] *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communications Infrastructure,* 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_review_final.pdf
[3] Convention on Cybercrime, CETS No 185, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.

incidents in NSW is difficult to obtain. There is also concern that many of these types of crime remain unreported.

However, other sources give some indication of the prevalence of e-security risks/cyber crime in Australia generally.

- Figures released by the Australian Institute of Criminology estimated that more than $600 million was lost through electronic crimes in the 2006-07 financial year. Approximately 40% of all identity frauds are facilitated online.[4]
- Twenty-seven percent of adolescent survey respondents who used chat rooms had received sexual solicitation.[5]
- Just over one-third of 13 to 16 year old Australian students surveyed reported being cyber-bullied online.[6]

In 2007, the Australian Bureau of Statistics (ABS) *Australian Personal Fraud Survey*[7] found that:

- 1.8 million people in NSW have been exposed to scams.
- Credit or bank card fraud and identity theft are more prevalent types of personal fraud in NSW than other types of scams.

b. <u>The implications of these risks on the wider economy, including the growing economic and security impact of botnets</u>

The Australian Institute of Criminology has published *The Australian Business Assessment of Computer User Security: a national survey*[8] which focuses on the cost of computer security incidents to Australian businesses. For 2006-07, the survey estimated the financial losses across all Australian businesses at between $595 and $649 million.[9] This figure does not take into account the costs borne by financial institutions as a result of cyber crime attacks on Australian businesses. This survey also compares the results of previous AusCERT Computer Security Surveys.

Attachment A provides further information on the economic loss caused by cyber crimes.

Botnets are having a significant impact on economic security and create several problems for law enforcement. Botnets are used to spread malicious software

---

[4] P Hoskin *Emerging fraud risks and countermeasures in government welfare* Paper presented at The Australian & New Zealand Society of Criminology 19th Annual Conference, 2006, Sydney, Australia.
[5] J Stanley 'Child abuse and the internet' *National child protection clearinghouse child abuse prevention issues* No 5.
[6] MJ Flemming, Greentree, D Muller-Cocotti, KA Elias & S Morrison 'Safety in cyberspace: Adolescents' safety and exposure online' *Youth & Society* 38, 135-154.
[7] Australian Bureau of Statistics, *Personal Fraud,* 2007. Available online at http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/4528.02007?OpenDocument
[8] K Richards, *The Australian Business Assessment of Computer User Security: a national survey,* Australian Government, Australian Institute of Criminology, 2009. Available online at http://www.aic.gov.au/publications/rpp/102/
[9] K Richards, p 73.

including Trojans. They are also used to create anonymous proxy servers, which effectively disguise criminal transactions on the Internet by masking the true Internet Protocol addresses of offenders. This in turn makes investigation difficult.

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

NSW has no clear information on the level of awareness of e-security risks within the community. However, the Australian Business Assessment of Computer User Security (ABACUS) survey shows there is a low level of awareness of security initiatives, with only 21% of businesses reporting being aware of any current awareness raising initiatives related to computer security including *Scamwatch, FIDO, AusCERT* etc.[10] This suggests that awareness of risks may be low amongst the business community, but this would require further examination.

On the other hand, the Australian Communications and Media Authority (ACMA) has recently released a report which found that 75% of children surveyed claim they know not to give out personal details while online and can remember key Internet safety messages.[11]

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

Education initiatives
The NSW Office of Fair Trading acts as a portal for many complaints by consumers who are targeted by, or fall victim to, cyber scams. The Office of Fair Trading responds to this by investigating complaints over which it has jurisdiction, forwarding complaints to appropriate authorities and educating consumers on scam awareness. For example, the Office of Fair Trading's network of 24 Fair Trading Centres distributes the Identity Theft kit developed as part of the Commonwealth Government's National Crime Prevention Program.
There are a number of resources on the internet, such as the Australian Government *Stay Smart Online, Scamwatch, FIDO, AHTCC,* and *AusCERT* websites that can educate consumers. For example SCAMwatch is a website owned and operated by the Australian Competition and Consumer Commission (**ACCC**) and is the portal for the Australasian Consumer Fraud Taskforce. SCAMwatch portal includes scams of electronic, paper-based and face-to-face varieties and allows consumers Australia-wide to report scams through one central point.

