INTERNET SAFETY INSTITUTE

House Standing Committee on Communications

Inquiry into Cyber Crime

Submission by

Alastair MacGibbon
Internet Safety Institute

www.internetsafetyinstitute.com.au

7 July 2009

Background

On Wednesday, 13 May 2009, the Minister for Broadband, Communications and the Digital Economy, Senator the Hon Stephen Conroy, asked the House Standing Committee on Communications to inquire into and report on the nature and incidence of cyber crime in Australia.

About the Internet Safety Institute

The Internet Safety Institute was founded in December 2008 to provide an honest and informed view of issues facing online consumers, businesses and governments. Through thought leadership, public comment, research and education, we aim to advance the cause of safety on the internet.

The founders of the Internet Safety Institute are experienced in the field of online consumer protection.

The author of this submission, Alastair MacGibbon, most recently spent 4 and a half years as head of Trust, Safety and Customer Support for eBay Australia and later eBay Asia Pacific. Prior to eBay, MacGibbon was the founding Director of the Australian High Tech Crime Centre, and was a Federal Agent with the Australian Federal Police for 15 years. As a consequence of his government and commercial experience, MacGibbon has worked in the field of internet crime from a national policing and a corporate perspective, has dealt with consumer victimisation and corporate survival in the online space, has championed consumer education and driven a range of public private partnerships aimed at reducing internet crime.

Executive summary

Our observation is that the uptake, use and reliance upon the internet by society has outstripped the development of capabilities within government to fight online crime, while criminals have gathered pace in their activities.

Our key recommendations are:

- We urge the Committee to recommend to government agencies to carry out more frequent and more robust quantitive studies that place a value on household and business losses due to eSecurity incidents.

- We believe that government agencies should expand their engagement of online businesses to help deliver security and safety messages to consumers when it is most relevant to them: when they are online.

- We recommend that the Australian Government undertake a ”public health” style approach to changing consumer and business eSecurity habits.

- Consideration needs to be given to regulation of the internet space, such as the responsibilities and requirements for ISPs and internet registries to know their customer, and to take action when they believe their networks or services are being abused, and when crimes are reported to them.

- We urge the Federal government to take an increased and leading role in developing a national capacity to protect all Australians online. This will require substantial increases in funding and staffing of police, regulatory and policy units, and would benefit from amalgamating several Federal functions under fewer agencies and departments.

- We urge the Attorney General’s Department to explore ways to streamline and improve securing and obtaining evidence in overseas jurisdictions, including the pursuit of bilateral agreements to that end.

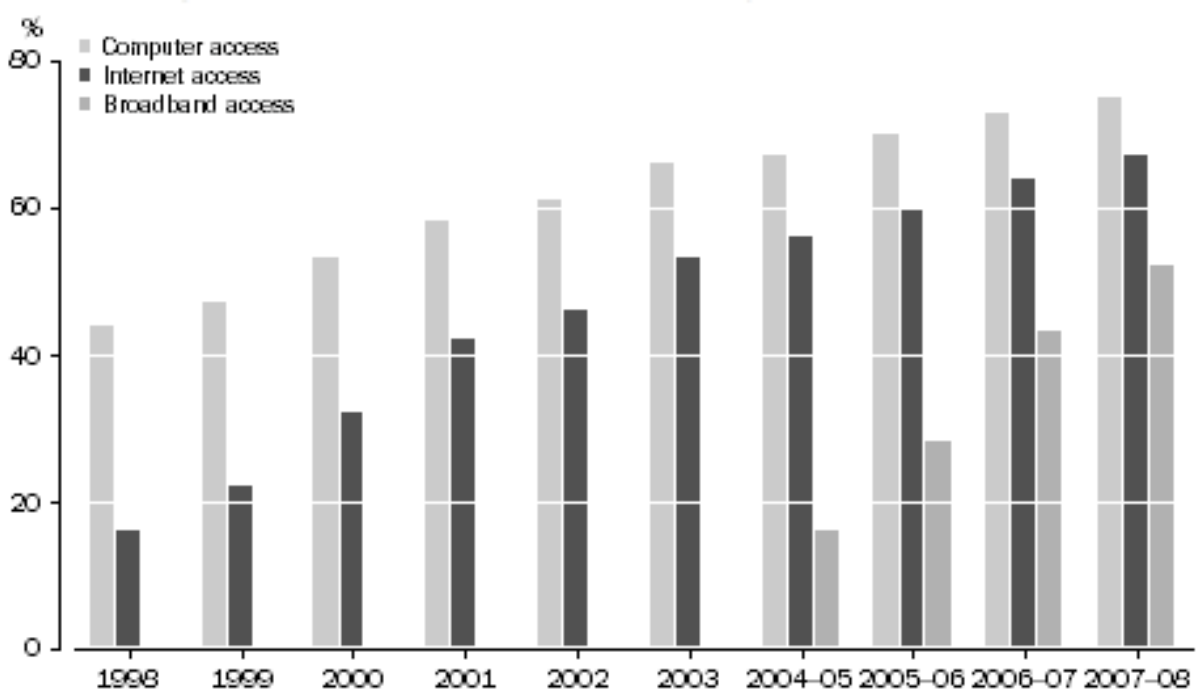
- We believe that the Federal government should establish a single point of contact for Australians to be able to report online incidents, so that the incidence of eSecurity crimes can be better quantified, the threat picture further developed, and offenders more easily identified.

