Australian Government

Department of Broadband,
Communications and the Digital Economy

SUBMISSION TO THE HOUSE OF REPRESENTATIVES

STANDING COMMITTEE ON COMMUNICATIONS

INQUIRY INTO CYBERCRIME

2009

Table of Contents

Executive summary

Australians are becoming increasingly reliant on communication services and information technology offered by the digital economy. These technologies and services are changing how we interact and socialise; people can connect and collaborate in previously unanticipated ways, developing new forms of information gathering and social engagement that enrich our lives. The digital economy offers many advantages to individuals, our economy and society.

The Department of Broadband, Communications and the Digital Economy (the Department) understands the importance of supporting Australians to safely and securely take advantage of the opportunities on offer by the digital economy. It recognises that criminal groups are also increasingly looking to take advantage of the digital economy by developing sophisticated methods to target the most vulnerable groups in society: home users and small businesses. The implications of this criminal activity can extend beyond personal or financial loss. A resulting loss of confidence in the digital economy could limit its potential. Similarly compromised computers can be aggregated by criminals into large networks that can be used to attack Australia's critical infrastructure and government networks.

E-security is an important consideration for all users when they go online. However, many home users and small businesses are unaware of the simple steps that they can practice to easily protect themselves. Enhancing the protection of home users and small businesses from electronic attacks and fraud is one of the three main objectives of the Government's E-Security National Agenda. The other two key objectives are to reduce the e-security risk to Australian Government information and communications (ICT) systems and Australia's national critical infrastructure.

The Department is responsible for leading work on enhancing the protection of home users and small businesses. It delivers a strong suite of awareness raising initiatives including:

- the National E-security Awareness Week, which aims to help Australians understand e-security risks and to educate home users and small businesses about the simple steps they can take;
- the Stay Smart Online website (www.staysmartonline.gov.au), which provides information for Australian internet users on e-security issues and the simple measures they can adopt to use the internet in a secure and confident manner;
- the Stay Smart Online Alert Service, which provides information in plain language on the latest e-security threats and vulnerabilities and possible solutions to address them; and
- an E-security Education Package consisting of two interactive, self-learning modules for students in years 3 and 9.

The Department is also partnering with industry to raise the level of community awareness of e-security. Industry is supportive and these partnerships have greatly expanded the reach of the Department's education initiatives.

Finally, e-security is an international issue. In addition to maintaining strong legal, enforcement and education frameworks in Australia, the Government is actively engaging through key international bodies as well as bilaterally to improve the international e-security environment.

Introduction: nature and prevalence of e-security risks

The Department welcomes the opportunity to respond to the Inquiry and considers it to be a timely recognition of the importance of combating cybercrime and e-security threats. This submission provides a general outline of the current and future trends in e-security. It also provides a summary of current Australian Government initiatives implemented by the Department.

This submission focuses on e-security issues rather than cyber-safety issues.[1] This is in line with the terms of reference of the Inquiry, which primarily focus on e-security. Further detail on the Government's work in relation to cyber-safety is available at **Attachment A**.

Cybercrime and E-security

Cybercrime is broadly defined as criminal offences against computer data and systems. Part 10.7 of the *Criminal Code Act 1995* sets out specific offences related to unauthorised access or impairment of data and electronic communications. These offences were introduced by the *Cybercrime Act 2001* and are designed to address the types of crime that harm the security, integrity and reliability of computer data and electronic communications.

Cybercrime is often confused with other offences that are committed with the use of technology. Offences such as fraud and harassment are commonly thought to be cybercrime when committed via new technology. In reality, many of these crimes existed before. The difference is that technology is now used to assist with the delivery of the crime. A typical example of such a crime is advance fee fraud scams, also known as Nigerian money scams. These scams involve fraud rather than cybercrime. Criminals have simply moved to using email to reach their targets from other means of communication such as through the post. It is important to recognise that the crime is the fraudulent behaviour rather than the use of email technology to communicate.

Examples of cybercrime:
- A person gains unauthorised access to online banking or e-mail accounts.
- A website installs spyware software on a person's computer without their consent or knowledge.
- A person damages a file on another person's machine.