The NSW Office of Fair Trading is also a member of the Australasian Consumer Fraud Taskforce (ACFT). ACFT is composed of 19 Commonwealth, State and New Zealand regulatory agencies that have responsibility for consumer protection in relation to fraud and scams. The Taskforce is a national working group that creates an annual coordinated education campaign timed to coincide with the Global Consumer Fraud Prevention Month. The Taskforce ran campaigns in 2006-09.

---

[10] K Richards, p 47.
[11] The Australian Communications and Media Authority, *Click and connect: Young Australians' use of online social media,* http://www.acma.gov.au/WEB/STANDARD..PC/pc=PC_311797, July 2009.

The 2009 campaign was influenced by the results of 2007 scams research undertaken by the Australian Bureau of Statistics on behalf of the ACFT. It ran from 2-8 March and consisted of an advertising campaign (metropolitan press, metropolitan radio, and online); a media kit; an online survey; print and electronic collateral; a Fraud Forum in Melbourne on 2 March 2009 and participation by private sector and community partners.

The advertising campaigns used four victims' stories with the slogan "All these people have lost money". The campaign intended to make consumers aware that anyone can lose money to scams and that they should report scammers to SCAMwatch.

Legislative and regulatory initiatives
NSW has released an Exposure Bill, the *Crimes Amendment (Fraud and Forgery) Bill 2009 (NSW)*, creating new and updated fraud, forgery and identity crime offences, for public consultation. The Exposure Bill is available at www.lawlink.nsw.gov.au/clrd.

NSW has also implemented computer offences in the *Crimes Act 1900* that make it illegal for a person to access data, modify data and impair electronic communications.

These legislative initiatives are based on the Model Criminal Code, which may be accessed at http://www.pcc.gov.au/uniform/crime%20(composite-2007)-website.pdf. The Model Criminal Code has been developed as a cooperative project between the Commonwealth, State and Territory Governments with the aim of developing uniform national criminal laws, to be adopted by States and Territories.

Cross portfolio and inter-jurisdictional coordination
Significant jurisdictional issues arise in cyber crime. For example an offender can be physically located in jurisdiction #1, the Internet Service Provider (**ISP**) the offender uses can be in jurisdiction #2, the satellite used can be governed by jurisdiction #3, the victim is located in jurisdiction #4 and the investigating Police are in jurisdiction #5. For this reason, it is essential that there is national and international coordination to address cyber crime.

To investigate cyber crimes requires sophisticated equipment and specialist knowledge that state-based consumer protection agencies do not have. The Australian High Tech Crime Centre (AHTCC) (operated by the Australian Federal Police (AFP)) has a function in determining policy and strategy issues but its role is also to provide a national approach to combating cyber-crime especially where the abilities of a particular jurisdiction to investigate are limited.

The National Identity Security Coordination Group, includes representatives from all Australian jurisdictions from a number of portfolios and discusses many of the issues that relate to identity security, including cyber crime.

International cooperation
Cyber crime is an international problem and can involve victims and offenders in a number of different countries. However, access to information held overseas which may assist a cyber crime investigation can be difficult to obtain, even if held by an ISP in a cooperative jurisdiction. The NSW Police Force often works with the AFP's network of Liaison Officers to obtain this information. There are also agents of the United States of America's Federal Bureau of Investigation located in Canberra and Sydney who are of assistance.

However, where formal evidence is needed for court proceedings, or coercive powers need to be used, the NSW Police Force uses the Mutual Assistance Scheme. This is a very important component in some investigations. However, obtaining evidence through the Mutual Assistance Scheme can be a long process. As the rate of cyber crime increases, the need to use the Mutual Assistance Scheme will also increase.

