House of Representatives Standing Committee on Communications Inquiry into Cyber Crime

Queensland Government Submission
10 July 2009

QUEENSLAND GOVERNMENT COMMENTS

1. General

The Queensland Government welcomes the opportunity to contribute to House of Representatives Standing Committee on Communications Inquiry into Cyber Crime. As the prevalence of e-security related crimes increases, a trend which can only be expected to continue as the impacts of the global economic crisis are felt across communities, this inquiry represents a timely opportunity to examine Australia's progress in combating cyber crime.

The Queensland Government has adopted a proactive approach to minimising the impacts of cyber crime. This approach includes, introducing strategies designed to increase public awareness, developing partnerships with industry, facilitating knowledge sharing and building the capacity of Queensland Government agencies and industry groups to prevent and manage fraud.

The Queensland Government is aware that jurisdictions are also committed to targeting the perpetrators of cyber crime and minimising e-security risks. However, jurisdictional responses are currently developed and undertaken in isolation. Due to the global and dynamic nature of the cyber environment, each individual investigation offers the potential for the discovery of new criminal methodologies, technological applications and investigation techniques. As a result all jurisdictions undertake research in an effort to keep abreast of the ever-changing landscape of cyber crime. Nevertheless, the Queensland Government is of the view that all jurisdictions would benefit from the development of enhanced strategies for learning and sharing knowledge and experiences across jurisdictions.

The Queensland Government is committed to promoting awareness and information sharing of the risks of cyber crime. Most recently, the Fraud and Corporate Crime Group (FCCG), a specialist investigative unit attached to the State Crime Operations Command of the Queensland Police Service, hosted the 2009 Hi Tech Crime Symposium in Brisbane between 7 and 8 July 2009. This symposium provided an important opportunity for government agencies, law enforcement and private enterprise to develop a wider appreciation of the impact of cyber crime within Australia and internationally.

2. Nature and prevalence of e-security risks and the implication of these risks on the wider economy

Queenslanders have most commonly experienced cyber crime in the form of the theft of financial and identity data via targeted intrusion, with significant implications for individual privacy rights. The Queensland Government notes the use of malicious software is growing significantly and can be expected to continue.

The Queensland Government considers Queensland will follow world-wide trends such that online fraud will continue to flourish due to increased take-up

of the internet, poor appreciation by users of the risks of the cyber environment, the development of more sophisticated malware and social engineering techniques by offenders, and the increased global rollout of internet capability.

According to Australian Bureau of Statistics data the number of active internet subscribers is continuing to grow significantly, with most subscribers being households, as opposed to business and government users. According to ABS data household consumers are the largest economic group, the health of the consumer is critical to the health of the Australian economy. For this reason the Queensland Government is of the view that minimising consumer exposure to, and enhancing consumer awareness of, e-security risks is vital in order to maintain consumer confidence in the e-marketplace and support Australia's economic growth.

The growing economic and security impacts of "botnets" were considered at the FCCG's recent symposium. This is the phenomenon whereby a group of computers that have been unknowingly compromised by the covert delivery of a "bot" are netwroked through the commands of a "bot controller". As a consequence these computers become "slaves", whose functions can be taken over by the "bot controller". The computers are then used to deliver spam email, disable legitimate websites, commit distributed denial-of-service (DDoS) attacks, spread keyloggers and steal data. Botnets can generate large amounts of money for the bot controller. The largest botnet in the world is believed to have contained 28 million computers.

The information shared at this symposium has strengthened the Queensland Government's opinion that Botnets represent an ever-growing threat. Botnets provide the foundation for cyber warfare and have been used to attack government sites. This was demonstrated by the recent Russian Georgian conflict and previously by the disablement of Estonian web sites by Russian operations. The fact that Australia currently has an internet take up of about 80%, whereas the rest of the world stands at approximately 23%, is a factor, which alone, will increase the size and prevalence of botnets. It is anticipated that DDoS attacks upon government infrastructure and private sector organisations can be expected in the future. Both the governments of the United States of America and the United Kingdom have appointed heads of cyber warfare/ terrorism.

The Queensland Government also considers it is important to note the social impact of cyber crime, particularly where victims are defrauded of large amounts of money. The impacts for victims can be devastating and many older victims may be unable to return to the workforce to earn what are often lost retirement funds.