Why understanding eSecurity is important

We suspect that many submissions will point out that Australians are increasingly using the internet, both at home and at work, so we will not dwell long on the subject.

As broadband levels increase, consumers, online businesses, and offline services that use the internet in their back-end operations will rely more and more on the internet. In parallel, criminals will increasingly target Australian computers with the aim of compromising them as the greater bandwidth enables the scaling of their criminal activities. Understanding eSecurity is needed as a first step to minimising the threats, so that Australians can reap the benefits of increased bandwidth.

The Committee would already be aware that a greater proportion of the Australian population now has access to, and uses the internet [as illustrated by the table below]. However, they are doing more than just using these technologies; they increasingly rely upon the internet to conduct their work and enrich their private lives.



ABS: Household Computer or Internet Access, Proportion of all households - 1998 to 2007-08[1]

Australia's Internet penetration rates compare very favourably to other OECD nations.[2]

The Committee would also appreciate that as broadband levels increase, consumers spend more time online, conduct more searches and visit more web pages. As broadband penetration (and speed) rises, so too will the influence of the internet on peoples' lives.

---

[1] 8146.0 - Household Use of Information Technology, Australia, 2007-08 Australian Bureau of Statistics, http://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0

[2] http://www.internetworldstats.com/stats16.htm

The recent announcement by the Federal Government of a National Broadband Network, will see a dramatic increase in the speed of internet connections, with many positive flow on effects. However, it will also introduce more opportunities for crime and victimisation, and increases the urgency of tackling the issues being considered by the Committee. There are three main reasons for this:

- Increased broadband will lead to more computer use, activity, and more access to both good and bad material on the web

- Computers will tend to be "always on", increasing the window of vulnerability for technical compromise

- Australian computers will be more attractive to criminals because the compromised computer will be able to perform a greater volume of criminal activities due to the increased bandwidth

In addition, and perhaps just as important as the amount of business and private use of the internet, is the huge and growing dependence even offline services have upon the internet, making the internet part of Australia's critical infrastructure.

For example, even though we may regard the supermarket as an offline service, the supermarket chains themselves may depend at critical points upon a functioning internet. The security of their computer systems, if disrupted, may affect their ability to stock the shelves with food. Even electricity, water and other utilities have connected Supervisory Control and Data Acquisition (SCADA) systems on the internet to enable remote monitoring and control, but these systems are inherently vulnerable and are now exposed to a range of internet threats.

So, understanding the level and impact of internet threats to the Australian population is important because Australians have chosen to the use the internet for a large and increasing amount of their commercial and private activities.