E-security is a related term that is often used when discussing cybercrime. E-security is defined by the Government as 'measures relating to the security, availability and integrity of information that is processed, stored and communicated by electronic or similar means.'[2] E-security is a useful term as it encompasses not just the problem of

[1] Cyber-safety concentrates on the broader social and personal risks associated with the use of technology, particularly in relation to children. These include issues such as cyber-bullying, sexual grooming, exposure to illegal and inappropriate content, and the promotion of inappropriate social and health behaviours.

[2] Attorney-General's Department. http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_E-Security

cybercrime but also the broader concept of security, trust and confidence in information systems. For this reason, this submission will predominantly use the term 'e-security'.

Due to the interconnected nature of the internet, e-security is an important issue for all users including government, industry (i.e. large, medium and small businesses) and consumers. There are a variety of e-security risks that users should consider when using online systems. Many of these risks involve malicious software or 'malware'.

Malware
The unauthorised installation of malware on a user's computer is a key method for delivering attacks. These attacks can take the form of denial of service attacks, tracking of the user's browsing habits and theft of personal information and passwords. Malware can also allow a hacker to gain control of a computer.

E-security environment

E-security threats are becoming increasingly sophisticated and targeted. For example, in addition to a significant increase in the proportion of all email that is spam (50% in 2006[3] to around 90% in 2008), around 80% of spam email contains malware attachments or links to malicious websites.[4] The AusCERT[5] *Home Users Computer Security Survey 2008* found that 30% of respondents have clicked on links contained in spam email.

Changes in how technology is used are also resulting in new e-security threats. One example is the increased use of social networking, where user behaviour such as sharing personal information online, can lead to or increase the risk of identity theft and damage to reputation.

E-security attacks are largely driven by personal and financial gain. Offenders range from individuals to sophisticated criminal networks. The ease of scaling activities to reach large numbers of individuals can make these offences attractive to criminal organisations.

Criminal groups are developing increasingly sophisticated methods of attack and are directly targeting the most vulnerable groups in society: home users and small businesses. Instead of widespread, headline-making virus outbreaks, criminals are targeting people's bank accounts, using spam and phishing to gather credit card and financial account information.[6] Phishing is the practice whereby a fraudster who is pretending to be from a legitimate organisation such as a financial institution, sends

[3] ABS. *8153.0- Internet Activity, Australia, DEC 2007*, 24 April 2008 http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_symantec_internet_security_threat_report_ix.pdf
[4] CA. *CA Internet Security Report Forecasts Top Online Threats for 2008*, 9 January 2008, http://ca.com/us/press/release.aspx?cid=163385
[5] AusCERT is the Australian Computer Emergency Response Team, based in the University of Queensland. It is a not-for-profit organisation that provides a range of security-related services on a user-pays basis, including incident response, alerts and advisories.
[6] Symantec. *Norton Online Living Report 09*, p 6

misleading emails requesting personal and financial details from unsuspecting people. Some offenders make use of the 'underground' economy to sell such information.

Example
A recent example is that of a 22-year-old man in Western Australia who used phishing attacks to obtain 56,000 credit card numbers, 53,000 user names and passwords, and 110,000 domain names.[7] The man tried to sell these details to criminals through an underground website.

E-security threats have risen in line with the uptake of ICT within the economy. The following statistics highlight the growing incidence of e-security threats:

- Symantec documented 5,491 vulnerabilities[8] in 2008, which was a 19 percent increase over the 4,625 vulnerabilities documented in 2007.[9]

- According to Verizon's report,[10] more data records were breached in 2008 than any other single year, which was more than the total number of breaches to occur over the previous four years.