3. Measures currently deployed to mitigate e-security risks

The Queensland Government has instituted various measures to try and mitigate the e-security risks faced by Australian consumers.

- Education Initiatives

The Queensland Government is of the view that educating e-consumers is an essential strategy in the fight against cyber crime. A number of education initiatives are run through the Queensland Police Service and the Queensland Office of Fair Trading (OFT).

The FCCG launched Project Synergy – an education and information sharing initiative designed to build the capacity of government agencies, private sector and community groups through the hosting of thematic conferences, such as the 2009 High Tech Crime Symposium referred to above. During 2008, the FCGG hosted the High Tech Crime and Digital Evidence Recovery Symposium..

The FCCG also established a Training and Fraud Prevention Unit to complement its investigative functions. Since its establishment this unit has delivered presentations to business groups and the broader community on topics such as Identity Crime and Computer crime. To date they have delivered 140 presentations to 12,000+ community members.

The FCCG is also currently undertaking the Seniors Online Fraud Project in conjunction with the Queensland University of Technology, which is a research project aimed at assisting the police to more effectively develop strategies to protect the senior members of our community from fraudulent online schemes.

The FCCG has also recognised the vulnerability of consumers using unsecured wireless networks from their homes and is currently developing a project to address this vital issue.

The Queensland Government through its OFT also endeavours to mitigate e-security risks by providing access to information regarding safe online trading through the OFT's website, fact sheets, consumer and trader information booklets, media releases and in education presentations given to community groups and schools. According to a November 2005 Queensland Household Survey commissioned by the OFT, 81.6% of Queenslanders had heard or read warnings issued by the OFT. The Queensland Government considers these are key strategies in promoting informed and responsible consumer and business behaviour.

The OFT website also contains links to the Australian Competition and Consumer Commission's "Scam Watch" website, which provides up to date information regarding scams, malicious emails and alerts to consumers.

Initiatives recently introduced by the OFT, including public access to an on-line Fair Trading licensing register, are designed to assist consumers and industry in determining whether an individual or business they are dealing with holds a current and valid licence or registration.

- Legislative and regulatory initiatives

In Queensland, there are a number of general offences in the Criminal Code which may apply to conduct falling within the ambit of cyber crime. The most common offences used to charge offenders who have committed cyber crime are computer hacking and misuse (s.408E), obtaining or dealing with identification information (s.408D) and general fraud (s. 408C).

The offence of obtaining or dealing with identification information was enacted by the Queensland Government in 2007 in direct response to a growing incidence of identity theft which was assisted by technological advances.

A more detailed overview of the operation of these jurisdictional provisions is at **Attachment 1**. In particular, this overview outlines the relevant evidentiary provisions that are available in Queensland to assist the prosecution of these kinds of offences, which often involve criminal activity occurring or originating outside of Queensland.

The Queensland Government is committed to constantly reviewing its criminal laws and penalties to ensure they respond to a changing community, technological advances and other issues as they arise.

- Cross-portfolio, inter-jurisdictional and international coordination and cooperation

In recognition of the borderless nature of computer based crime, the Queensland Government is committed to developing partnerships and crime prevention and detection strategies that operate across jurisdictions at a national and international level.

The FCCG, which has responsibility for conducting and assisting in investigations for various serious crimes, including computer related crime, was early to recognise the importance of developing and undertaking proactive activities that focussed on target hardening the Australian environment, is lessening the risk that Australian consumers will become the targets of cyber criminals.

Pivotal to the FCCG's endeavours to mitigate e-security risks was the development of key relationship partnerships with industry and government. Most notable is the partnership established between the FCCG and Western Union. Western Union is an American company that provides money transfer services to facilitate people transferring money across the world. It is also unfortunately the primary vehicle used by international cyber criminals to fraudulently obtain funds from Australian consumers. Western Union worked with the Queensland Police Service to launch a pilot program designed to

educate consumers about the current types of frauds and scams and to provide preventative methods to help stop future fraud activities. One of the measures taken involved Western Union redesigning their money transfer forms, so that every form issued in Queensland contained a fraud warning, a series of descriptive prompts, a Queensland Police Service badge and a hotline direct to the FCCG to allow consumers to discuss their concerns.