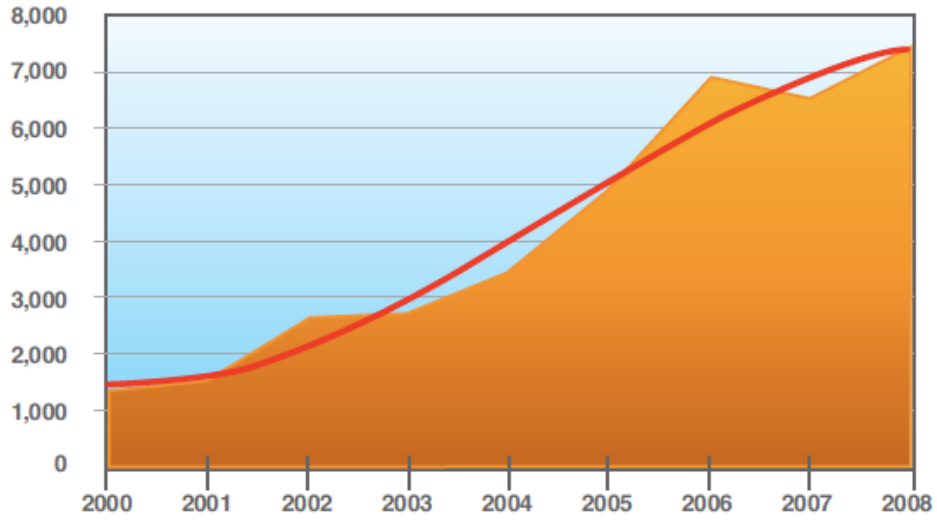
a) nature and prevalence of eSecurity risks

One does not need to spend long in the eSecurity space to learn that there are many people and organisations willing to provide a laundry list of the threats to consumers, businesses and governments in the online space. Infact, there are industries built around just this activity.

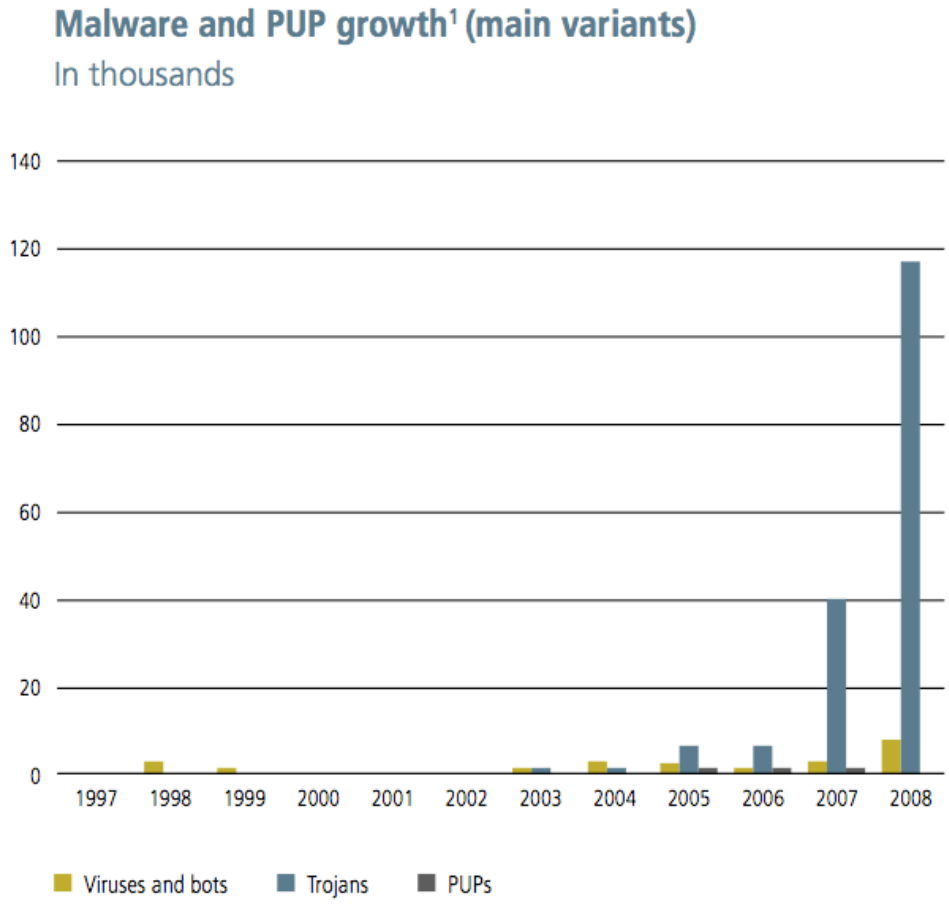
Our view is that the nature of the threat has changed for the worse over the last several years. Some commentators make reference to the "industrialisation" of the online criminal threat. In our opinion, this is a fair use of the term: the threat to online computers is no longer coming from curious intellectuals who traditionally tried to gain access to large central (often government) computer systems. Instead, any and all computers connected to the internet are subject of automated attacks for the purposes of criminal profit.
The aim of the criminal is to either directly steal financial credentials (such as credit card data, internet bank passwords), personal identity information (which may be resold or used), email and telephone lists for the purposes of sending unsolicited communications, the computing power of the compromised the computer to form botnets, and so on.