- According to Verizon, the price associated with selling stolen credit card data has dropped from between $10 US and $16 US per record in mid-2007 to less than $0.50 US per record today.[11] Symantec reported that because of the large quantity of credit card numbers available, the price for each card can be as low as 6 cents US when purchased in bulk.[12]

According to the Australian Bureau of Statistics, total internet subscribers in Australia increased from over 7.1 million to almost 8 million from the December 2007 quarter to the December 2008 quarter. Of these, non dial-up subscribers increased by 28 percent from over 5.21 million subscribers to 6.68 million.[13]

Like the internet, e-security is transnational. Criminals can easily locate themselves in countries with favourable regulatory environments and reach out to Australian users despite our strong regulatory regime. A large portion of the e-security attacks that impact on Australia seem to be perpetrated from Eastern Europe, with Asia and West Africa suggested as emerging regions.[14] While Australia and many developed countries have strong legal, enforcement and education frameworks in place to improve Australia's e-security, the Government recognises that e-security is a global issue requiring international cooperation. The Department is actively engaging internationally through key international bodies as well as bilaterally. Australia's international efforts are discussed later in the submission.

---

[7] Bolton, Hayley. *$150 fine for nerd who stole 60,000 lives*, Sunday Times, 21 June 2009, p 30.
[8] A vulnerability refers to a case where the integrity of a computer, network or software is at risk of an e-security threat such as malware.
[9] Symantec. *Symantec Internet Security Threat Report, Trends for 2008*, Volume XIV, April 2009 p 10
[10] Verizon. *2009 Data Breach Investigations Report*, 2009, p 32
[11] Verizon. *2009 Data Breach Investigations Report*, 2009, p 5
[12] Symantec. *Symantec Internet Security Threat Report, Trends for 2008*, Volume XIV, April 2009 p 6
[13] Australian Bureau of Statistics. *8153.0 - Internet Activity, Australia, Dec 2008*, April 2009.
[14] Phair, N. *Cybercrime: The reality of the Threat*, 2007, p 7.

Implications for home users, small businesses and the wider economy

Direct impact on home users and small businesses

The biggest concerns for most home users and small businesses are financial fraud and loss of personal information.

According to the Australian Institute of Criminology (AIC), 14 percent of businesses surveyed experienced computer security incidents[15] for the 12 month period ending on 30 June 2007.[16] Thirteen percent of small businesses[17] have experienced one computer security incident or more. The average financial loss from computer security incidents for all businesses that experienced computer security incidents was $4,469. The average loss to small businesses was $2,431.[18] The AIC provides several estimates of the total financial losses from all computer security incidents across Australian businesses, ranging from $595 million to $649 million. For small businesses, the range is from $276 million to $293 million.[19] This estimate gives an indication of the scale of the issue for businesses in financial terms.

Maintaining confidence in the digital economy

Australians are increasingly accessing the internet to do their banking, shopping, social networking and to run their businesses. Government and industry are investing in e-Government, e-Health and e-Commerce to take advantage of this trend and to increase uptake. These activities will increase as Australians have greater access to 'always on' broadband and continue to embrace the digital economy.

The development and uptake of new technology creates opportunities and benefits for all Australians, including home users and small businesses. It is important that they are able to make the most of the opportunities offered by the digital economy in a secure and confident manner.

E-security attacks directed at persons or businesses can impact on their confidence in the digital economy, affecting their use of online financial transactions or other services which require authentication or personal identification. Large scale or widespread attacks have the potential to damage Australia's digital economy. Loss of consumer confidence in the online environment can stifle uptake of online services, limiting the potential benefit to be derived from participating in the digital economy.

[15] Defined as 'any unauthorised use, damage, monitoring, attack or theft of your business information technology.'
[16] Richards, Kelly. *The Australian Business Assessment of Computer User Security (ABACUS): a national survey*, Australian Institute of Criminology Report 102, 2009, pp. 49-50.
[17] A small business is defined as one having 0 – 19 employees.
[18] Richards, Kelly. *The Australian Business Assessment of Computer User Security (ABACUS): a national survey*, Australian Institute of Criminology Report 102, 2009, pp. 69-70.
[19] Richards, Kelly. *The Australian Business Assessment of Computer User Security (ABACUS): a national survey*, Australian Institute of Criminology Report 102, 2009 p. 71.