Western Union in conjunction with QPS also prohibits suspicious transactions and "black bans" identified fraudsters, effectively stopping that person from receiving money from any person, anywhere in the world via Western Union's services.

So successful was this initiative, that it was subsequently launched nationally. Now Western Union forms contain the national Crime Stoppers Logo and a national information hotline number. The project has also recently been replicated in Singapore and the Queensland Government understands that negotiations are underway to commence the program in New Zealand and Malaysia.

In an effort to address a key area of consumer cyber fraud and reduce the burden to front-line police involved in combating this fraud across Australia, the FCCG established the eBay project. This project allows for the Australia-wide electronic reporting and filtering of eBay fraud via a national web-based reporting system. Members of the public who wish to report eBay fraud are assisted by an on-line reporting function, including pre-formatted statements. The details of the offence once submitted by the consumer are then forwarded to the relevant policing agency in the jurisdiction where the alleged offender is located and, in the case of an overseas suspect, an Interpol report is sent to the relevant jurisdiction. The project effectively works as a triage system in isolating and eliminating what in actual fact are complaints of a civil nature, thereby allowing police to focus on the criminal matters.

Since the commencement of the eBay project in mid May 2007 there has been a steady acceleration in the number of on-line reports made. As a result the project has served as an invaluable intelligence gathering tool assisting police to identify serial offenders operating across jurisdictions. In Queensland alone, 788 complaints have been logged to date via this system. It is believed the e-Bay project will allow for more timely investigations and prosecutions by law enforcement agencies thereby limiting the time available for serial offenders to continue committing offences.

The FCCG has also undertaken significant work in the area of Nigerian Fraud, also known as Advanced Fee Fraud through project operations Echo Track and Hotel Fortress. These projects involve providing advice to scam victims, who have agreed on fraudulent pretences, to send money to Nigeria and other places about their real nature of their activities. This kind of information has also been used extensively in media briefings and public warnings.

In furtherance of this work the FCCG has developed an online reporting portal for direct reference to the Nigerian Economic Financial Crime Commission and the Ghana Police.

Additionally, as a consumer protection regulator, the OFT undertook a tender process on behalf of the national Standing Committee of Consumer Affairs Officials (SCOCA) for the development of a consumer complaints and alerts system named AUZSHARE.

On 14 March 2005, the OFT launched the AUZSHARE database with the aim of the project being to improve information sharing between participating agencies. All fair trading agencies in Australia and New Zealand as well as the Australian Competition and Consumer Commission participate in AUZSHARE.

There is an alert function within AUZSHARE which allows authorised users to post alerts, and subsequently forwards an email notification to all users. This function has been used successfully to inform and flag systemic and cross border issues and investigations for users and alert them to any issue of importance that may be of a national significance. Information is available in Australia and New Zealand immediately after the information has been posted.

4. Future initiatives and emerging technologies to mitigate and combat e-security risks

Cyber-crime presents unique challenges for governments, particularly law enforcement and crime prevention agencies, due to the national and international connectivity provided by the internet. In this regard, the Queensland Government encourages consideration being given to the following national-led initiatives in an effort to mitigate e-security risk:

- Australia-wide consistent training to police.
- Development of national community education and training products, including education targeted specifically at school children and senior communities.
- A centralised national reporting centre such as the IC3 (Internet Computer Crime Complaints Centre) which operates in the United States of America. The IC3 is managed by the Federal Bureau of Investigation and is an online crime reporting centre and clearing house for cyber crime. It is understood that the IC3 plays a pivotal role in detecting and reporting the identity of cyber criminals and providing information to victims of cyber cime.
- Establishment of the e-Crime Managers Group. It is envisaged this group would contain representatives from across Australian policing agencies whose function would be to develop proactive strategies to combat cyber crime, including facilitating inter-jurisdictional operations, establish national standards and facilitate information sharing.

- Australian membership of the Council of Europe's Convention on Cybercrime in order to achieve greater international cooperation and assistance in the fight against cyber crime.