The scheme is currently inadequate to deal with any increased use.
Australian law enforcement agencies also have very good access to some overseas providers such as Microsoft and Google. In some cases though there is substantial difficulty obtaining information from similar organizations and further work is required to develop these international networks.

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

Legislative/Policy initiatives
As noted above, NSW has implemented computer offence laws, and is currently consulting on a new Bill that will introduce, fraud, forgery and identity crime offences. However, this should only be the beginning of legislative reforms to tackle cyber crime.

There are still gaps in our current model national legislation. For example, the Computer Offences focus on the hardware rather than cyber space more broadly. The model identity crime offences were established to capture the members of the syndicates that are using the information to commit a crime rather than those at the head of the syndicates or those that develop the means to obtain the information. Identity crime is growing and merging with cyber crime as technologies develop, it crosses national and international borders, with the more serious cases of identity crime coordinated by international syndicates. Identity crime occurs in many forms. At the low end it may be through the photocopying of a document. High volume, high impact identity fraud is, however, most often achieved by exploiting the opportunities the internet provides. Whilst the states can pass legislation tackling identity crime the extreme and aggravated form of the offending should be separately reflected by a specific offence in the Commonwealth Criminal Code - committing identity crime using the internet. Relevant policy and legislative mechanisms need to be developed to deal with this issue as well as others.

A broader issue relating to cyber crime is police powers, such as 'remote access powers'. By allowing a warrant to be obtained for remote access, law enforcement are more likely to be able to decipher encrypted data by conducting

surveillance at a point between the user and the encryption interface. This would involve remotely accessing (or "hacking into") a computer via the internet to obtain transmissions of product passing over that computer at a point at which it is unencrypted. This would require legislative amendments both at a State and Commonwealth level.

It is recommended that a national cyber crime working group be established to develop legislative initiatives for cyber crime for both Commonwealth and State jurisdictions to implement. The working group would report to an appropriate Ministers' Council. This group could also give further consideration as to whether Australia should become a signatory to the *Cyber Crime Convention*. This group would need to include policy developers from justice and police agencies of all jurisdictions with significant input from the AHTCC.

International cooperation
It is suggested that consideration be given to increasing the speed of the Mutual Assistance process. NSW has become aware in the preparation of this submission that an Exposure Bill has been released by the Commonwealth that amends the *Mutual Assistance in Criminal Matters Act 1987*. Any endeavour to streamline the Mutual Assistance process is welcomed, however further review may be required in order to keep abreast with the rapidly changing area.

Further consideration should be given to whether Australia should become a signatory state of the Cyber Crime Convention. However, the work that was begun by establishing the cyber crime convention could be furthered by bringing like minded nations together as was recommended in the US Cyber Space Policy Review. The international community could establish technical standards, and legal norms regarding territoriality. *Public awareness*
Large proportions of the community are unaware of the dangers of cyber crime and are even less aware of how to prevent or minimise the chances of becoming a victim of cyber crime. Effective national campaigns, such as the Australian Government's National e-Security Awareness Week, should be maintained to educate the broader community of cyber crime (eg anti-smoking campaign). wg

Consumers would also greatly benefit from a centralised, coordinated point to receive and act on complaints of cyber crime. At present, agencies such as ACMA and others provide an avenue for reporting some cyber crimes (eg spam), but the broad range of cyber-scams that now exist suggest that the community may be better served by providing a central point to refer suspected cyber-scams, rather than the segmented and ad-hoc arrangements currently in place.

Cooperation between the public and the private sector
In ensuring the security of cyber space the public and private interests are intertwined. It is recommended that guidelines be developed between Governments and the private sector, which will establish the roles and responsibilities of the different sectors.

Increasing Australia's skills for combating cyber crime
The Australian law enforcement cyber crime community is small. This community needs to be increased. Deakin University's School of Law has just introduced a graduate certificate of commercial law (financial crime control). I would

encourage universities across Australia to offer such courses as well as IT courses focused on teaching students how to combat cyber crime.