There are many ways for us to illustrate the continued rise in the criminal online threat.

Below is a chart taken from the *IBM Internet Security Systems X Force 2008 Trend and Risk Report* published in January 2009 which shows the steady climb of vulnerability disclosures in software.[3] These vulnerabilities are potentially used by criminals to attack the computer systems and applications that we use.



The *McAfee Virtual Criminology Report 2008*[4] looks at the unique attack tools used by criminals, which, as with the chart above, shows a growth in the threat:



[3] http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf page 18

[4] http://resources.mcafee.com/content/NAMcAfeeCriminologyReport

The first large scale consumer attacks started around 2003 with bank phishing scams. It was at this point when online criminals showed that they saw as much value in the aggregate (largely unprotected) data on home computers as they did in the (better protected) computer systems of large organisations. If they could steal or trick consumers out of passwords to their bank, they could access the money being protected in the bank computer systems.

The dramatic growth of attacks has created a profitable and increasingly sophisticated criminal industry - where it's easy to buy trojans, access to compromised computers, and to the information gleaned from those computers, on underground trading websites. As in all economies, improving efficiency has increased the abundance and quality of their output (access to personal data), decreasing the price of this data, enabling higher purchasing volumes by criminals.

In many respects online crime is the same as offline crime: the criminal motivations, even many of the methods used, and the ways in which criminals interact, react, learn and change their methods of operation. The key distinctions are that of jurisdiction, volume, perception of anonymity and the perceived (lower) impact of the crime.

Jurisdiction

Clearly, the internet allows criminals to reach victims in all internet-enabled countries, unlike offline crime where there is often a physical nexus between the offender and the victim. With online crime investigations it is not uncommon to have a criminal in one country, victims in a range of other countries, and crucial evidence of the crime in yet another country.

Criminals have benefited greatly from the disparity in laws and the enforcement of laws in certain jurisdictions, but also from the lack of robust timely and scalable international exchange of intelligence and evidence between jurisdictions.

Volume

Internet crime is a volume business. Many millions of consumers/computers can be targeted at one time by a criminal, and, if even a fraction of a percent fall victim, we are left with hundreds, maybe thousands, of incidents. Criminals also leverage the internet in such a way that marginal value crimes - sometimes undetected, and often unreported - carried out against a large number of people can reap high rewards, with little attention from police and regulators.

Perception of anonymity

There is a perception amongst many online criminals that they are anonymous. While this is not always (or often) strictly the case, the perception of anonymity has emboldened would-be internet criminals to engage in online crime.

Impact of the crime

Largely due to the incremental nature of many of the crimes, and also because internet crime is incorrectly viewed as "virtual", this crime type tends to be given a lower priority and resourcing by police than offline crimes of a similar magnitude.

Sadly, there has been much less effort directed at actually understanding the impact of the various eSecurity threats on consumers and businesses: either in direct financial losses or the impact of negative experiences on their lives and activities.

In terms of trying to quantify direct financial cost, there are two recent reports the Committee may care to examine:

- From a consumer perspective, the Australian Bureau of Statistics report *Personal Fraud 2007*, released in June 2008[5] looks at consumer victimisation to scams and identity theft in both the on and offline worlds, estimates, for example, that nearly 500,000 Australians were victims of identity fraud in the 12 months leading up to the survey.

- From a business perspective, the June 2009 Australian Institute of Criminology report *The Australian Business Assessment of Computer User Security: a national survey*[6] looks at eSecurity impacts on Australian businesses, and the incidents they have encountered.

b) The implications of these risks on the wider economy

Clearly, as Australian households and businesses rely more on the internet, the risks from destabilisation of the internet and the victimisation of consumers and businesses increases. It is essential that consumer and business confidence in internet transactions is maintained.

We urge the Committee to recommend to government agencies to carry out more frequent and more robust quantitive studies that place a value on household and business losses due to eSecurity incidents.