Protection of critical infrastructure

The e-security of home users and small businesses can also have flow on effects for Australia's critical infrastructure. Compromised home user and small business computers can be aggregated into networks of thousands of compromised computers known as 'botnets'. These botnets can then be remotely controlled by their creators to attack other computers, spread spam emails and malicious software, host malicious websites or conduct denial of service attacks. It has been reported that criminals can hire one thousand compromised computers for as little as $100.[20] Symantec detected an average of 75,158 active bot-infected computers per day in 2008, an increase of 31 percent from the previous period.[21]

The owner of the compromised computer is often unaware that their computer has been compromised or that it is part of a botnet. From a personal perspective, the impact of the compromise may be relatively benign and may not be treated seriously by the owner of the compromised device. However, in the wider context, such compromises can have serious implications for Australia's critical infrastructure when aggregated.

Example
In October 2005, a Dutch organised crime group was apprehended for setting up a botnet of around 1.5 million compromised computers.[22] The attackers used this network to steal credit card numbers, passwords and personal identification details and to blackmail online businesses.

Level of awareness

There are simple steps that consumers can take to significantly mitigate e-security risks. These steps include consumers enhancing the security of their online devices by installing and regularly updating security software and adopting secure online practices and behaviours such as not sharing personal information online. While these steps are effective and easy to practise, evidence suggests that there is a lack of awareness among home users and small businesses about e-security issues.

The AusCERT *Home Users Computer Security Survey 2008*[23] included findings that home internet users' awareness of e-security issues is generally low:

- 8 percent of home users do not update their anti-virus software;
- 30 percent of home users have clicked on links in spam email;

[20] SC Magazine, *'One stop' botnet market uncovered*, 17 June 2009.
http://www.scmagazineuk.com/One-stop-botnet-market-uncovered/article/138624/
[21] Symantec. *Symantec Internet Security Threat Report, Trends for 2008*, Volume XIV, April 2009 p 9
[22] Evers, Joris. *Dutch botnet hackers sentenced to time served*, CNET News, 31 January 2007
http://news.cnet.com/2100-7348_3-6155251.html
[23] AusCERT, University of Queensland. *Home Users Computer Security Survey 2008*, 2008.

- 9 percent of home users with WiFi networks do not secure them;

- 5 percent reported using their neighbour's unsecured WiFi access point to access the internet; and

- 23 percent of home users had confirmed malware infections over the past 12 months – this is compared to only 14 percent of businesses that suffered an e-security incident as surveyed in the *ABACUS Survey*.[24]

The Australian Communications and Media Authority's (ACMA's) recent report, *Australia in the Digital Economy: Trust and Confidence*[25] concluded that Australian internet users should take more steps to mitigate online risks than they currently do and should be more concerned about their online security. Emphasising this point is the report's finding that 9 percent of the internet users surveyed had not taken any protective measures. The report also found that consumers currently place a high reliance on informal methods of training and acquiring knowledge about the internet.

Information asymmetry

The low level of awareness outlined above can be attributed to an information asymmetry between home users and small businesses on the one hand, and software and hardware vendors, ISPs, researchers and e-security experts on the other hand.

The AusCERT *Home Users Computer Security Survey 2008* found that 92 percent of respondents surveyed thought their ISP should inform their customers if they have received information indicating their customers' computers were infected. Sixty-one percent were in favour of their ISP restricting their access via a restricted connection until their computer was fixed. This represents a consumer perception that it is not the home users who should be required to prevent e-security breaches, but rather that it should be part of the service offered by an ISP's internet connection plan.

ACMA has developed the Australian Internet Security Initiative. The Initiative provides data to ISPs about compromised computers on their networks with a view to them informing and providing assistance to affected customers. The program now has 62 participating ISPs covering at least 90 percent of all Australian ISPs. However, preventing e-security threats from affecting computers is preferable to dealing with a computer after it has been compromised.

There is a clear role for the Government to help address the information asymmetry between home users and software and hardware vendors, ISPs, researchers and e-security experts. The Government represents an independent and unbiased source of e-security information.

---

[24] Richards, Kelly. *The Australian Business Assessment of Computer User Security (ABACUS): a national survey*, Australian Institute of Criminology Report 102, 2009.

[25] Australian Communications and Media Authority. *Australia in the Digital Economy – Report 1: Trust and Confidence*, March 2009. http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf.