The current cyber crime law enforcement specialists need to be trained to develop and maintain a cyber crime investigation capability. Western Australian Police are leading a project, presently under consideration by the Australia New Zealand Policing Advisory Agency (**ANZPAA**), to define competencies for investigators at three levels of response. This is an important, but first step in improving skills in this area.

Information sharing portal
There are limited means of effectively sharing important intelligence information between jurisdictions. One way of addressing this is to have a common information portal available to Cyber Crime investigators, including the use of Web 2.0 technologies, for example an online wiki.

f. <u>Emerging technologies to combat these risks</u>

There is often an abundance of digital evidence relevant to a cyber crime investigation. Law enforcement officers are faced with the challenge of providing investigators with access to this evidence in a timely manner.

New Zealand Police have launched a project, code named *Eve*, which enables investigators to readily access digital evidence from their desktop. Some agencies, including in NSW, are beginning to roll out solutions relating to the examination of mobile telephones. The quantity of data involved also poses an issue of how to link it to other criminal investigations, including interstate matters.

On the other hand, the increase in the use of VOIP (ie voice over Internet Protocol, a telecommunications system that uses the Internet or other Internet Protocol network to transmit telephone calls) poses a major threat to the ability to intercept conversations. Currently, some VOIP communications are not able to be intercepted at all (see **Attachment A**).

Encryption also poses a threat to the ability to intercept communications and examine digital evidence. Some encryption methodologies such as TrueCrypt even permit cyber criminals to provide keys that unlock only innocent looking data.

There are some investigation techniques, which in some cases would greatly assist in combating these risks, for example remote access methodologies.

ATTACHMENT A
EXAMPLES OF CYBER CRIME

Credit Card Database hacking:
A hacker successfully compromised the website of an Internet vendor in Sydney, stealing thousands of credit card details. The target computer was a Windows 2003 server and at least one of the tools used to hack into the system was "Hacker Defender", which is a rootkit. A rootkit is a software system that consists of a program (or combination of several programs) designed to hide or obscure the fact that a system has been compromised. "Hacker Defender" is readily available online (eg http://www.rootkit.com/) and used widely within the hacker.

The NSW Police Fraud Squad Computer Crime Team (the Fraud Squad) believes that the stolen credit card details were sold by the hacker on a carder site (see below). The stolen credit card details were then used to make millions of dollars worth of fraudulent purchases, mainly overseas.

Based on a forensic examination of the compromised server, the Fraud Squad suspected a person based in Vietnam as the primary instigator of this particular hack. Law enforcement agencies in that jurisdiction were informed.

Another, more common form of database hacking is a technique referred to as a Structured Query Language (SQL) attack or SQL injection. This technique involves directing queries to a SQL database exposed to the Internet in a manner which permits the attacker to create a root or administrator account on the server, or to copy data tables. The complexity of this type of cyber crime requires highly skilled law enforcement officers with a high degree of skill in computer security and forensics to quickly liaise with their counterparts in other states, territories and countries.

Phishing:
Phishing is a very common form of hacking that causes huge financial losses to Australian Financial Institutions and the community. Phishing is the criminally fraudulent process of acquiring sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

When this technique was first used in Australia, it appeared to be exclusively of Eastern European origin. Recent investigations have identified persons in Sydney organising phishing attacks combined with spam.

Vishing:
This is a recent cyber crime technique combining Voice over the Internet Protocol (VOIP) and phishing. "Vishing" scams usually begin when an individual criminal configures a war dialler (sequentially dialled regional phone numbers) to call numbers in a given region. When each phone is answered, an automated recording is played to alert the consumer that fraudulent transactions have been made with their credit card and that they should call a particular phone number

immediately. When the phone number given is dialled, the caller ID of the consumer's financial institution is displayed.[12]

Trojans:
The use of Trojan software has been a successful attack vector for several years. Trojans facilitate unauthorised access to computers.