The Queensland Government also recommends recent technology involving biometrics and device fingerprinting supported by secure gateways and quality encryption be explored. Such strategies would assist in overcoming the anonymity of a good deal of internet activity and provide enhanced security. For example, should a senior member of government have their laptop stolen from their vehicle or residence, or perhaps lose their USB storage device, such items may be opened and used or viewed by the person finding them. However, if they were encrypted this would not be possible

The move by the banking industry to 100% chip pin technology at point of sale terminals and ATMs would also be of significant benefit to the Australian community. The experience of the American company TJX illustrates the potential benefits of chip pin technology. In this example a data intrusion on the company resulted in 40,000,000 identities and credit card accounts being stolen. A person with access to these kind of details could have cloned them onto a magnetic stripe type card and used this to exploit the card holder and merchant in direct purchase contacts. This would not be possible with chip pin technology.

Attachment 1
RELEVANT QUEENSLAND CRIMINAL CODE OFFENCES

The most common offences contained in the Queensland Criminal Code used to charge offenders who have committed cyber crime are computer hacking and misuse (s.408E), obtaining or dealing with identification information (s.408D) and general fraud (s. 408C).

The offence of computer hacking and misuse applies where a person uses a restricted computer without the consent of the computer's controller. 'Use' includes (a) accessing or altering any information stored on; (b) communicating information to or from; (c) causing a virus to become installed on; or (d) otherwise affecting; the restricted computer.

For the purposes of this section, 'controller' is defined to mean a person who has a right to control the computer's use and generally speaking, a 'restricted computer' is a computer for which a device, code or sequence of electronic impulses is necessary to gain access and the controller withholds, or attempts to withhold or restrict access.

The offence is punishable by 2 years imprisonment increasing to 5 years if detriment is caused or a benefit is gained, or there is an intention to do so. If the value of the detriment, damage or benefit is more than $5,000 or there is an intention to commit an indictable offence, the maximum penalty is 10 years imprisonment.

In relation to computer hacking and misuse, the Queensland Court of Appeal indicates that in sentencing 'public deterrence may be thought to be a significant consideration' – *R v Boden* [2002] QCA 164.

The offence of obtaining or dealing with identification information, contained in section 408C, applies where a person obtains or deals with another entity's identification information for the purpose of committing, or facilitating the commission of, an indictable offence, for example fraud or theft. The offence is punishable by a maximum penalty of 3 years imprisonment.

When a person is sentenced for this offence, the sentencing court may issue a certificate to the victim stating the offence, the victims name and anything else the court considers relevant for the victims benefit. This certificate is intended to assist a victim in repairing damage to their reputation (for example, their credit rating).

The Queensland Criminal Code also contains other offences which may be relevant depending to the use made of the computer or the information thereon. These offences include fraud, forgery, uttering, stealing and personation.

For example, the offence of fraud could be charged where a hacker gains access to a personal computer and locates banking details which they use to purchase property. Fraud applies to acts of dishonesty where, for example, a

person obtains property from another or a benefit or advantage. The offence is punishable by 5 years imprisonment increasing to 12 years in certain circumstances, for example, where the offender is a director of the victim corporation or the yield is $30,000 or more.

Queensland's Criminal Code contains a number of provisions relevant to the jurisdictional and evidentiary issues that can arise when prosecuting offences for cyber crime.

Section 12 of the Code provides that:

A) where acts or omissions occur outside of Queensland which, if committed in Queensland, would constitute an offence and any one of the acts or omission actually take place in Queensland, the person responsible is guilty of an offence of the same kind and is liable to the same punishment as if all the acts or omissions had occurred in Queensland.

B) where an event occurs in Queensland caused by an act done or omission made outside of Queensland which, if committed in Queensland, would constitute an offence, the person responsible is guilty of an offence of the same kind and is liable to the same punishment as if the act or omission had occurred in Queensland.

C) where an event occurs out of Queensland caused by an act done or omission made in Queensland, which would have constituted an offence if the event occurred in Queensland, the person who does the act or makes the omission is guilty of an offence of the same kind and is liable to the same punishment as if the event had occurred in Queensland.

Sections 13 and 14 of the Code also deal with liability for persons who enable, aid, procure or counsel another, whilst outside of Queensland to commit an offence in Queensland or who, in Queensland, procures another to do an act or omission outside of Queensland.