---

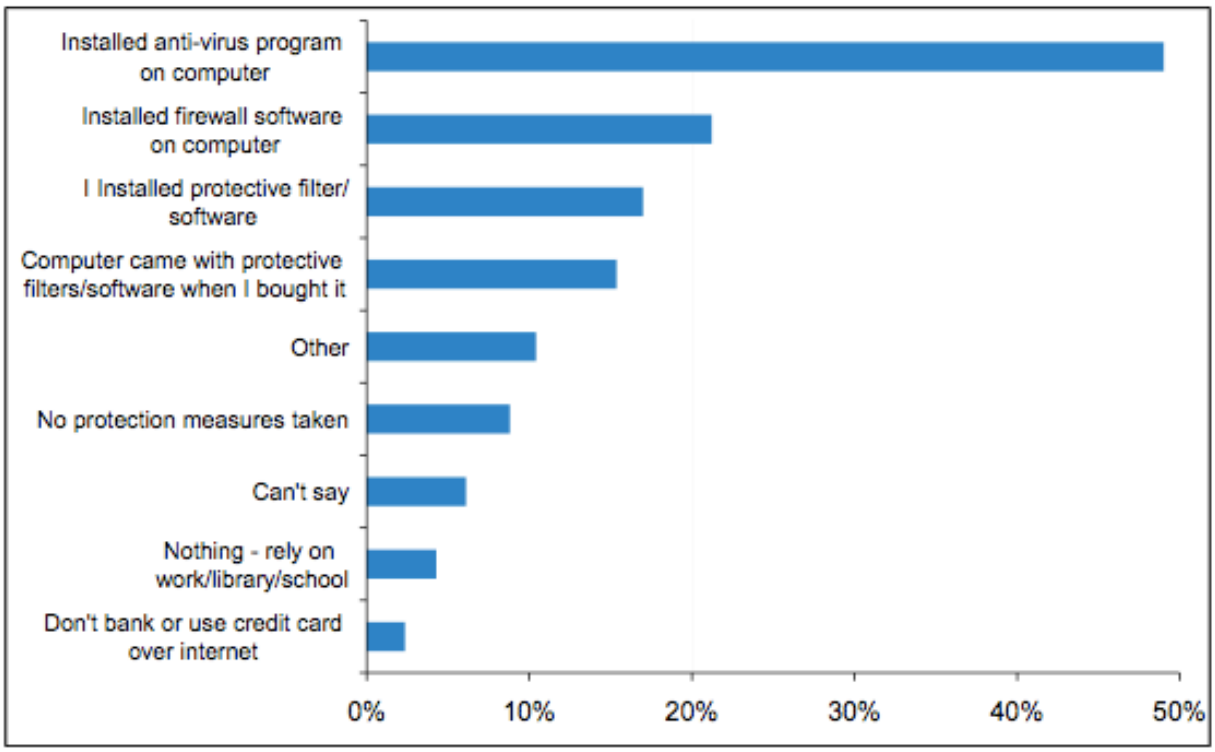
[5] http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/866E0EF22EFC4608CA2574740015D234/$File/45280_2007.pdf

[6] http://www.aic.gov.au/documents/3/B/3/{3B3117DE-635A-4A0D-B1D3-FB1005D53832}rpp102.pdf

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

A March 2009 report released by the Australian Communications and Media Authority, *Australia in the Digital Economy Report 1: Trust and Confidence*[7] highlights an incredible degree of complacency within the Australian internet population, with less than 50% of their survey respondents having installed anti-virus software on their computers, and even fewer people firewalls and other protective measures:

Figure 12. Internet users' measures against online risks and dangers



Source: ACMA-commissioned consumer survey, May–June 2008, internet users aged 18+, (n = 1346).

At the Internet Safety Institute we sometimes refer to this as the "wildebeest theory of defence": consumers reason that they travel in a large herd, so statistically it will be unlikely - they hope - that they will be victimised. Sadly, that just isn't the case with computer crime, especially given the automated nature of the attacks.

Our view is that the Australian internet population is still in the process of maturing when it comes to their knowledge of the threat environment. A fine line needs to be trodden between not talking about threats and scaring users to a point where they wonder about the efficacy of even trying to protect themselves: why should they if all hope is lost anyway?

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

The general observation we would make is that online consumers, and to a lesser degree, businesses, have been left to fend for themselves online.

---

[7] http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf

Education initiatives

Based on the technical,and often undetectable, nature of many of the attacks perpetrated against computer users it would seem hopeless to direct education (or awareness) at the consumer level, but we firmly believe that their are prudent technical security measures consumers must put in place, and more importantly behavioural advice they should follow.