DBCDE initiatives to address e-security for home users and small businesses

The Department recognises the need to address the low level of e-security awareness and information asymmetry. To this end, the Department delivers a strong suite of awareness raising initiatives. These initiatives sit within the Government's overarching e-security framework, the E-Security National Agenda, which was established in 2001 to create a secure and trusted electronic operating environment for both the public and the private sectors. A 2006 review of this National Agenda set out three priorities to address Australia's e-security in an integrated manner:

(i) reducing the e-security risk to Australian Government ICT systems;

(ii) reducing the e-security risk to Australia's national critical infrastructure; and

(iii) enhancing the protection of home users and small businesses from electronic attacks and fraud.

This e-security policy framework was reviewed in 2008 and a new framework that builds on this approach will be released later this year.

Under the E-Security National Agenda, the Department is responsible for leading work on the third priority listed above. The 2006 review identified the security of home users and small businesses as a key line of defence to secure both critical infrastructure and government networks. The Department undertakes the following activities:

(i) an annual E-security Awareness Week to be held in partnership with industry and community organisations;

(ii) enhancing the Government's e-security information website – www.staysmartonline.gov.au;

(iii) a plain English National E-security Alert Service for home users and small businesses to provide them with up-to-date information on e-security threats and how to address them; and

(iv) an e-security education module for Australian primary and secondary schools.

National E-security Awareness Week

The National E-security Awareness Week aims to help Australians understand e-security risks and to educate home users and small businesses about the simple steps they can take to protect themselves, their families and their businesses online. During this year's Awareness Week, held from 5 to 12 June, the Department partnered with more than 35 industry, community and State and Territory Government partners to hold more than 70 events around Australia, both in metropolitan and regional areas. Five simple messages were promoted through the week:

- Get a better, stronger password and change it at least twice a year.
- Get security software, and update and patch it regularly.
- Stop and think before you click on links or attachments from unknown sources.
- Information is valuable. Be careful about what you give away about yourself and others online.
- Log on to www.staysmartonline.gov.au for further information and to sign up for the email alert service.

The Department is currently evaluating the outcomes of the Week. Preliminary analysis of media engagement indicates that the e-security messages reached a significant number of Australian internet users. Over 170 media articles appeared in print, TV, radio and online about the National E-security Awareness Week. These reached a total potential audience of over four million Australians.

Stay Smart Online website

The Stay Smart Online website (www.staysmartonline.gov.au) is a key element of the Government's e-security awareness raising initiatives. The website provides information for Australian internet users on e-security issues and the simple measures they can adopt to use the internet in a secure and confident manner. The website provides access to a range of resources including top tips, quizzes and guides and is designed to educate users. It also directs parents and teachers to existing resources that will help them protect their children online.

The website received over 8.4 million hits during 2008-09. The website is reviewed and updated regularly so that it remains effective and user friendly.

Stay Smart Online Alert Service

The Stay Smart Online Alert Service provides information in plain language on the latest e-security threats and vulnerabilities and possible solutions to address them. This free subscription based service is delivered through the Government's Stay Smart Online website.

The Alert Service has had over 34 thousand hits during 2008-09. AusCERT, the organisation that provides the Alert Service on behalf of the Department, undertakes a biannual user-survey on the Alert Service. The latest report, produced in April 2009, found that 89 percent of respondents rated the Alert Service as good, very good or excellent. Significantly, 90 percent of respondents said that their awareness of e-security had improved as a result of the Alert Service.

Education Package

To help children understand the importance of e-security, the Department has developed an E-security Education Package consisting of two interactive, self-learning modules for students in years 3 and 9. The objective of the modules is to

provide children with the skills and knowledge necessary to protect themselves online. It is also expected that educating school students will have a positive impact on the awareness levels of parents and guardians, as students share the information they have learned. The modules are available free to all Australian schools through the Government's Stay Smart Online website or on CD-ROM.

The development of the modules involved consultation with a range of stakeholders, including students, teachers and curriculum experts, as well as Commonwealth and State Government agencies. The E-security Education Package was launched this year as part of the 2009 National E-security Awareness Week. Since the end of May 2009, over 400 schools have directly requested CD-ROMs, and the Department has received a large amount of positive feedback.

