SUBMISSION NO. 45

Internet Society of Australia
A Chapter of the Internet Society
ABN 36 076 406 801

C/- Maddocks, Level 7, 140 William Street
Melbourne, Victoria 3000
Accounts: P.O. Box 351, Glenorie NSW Australia 2157

To: Committee Secretariat

House of Representatives Standing Committee on Communications

By email: coms.reps@aph.gov.au

Sunday, 12 July 2009

INQUIRY INTO CYBER CRIME

The Internet Society of Australia (ISOC-AU) welcomes this opportunity to comment on the Committee's Inquiry into Cyber Crime.

ISOC-AU's fundamental belief is that the Internet is for everyone. We provide broad-based representation of the Australian Internet community both nationally and internationally from a user perspective and a sound technical base. We also consistently promote the availability of access to the Internet for all Australians. Because the Internet is a central driving factor in the demand for broadband, ISOC-AU has a direct interest in the outcomes of the arrangements that will underpin the provision of the NBN.

The importance of the Internet and ICT networks/services for the advancement of a digital economy were recognised in the OECD's 'Seoul Declaration' of June 2008, in the need to:

> …promote the Internet Economy and stimulate sustainable economic growth and prosperity by means of policy and regulatory environments that support innovation, investment, and competition in the information and communications technology (ICT) sector….. The further expansion of the Internet Economy will bolster the free flow of information, freedom of expression, and protection of individual liberties, as critical components of a democratic society and cultural diversity.[1]

Without user confidence in the security of electronic transactions, however, participation in the digital economy will not progress. The security issue was highlighted by, for example, a paper prepared by the OECD as background for its 2008 meeting on the Internet Economy, on the risks:

> These risks are manifold. They threaten personal security—that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organisations, government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit.
>
> Online risks may also impact upon personal safety—by which we mean they may lead to direct physical or psychological harm to the individual. One

[1] OECD, The Seoul Declaration for the Future of the Internet, 18 June 2008, p. 7-8.

high-profile threat is that posed to children by predatory paedophiles, who conceal their true identity whilst using the Internet to "groom" potential victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information.[2]

The Society's response to the Inquiry's individual Terms of Reference are as follows:

1. NATURE AND PREVALENCE OF E-SECURITY RISKS

1.1. *Nature*

As an earlier Australian Parliamentary Inquiry on Cybercrime observed, there is no statutory definition of cybercrime, although a number of definitions were proposed.[3] The first term of reference for this Inquiry, however suggests this Inquiry's focus is on 'financial fraud and theft of personal information, including the impact of malicious software as viruses and trojans', as they impact on consumers and the wider economy.

The kinds of cybercrime that would, therefore, be the subject of this Inquiry include two categories of cybercrime, defined by the Australian Crime Commission in its submission to the 2004 Inquiry:

> The first kind is an offence which is committed using the technology; effectively it is a conventional crime such as fraud which is committed by technological means.
>
> The second kind involves offences which target the computers themselves, and seek to destroy or alter information or data held in them, sometimes with a view to interfering in the processes which that data governs. An example would be an attempt to disrupt a city's water supply by interfering with the computers which control it. The interference can be exercised by a number of means including by hackers, worms, viruses and Trojans.[4]

1.2. *Prevalence*

There are a number of sources of information on the prevalence of cybercrime, both national and international. The Australian Institute of Criminology publishes a number of reports related to the incidence of cyber crime including, for instances, information on the computer incidents experiences by Australian businesses.[5] AusCERT has also looked at both home user awareness of how to protect themselves against various forms of cyber crime and steps they do (or do not) take to protect themselves.[6]

Internationally, The OECD's report on malware includes recent data obtained by the national CERTS on malware in their jurisdiction. [7] The international Anti-Phishing Working Group regularly reports on phishing activity trends. Its latest report for the second half of 2008 shows phishing reports reaching over 34,000 in October 2008, and that rogue anti-

---

2 OECD, Malicious Software (Malware): A Security Threat to the Internet Economy (OECD Ministerial Background Report DSTI/ICCP/ REG(2007)5/FINAL, p. 8

[3] Parliamentary Joint Committee on the Australian Crime Commission, Cybercrime, March 2004, see particularly pp 5-7.

[4] Ibid, p. 6.

[5] See AIC Crime Facts Info No 191, Computer Incidents Experiences by Australian businesses, June 2009, on www.aic.gov.au

[6] AusCERT, Home Users Computer Security Survey 2008

[7] OECD report on Malicious Software, Op Cit, Appendix A.

malware programs had risen by 225%.[8] Indeed, in a UK House of Lords Inquiry into personal internet security in 2006-7, the report found that the level of 'bad traffic is at 170 times the basic level of Internet traffic and is expected to be 500 times the basic level by 2010'.[9]

2. THE IMPLICATIONS OF THESE RISKS ON THE WIDER ECONOMY

The House of Lords' report spells out the variety of risks – from the personal to the economy wide – that cybercrime poses.

> These risks are manifold. They threaten personal security—that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organisations, government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit.
>
> Online risks may also impact upon personal safety—by which we mean they may lead to direct physical or psychological harm to the individual. One high-profile threat is that posed to children by predatory paedophiles, who conceal their true identity whilst using the Internet to "groom" potential. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information.[10]

The OECD Study on malware highlighted the particular dangers of malware to broader threats to national infrastructure and the digital economy.

> Although its economic and social impacts may be hard to quantify, malware used directly or indirectly can harm critical information infrastructures, result in financial losses, and plays a role in the erosion of trust and confidence in the Internet economy.[11]

The particular threat of botnets, or 'zombies' to e-security was explained in the House of Lords report.