Without being critical, to date government (and most corporate) education efforts have been sporadic and have failed to reach most consumers. From the Federal Government, the two main initiatives are the eSecurity Awareness Week, coordinated by the Department of Broadband, Communications & the Digital Economy, and the Australasian Consumer Fraud Taskforce, coordinated by the Australian Competition & Consumer Commission. Basic marketing and brand theory dictates that a simple message must be delivered multiple times over a sustained period to have any chance of altering consumer behaviour.

We believe that government agencies should expand their engagement of online businesses to help deliver security and safety message to consumers when it is most relevant to them: when they are online. Our experience at eBay showed that it is possible to influence consumers to make online decisions by delivering a relevant message, to the right person, at the right time.

We recommend that the Australian Government undertake a “public health” style approach to changing consumer and business eSecurity habits.

Legislative and regulatory initiatives

We believe that there is adequate legislation in Australia from a criminal perspective.

Loose internet registry practices contribute to phishing and a range of other internet crimes, and internet service providers (ISPs) for too long have taken a hands off approach to helping drive down internet crime. Consideration needs to be given to regulation of the internet space, such as the responsibilities and requirements for ISPs and internet registries to know their customer, and to take action when they believe their networks or services are being abused, or when crimes are reported to them.

While we applaud the enforcement and regulatory approaches to date undertaken by a range of Federal and state agencies and departments, we believe that they have not been scaled to the actual threat environment being experienced online. Spending and staffing has, simply, not kept pace with consumer and business uptake of technology.

We urge the Federal government to take an increased and leading role in developing a national capacity to protect all Australian online. This will require substantial increases in funding and staffing of police, regulatory and policy units, and would benefit from amalgamating several Federal functions under fewer agencies and departments.

Cross-portfolio and inter-jurisdictional coordination

We believe several functions should be amalgamated in Federal government agencies.

We believe more needs to be done in rebuilding linkages between the state and territory police computer crime units and consumer protection agencies and Federal agencies in order to better protect online Australians.

International co-operation

While Australia has been active internationally, when dealing with eSecurity matters it would be impossible to focus too much on international efforts. Australia must continue to strive to reduce the advantage online criminals gain through playing jurisdictional differences.

We urge the Attorney General's Department to explore ways to streamline and improve securing and obtaining evidence in overseas jurisdictions, including pursuit of bilateral agreements to that end.

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

The Internet Safety Institute hopes than ICANN and the Internet Governance Forum, two key international bodies involved in internet rules and stability, increase their efforts to provide a safe and secure internet environment by pursuing policy and technical improvements at the highest levels of the internet.

There is no single institution in Australia (or for that matter anywhere else in the world) which has a whole-of-internet national view of eSecurity victimisation. There are several Federal and state government bodies with a fractional interest, ranging from the Australian Federal Police, Australian Securities and Investments Commission, Australian Competition and Consumer Commission, Australian Communications and Media Authority through to state Offices of Fair trading and state police services.

To their credit the Queensland Police Service have established a pilot portal for some online fraud offences, coordinated with the other state police jurisdictions.[8] We understand that the Queensland Police Servicee is contemplating improvements to the functionality and flow of this service. Media reports attributed to the former Queensland Police Minister suggest that less double handling of complaints, an ability to find appropriate jurisdiction, and greater satisfaction for complainants have made the pilot site a success.[9]

---

[8] http://www.police.qld.gov.au/programs/crimePrevention/eCrime/internet/report/

[9] http://www.police.qld.gov.au/programs/crimePrevention/eCrime/internet/report/

One of the best public-private online crime clearing houses is the US National Center for Missing and Exploited Children.[10] The Internet Crime Complaint Center[11] is a model suited to Australia. Both facilities are well structured and go some way to helping coordinate the actions of the many thousands of US law enforcement agencies. The model would work so much better in Australia because there are fewer jurisdictions and thousands fewer agencies.

We believe that the Federal government should establish a single point of contact for Australians to be able to report online incidents, so that the incidence of eSecurity crimes can be better qualified, the threat picture further developed, and offenders more easily identified.

f) Emerging technologies to combat these risks

We have no specific comment.

Conclusion

We would be happy to provide further information and advice to the Committee. We wish the Committee well in its deliberations.

Alastair MacGibbon
Internet Safety Institute

7 July 2009

[10] http://www.missingkids.com/en_US/documents/CyberTiplineFactSheet.pdf

[11] http://www.ic3.gov/default.aspx