In addition to evaluating the awareness initiatives, the Department released a request for tender in May this year to develop and implement a repeatable survey designed to collect information from parents, guardians and teachers on cyber-safety and e-security issues. This survey will enable tracking of changes over time in e-security and cyber-safety behaviour. It is envisaged that the survey will be conducted in the second half of 2009 with a report to Government in the first quarter of 2010.

The Department's strong links with stakeholders

The Department's strong links with industry stakeholders enable it to effectively partner with industry to improve the e-security of home users and small businesses. The e-security programs managed by the Department facilitate industry cooperation in an otherwise highly competitive environment. This capacity results in industry and Government working together to enable the Government to deliver its e-security messages to the community at minimal cost.

The Department works closely with key agencies such as the Attorney-General's Department, Defence Signals Directorate, the Department of the Prime Minister and Cabinet, the Australian Security Intelligence Organisation and the Australian Federal Police in a whole-of-government framework. The E-Security Policy and Coordination Committee is the primary forum for Commonwealth Government collaboration on e-security issues. It covers efforts across the Government's current priority areas: government, critical infrastructure and home users and small businesses. The Department is an active member of the Committee. The Department's success in addressing e-security for home users and small businesses also has positive flow on effects for the first two priorities of the E-Security National Agenda which focus on national critical infrastructure and government information systems.

Future trends in the digital economy

Because of the growing incidence of e-security threats, it is important that e-security awareness raising initiatives can continue to be shaped and expanded in accordance with the emerging communications landscape.

National Broadband Network

One facet of the emerging communications environment is the rollout of the National Broadband Network. The new network will use optical fibre to the home and workplace, and next generation wireless and satellite technologies, to deliver high speed broadband services to all Australians. The Department aims to utilise opportunities to integrate e-security awareness raising activities with the rollout and take-up of services of the National Broadband Network. In addition, the Department will regularly review the initiatives to ensure the messages incorporate relevant aspects of the new network.

Convergence

We are seeing the convergence of different forms of technology to provide the same services. The way we communicate and access content is changing. We are increasingly demanding access 'anywhere, anytime'. End users are increasingly able to communicate with each other and enjoy online entertainment over a variety of devices.[26] For example, television shows are being streamed on the web, laptops can be used to make telephone calls and mobile phones can access the internet. These trends will likely be driven by the increasing availability of high speed fixed and mobile broadband and the increasing sophistication of internet enabled devices and web services. As communications and content delivery become increasingly reliant on the online environment, e-security awareness raising initiatives will need to take into account the level of consumer knowledge and understanding of the tools required to securely use this technology.

Regular reviews of e-security arrangements

These and other changes to the communications landscape reinforce the importance of undertaking reviews of e-security arrangements on a regular basis. The Government is conscious of this and regularly reviews its e-security policies, programs and capabilities.

The most recent review into Australia's e-security arrangements was completed in October 2008. The purpose of the Review was to develop a new Australian Government e-security framework in order to create a more secure and trusted electronic operating environment. Some elements of the Review have already been announced, including the development of an e-security ISP code of practice, which is discussed below.

The new Australian Government policy framework for e-security will be released later this year which will articulate the Government's e-security objectives and identify the strategies and capabilities required to achieve these objectives.

[26] Australian Communications and Media Authority. *Fixed-mobile Convergence and Fixed-mobile substitution in Australia Report*, July 2008.

ISP E-security Code of Practice

ISPs are uniquely placed to help create a security culture among Australian internet users by ensuring their customers are aware of the simple things they can do to protect themselves online. For this reason, the E-Security Review 2008 recommended the development of a Code of Practice. ACMA and the Department are working with the Internet Industry Association on the Code's development. The Code aims for a consistent approach for ISPs to inform, educate and protect customers. The development of the ISP Code of Practice demonstrates that ISPs are taking an increasing interest in their responsibility to educate their customers. Key elements of the Code will focus on ISPs:

- providing plain language information to their customers to raise awareness about the importance of e-security and the simple steps Australians can take to better protect themselves online;

- seeking data to identify compromised computers on their networks from sources such as ACMA's Australian Internet Security Initiative, mentioned earlier;

- adopting a consistent approach in informing customers about compromises and how best to address them. While there are 62 ISPs that participate in the Australian Internet Security Initiative, covering over 90 percent of Australian residential internet users, there is no consistency between the participating ISPs in their approach to assist their clients; and

- sharing information and developing mechanisms to minimise the effect of compromises on other ISPs' networks.