> Putting malware onto machines is often done in order to create a "botnet". The individual machines, usually called "zombies", are controlled by a "botmaster" who can command them to act as a group. Botnets are hired out by their botmasters for the purpose of hosting illegal websites, for sending email spam, and for performing DDoS attacks. These activities take place without the knowledge of the individual machine's owner—although normal traceability will enable the source of individual examples of the traffic to be identified. The total number of "zombies" is unknown, but in the course of

[8] Anti phishing Working Group, Phishing Activity Trends Report Second Half of 2008, p. 2
[9] House of Lords, Science and Technology Committee 5th Report of Session 2006-7, Personal Internet Security, Vol. 1 (HL Paper 165-1) p, 15.
[10] Ibid, pp 7-8.
[11] OECD, Malicious Software, Op cit.m p. 7.

> our visit to the Center for Information Technology Research in the Interest of Society (CITRIS) at the University of California, Berkeley, we heard an estimate that the number might be of the order of five percent of all machines, or up to 20 million in total.[12]

Vint Cerf, the 'Father of the Internet', put the figure much higher. He was quoted at the World Economic Forum in 2007 was saying that botnets could undermine the future of the Internet, and estimated that up to one quarter of all PCs connected to the Internet – approximately 250 million – could be infected by Trojans.[13]

3. LEVEL OF UNDERSTANDING AND AWARENESS OF E-SECURITY RISKS

The most recent study by the Australian Communications and Media Authority suggests that Australian young people have a high level of awareness of the risks of Internet use, particularly when involved in social networking on the Internet. Indeed, many parents reported having less understanding than their children on the use of the Internet. However, the Report recommended continuing education, particularly for children and teenagers, in new and engaging ways, as well as programs to educate their parents.[14]

The AusCERT study confirms a general awareness by home users of the Internet on both security threats and some level of awareness on precautions that should be taken. However, that study also chronicles continuing risky behaviour by home users, even though they are aware of the risk. And the report suggests some basic rules that users should follow for safer use of the Internet.

4. MEASURES CURRENTLY DEPLOYED TO MITIGATE E-SECURITY RISKS FACED BY AUSTRALIAN CONSUMERS INCLUDING:

4.1. *Education initiatives*

Information on security risks

The Australian Federal Police, the Australian Communications and Media Authority (ACMA) the Department of Broadband, Communications and the Digital Economy all have websites which, either on their home page or easily found, provide easily understood information on Both the security risks on the Internet and what businesses and individuals can to help protect themselves. There is similar information available on sites such as AusCERT, and private organizations such as Microsoft or SOPHOS.

---

[12] House of Lords, Op Cit., p. 14. For an Australian view of the costs of cybercrime, see Australian Institute of Criminology, The costs of high tech crime, Crime facts info no. 134. October 2006, ISSN 1445-7288.

[13] ZDNet, 29 January 2007, p. 1.

[14] Australian Communications and Media Authority, Click and Connect: Young Australians' Use of Social Media, Qualitative Report Volume 1. Pp 10-11.

ACMA has also developed a range of educational tools designed for various age groups for children, plus additional material for parents and teachers, on both e-security threats and steps that can be taken to address the threats. ACMA also runs a program where children can interact with trained detectives, learning appropriate behaviour when on the Internet.

The Internet Industry Association is also developing a Code of Practice under which its members will educate Internet users on security risks, on the assistance ISPs can give to their customers when a customer's computer is compromised, and on what actions the customer can take.

4.2. *Cross-portfolio and inter-jurisdictional coordination*

While we have no direct knowledge of all cross portfolio and inter-jurisdictional coordination, the conduct of the recent e-security awareness week suggests such coordination exists. The E-security awareness week organising committee membership included representatives from DBCDE, the AFP, Department of Defence, and Attorney-General's Department, as well as representatives from user groups and the private sector (such as Microsoft, MySpace and McAfee). The programs run under the e-security awareness week also involved state governments and other supporting members of the private sector including Harvey Normans and Dick Smith shops.

One government agency that was not, however, a part of E-Security week was the Privacy Commissioner's Office. Given the implications for an individual's privacy from security threats such as identity theft, and the clear implications for an individual's privacy when they put personal information on social networking sites, they might be involved in initiatives such as e-security week in the future.

4.3. *International co-operation*

Clearly, Australian Departments and agencies do cooperate internationally on the issue of cybercrime. This would be true for law enforcement agencies and Government departments, for the regulator ACMA, and for other organizations involved in e-security such as AusCERT.

One area for international co-operation is within ICANN and other bodies such as the Anti-Phising Working Group. There are a number of initiatives that ICANN has identified, that can be followed through, that will contribute to e-security. For example, the Anti-Phishing Working Group (APWG) has identified a practice called 'fast flux hosting' that can be used by criminals or others to make their detection more difficult. The APWG has made recommendations on stopping the practice. There are other recommendations by the ICANN Saafety and Security Advisory Committee (SSAC) on steps DNS registries and registrars can take to improve e-security. Australians are participants in both APWG and ICNN and can promote the adoption of recommendations on improving e-security.

5. FUTURE INITIATIVES THAT WILL FURTHER MITIGATE THE E-SECURITY RISKS

There is no one agency or action that will provide absolute security for Internet use. However, a range of actions both nationally and internationally can significantly reduce security risks for Internet users. Nationally, these include ongoing education programs, targeted particularly at different age groups of children, at teachers and at parents. They include responses both nationally and internationally of law enforcement agencies, regulators and organizations such as AusCERT or GovCERT. Finally, there are the steps individual Internet users can take to educate themselves and their families about actions they can and should take in the interests of e-security.

We will be happy to provide any further comments on issues raised by this Inquiry

Tony Hill
President
Internet Society of Australia

Holly Raiche
Executive Director
Internet Society of Australia