Individuals purchase Trojan kits to create infections and harvest personal financial information from victims' computers. In Strike Force Aubert, an Indonesian syndicate was identified in Australia using the *Perfect Keylogger* program which is readily available online from www.blazingtools.com. A sample of the keylogger was obtained from one of the victims, and through a combination of reverse engineering and network monitoring, the destination to which the keylogger was sending information could be identified.

Trojan infections are common in Australia. The 2006 AusCERT Computer Security Survey found that survey participants reported a 20% rate of rootkit infection.

Share Market manipulation by Trojan compromise:
Individuals may infect computers (for example, a case currently being investigated by the Fraud Squad involved computers at an internet café) with a keylogging Trojan, compromising internet banking and online share trading accounts. The share trading accounts may then be used to create a "pump and dump" situation, i.e: trading high volumes of shares to artificially inflate their value over a short period of time. Accomplices may then trade in these shares to make a profit. This form of criminal activity is generally detected by financial institutions and the losses contained. Losses from these sources appear to be exclusively borne by financial institution shareholders. However, there are several scams where victims bear the losses themselves.

Advance fee fraud:
Advance fee fraud has been active in various forms for many years. An advance fee fraud involves the offender persuading the victim to advance sums of money in the hope of realising a significantly larger financial gain. These scams mainly originate from Nigeria and Ghana.[13]

However, it is difficult to determine the total number of Australians that have fallen victim to advance fee fraud. Victims are often vulnerable members of the community and may be too embarrassed to report that they have been a victim to such a crime (or may not even be aware of it). The losses suffered sometimes represent the life savings of elderly people, who are particularly vulnerable to such scams, and the effect can be catastrophic.

Online Auction Trading Site Fraud:
Online auction fraud involves fraud conducted on online auction sites such as www.ebay.com, where the seller or the product for auction does not exist).

---

[12] R Jaques, 10 July 2006, *Cyber-criminals switch to VoIP 'vishing'* accessed at http://www.v3.co.uk/vnunet/news/2160004/cyber-criminals-talk-voip?page=2

[13] http://www.police.qld.gov.au/programs/crimePrevention/eCrime/scams/Nigerian_Scams.htm.

For example, organised groups of criminals may advertise cars and boats for sale through online trading sites. The seller typically claims to have reduced the price of their car based on a plausible excuse. The victim then pays for a car which is never delivered. Victims of these scams typically lose about $9,000 per transaction, and some are tricked into a further payment of $2,000. There have been victims in every state of Australia. The actual losses are difficult to quantify. However, NSW Police estimate that about $600,000 has been transferred to one particular syndicate over a three month period.

Carding Sites:
Individuals can sell data, such as credit card details, on 'carding sites' or 'carder forums'. These sites provide effective and secure means for criminals to exchange information and purchase compromised data for internet banking and identity crimes. These sites also have sophisticated reputation systems that inhibit penetration by law enforcement agencies.

Another effective inhibitor for law enforcement agencies in investigating these crimes is that, in order to collect information from the sites, law enforcement officers need to engage in the purchase of data. These sites often require new members to be introduced, and purchase a security certificate. The legality of a police officer engaging in such activities may be challenged in the absence of parallel controlled operations issued by both the Commonwealth and State. Such controlled operations, while they can be renewed, are typically of short duration whereas developing a covert capability is a long term operation.

Carding sites have effectively lowered the entry level for people who want to make money out of identity and cyber crime, and investigations have demonstrated a strong link between the use of these sites and cyber crime offences. These sites also provide advice on how to defeat law enforcement, and many also maintain a list of those people who kept funds obtained instead of transferring them overseas or to the head of a syndicate as agreed.

These sites are now an integral enabler of cyber crime in Australia.

Online alternate remittance schemes:
Another development which has assisted cyber criminals is the development of online alternate remittance schemes, such as E-Gold and Web Money.
E-Gold was prosecuted for money laundering by the US Secret Service and is not as commonly used now. However, services such as Web Money offer secure exchange of value for payment on these sites, and are quite invisible, and they may be immune from law enforcement action.