It is anticipated that the Code will be operational by December 2009.

International cooperation

The Australian Government's integrated e-security approach recognises the importance of international engagement in addressing e-security challenges. Given the borderless nature of the internet, the isolated efforts of individual countries are not enough to effectively address global e-security challenges. Australia is actively working bilaterally and in key international forums to improve the international e-security environment.

The main objective of this work is to assist countries that may be sources of e-security threats to improve their domestic response and to set in place international cooperative arrangements to address e-security threats.

A summary of current international efforts is set out below. Of particular interest are the Australian Government's anti-spam efforts, which present as a useful model for international cooperation.

Anti-spam efforts: a model for cooperation
Australia's anti-spam work provides a good example of how Australia is able to improve the international e-security environment through international cooperation.

Australia introduced anti-spam legislation in 2003 in response to concerns about the impact of spam on the effectiveness of electronic communication and the costs imposed on end-users. Internationally, this was considered model legislation.

Leading from this domestic work, Australia was able to help foster the establishment of a number of international anti-spam information sharing and enforcement arrangements with other governments and agencies.

The Department, on behalf of the Australian Government, was successful in facilitating a multilateral memorandum of understanding (MoU) with countries in the Asia-Pacific region. The memorandum, known as the Seoul-Melbourne Multilateral Anti-spam Agreement, promotes cooperation on countering spam. ACMA, as the enforcement agency for spam, now continues this relationship on behalf of the Australian Government. In addition to the Seoul-Melbourne Agreement, Australia has the following anti-spam arrangements with other countries:

- Bilateral MOU between Australia and New Zealand;
- Bilateral MOU between Australia and Taiwan;
- Bilateral MOU between Australia and Korea;
- MOU between Australia, the UK and the USA; and
- Australia-Thailand joint statement on telecommunications and IT.

Similarly, Australia is a key contributor to the London Action Plan (established on 11 October 2004), working with law enforcement and government agencies from 27 countries to exchange information, share techniques and address spam related problems, such as online fraud and deception, phishing, and the dissemination of viruses.

With AusAID funding, the Department has conducted spam legislative projects in the Cook Islands, Niue, Samoa, Tonga and Vanuatu, including an enforcement capacity building workshop.

Asia-Pacific Economic Cooperation (APEC) Telecommunications and Information Working Group

The Department, on behalf of the Australian Government, is a key driver of e-security work in the APEC Telecommunications and Information Working Group (APEC TEL) and has led a number of e-security projects including:

- the development of awareness raising materials for small businesses and consumers on wireless security and Voice Over Internet Protocol (VoIP) security;

- a joint project with the United States within APEC TEL on e-security awareness raising which aims to develop a coordinated approach in the region;

- participating actively in projects focused on ICT products and standards and hand-held mobile device security; and

- joint projects between APEC TEL and the OECD on e-security issues. The two groups have developed an analytical report on malware. These projects ensure common policy approaches are developed over a wider number of countries which leads to better outcomes for consumers.

These practical projects have developed e-security capacity in economies throughout the region and have encouraged a best practice, streamlined approach to emerging issues.

OECD Working Party for Information Security and Privacy

The OECD Working Party for Information Security and Privacy (WPISP) has provided an effective platform for pursuing international aspects of Australian communications policy relating to e-security, critical infrastructure protection, authentication, privacy, malware and spam.

Australia currently chairs the WPISP and has been an active contributor in the development of common policy approaches to identity management, malware, critical infrastructure protection, cross border cooperation and privacy. Australia was the primary author of the OECD's Spam Toolkit which provided a multi-pronged strategy to deal with spam. This has improved international cooperation and information sharing on the issue of spam. The WPISP was also the vehicle for launching the joint APEC-TEL/OECD work on malware.

Current work includes consideration of:

- identity management;
- malware;
- sensor-based environments;
- privacy in light of technology, and globalisation; and
- APEC–OECD work on protection of children online.

Future work items may include work on generic best practice guidelines for ISPs to provide assistance to their customers on e-security matters. This work could build and potentially expand on work being done on the proposed Australian ISP E-security Code of Practice.

International Telecommunication Union

The Department, on behalf of the Australian Government, participated in the regional workshop on *Frameworks for cybersecurity and critical information infrastructure protection* in August 2007 in Vietnam. This representation has allowed Australia to play a part in the development of policy documents on these issues for developing countries.

The Department also held an International Telecommunication Union (ITU) workshop on e-security and critical infrastructure protection in Brisbane in July 2008. This provided Australia with an opportunity to bring together Pacific Island countries to share e-security experiences and resources with these countries.

The ITU, with assistance from the Department, commissioned a scoping study on the feasibility of establishing a Computer Emergency Response Team for the Pacific Region (PacCERT).The first part of the study identified a definite need to develop a PacCERT, and found that a growing capability to deliver this already exists within the region. The second part of the study, relating to the implementation of a PacCERT, will be finalised by the ITU in the second half of 2009. This work will include a detailed project plan covering staffing, location, funding, governance and the required linkages with other relevant parties, including domestic law enforcement authorities.

Conclusion

The online environment is playing an ever more important role in our daily lives. Australians are increasingly utilising online technologies to undertake a variety of activities and this trend is set to continue. It is therefore important that Australians can take full advantage of the benefits offered by the digital economy in a secure and confident manner. This is in the interests of both the end user and the wider economy.

The Department is firmly committed to educating home users and small businesses about e-security, and delivers an effective suite of awareness raising initiatives. The Department facilitates industry cooperation in an otherwise highly competitive environment to ensure that its e-security messages connect with the community. The Department continues to tailor its initiatives to suit transformations in the communications environment.

Any overview of e-security would be remiss to not stress the borderless nature of the internet. Isolated efforts of individual countries are not enough to effectively address global e-security challenges. Australia is actively working bilaterally and in key international forums to improve the international e-security environment.

Attachment A: Overview of the Government's Cyber-safety Plan

The internet is an essential tool for all Australians, including children. It is an integral part of our economic and social activities, and a vast resource of information, education and entertainment. The ability to use online tools is a skill for life and provides the means to acquire new skills.

While the internet has created substantial benefits for children, it has also exposed them to a number of dangers, including illegal and prohibited content. Parents rightly expect the Australian Government to play its part in helping protect children online.

Cyber-safety commitment
In May 2008, the Government committed $125.8 million over four years to a comprehensive range of cyber-safety measures, including education, international cooperation, research, law enforcement and ISP filtering.

The Cyber-safety Plan includes funding for:

- the Australian Federal Police's (AFP's) Child Protection Operations Team—$49.0 million over four years for detection and investigation of online child sex exploitation;
- the Commonwealth Director of Public Prosecutions—$11.3 million over four years to help deal with increased activity resulting from the work of the AFP, to ensure that prosecutions are handled quickly;
- filtering—$44.2 million over four years for:
    - ISP level filtering—to develop and implement ISP filtering; including undertaking the live 'real world' pilot in 2008-09; and
    - free PC filters—for the National Filter Scheme to provide free filters until 31 December 2008, and free ongoing technical support until 30 June 2010;
- education and outreach activities—$9.9 million over four years to the Australian Communications and Media Authority (ACMA) to implement a comprehensive range of education and outreach activities;
- websites/ online helpline—$4.3 million over four years to ACMA to improve the current NetAlert website—ACMA will develop a new cyber-safety website with comprehensive up-to-date and age appropriate cyber-safety educational material, and improve the online helpline to provide a quick and easy way for children to report online incidents that cause them concern;
- a Consultative Working Group—$0.8 million over four years for a Consultative Working Group to consider the broad range of cyber-safety issues and provide advice to Government to ensure properly developed and targeted policy initiatives;
- a Youth Advisory Group—$3.9 million over four years for a Youth Advisory Group and online forum to provide advice on cyber-safety issues from a young person's perspective; and
- research—$2.3 million over four years for research into the changing digital environment to identify issues and target future policy and funding.