Senator the Hon Stephen Conroy
Minister for Broadband, Communications and the Digital Economy

Deputy Leader of the Government in the Senate

Towards a framework for cybersecurity and critical information infrastructure protection

Address to ITU Cybersecurity Forum

Lawson Room, Novotel Hotel, Brisbane
Wednesday, 16 July 2008

20 mins

Thank you, [MC TBA]

- Mr Joong-Yeon HWANG [President & CEO, Korea Information Security Agency (KISA)]
- Distinguished delegates and guests

I must begin by apologising for my late attendance today.

Unfortunately, other commitments have delayed my arrival.

But I wish to stress that I appreciate the importance of this meeting for the economies of all the nations represented here today.

This is a very important discussion between neighbours.

The issue of e-security has the potential to disrupt our economies if not properly managed.

But there is also the potential for economic rewards if we can get the policy settings right.

I want to acknowledge that Mr Hwang has already provided a very useful overview of the digital landscape that lies ahead of us.

I will begin with an anecdote that highlights the fact that we can never be too relaxed about online security.

I was interested to see a media release from ICANN earlier this month headed 'Response to Recent Security Threats'.[1]

It outlined the actions ICANN took when its own security policies were breached.

A number of ICANN's own domain names were briefly redirected to other servers for the purpose of capturing traffic for advertisers.

As a result, ICANN has reviewed its own security measures and will begin a review of the security policies used by domain registrars.

[1] *www.icann.org/en/announcements/announcement-03jul08-en.htm*

This incident highlights the fact that even peak bodies—even those that should have the most awareness of e-security measures—are vulnerable to attack if their security policies are not maintained.

None of us can afford to relax.

The Australian Government is committed to working with other nations to create safer online environments.

We see the developing digital economy as offering great benefit to all nations of the world.

The internet is a powerful tool for seeking and storing information and entertainment, but this can work against our interests as much as for them.

We need to set up safeguards against the criminal exploitation of the online world.

We need the software and security protocols to safeguard our financial transactions.

We need firewalls to protect our homes and workplaces against intrusions that invade our privacy and steal personal information and identities.

We need filters and other tools that will ensure our children and families are not exposed to danger or distress during their online activities.

And we need the skilled law enforcement agencies to track undesirable online activities.

True online security and success in the digital economy require the foundations of international agreement on security standards and protocols and a commitment to effectively enforce them.

The purpose in having these common standards and protocols is to build trust and confidence in our online transactions—in banking, negotiation and trade in the electronic marketplace.

Without trust, we are forever suspicious—looking over our shoulder.

It is difficult to make much progress when you are looking backwards.

It is impossible to conclude a business deal when you have no trust in the other party.

Shared standards for online security and a shared commitment to enforce them provide us with a security perimeter around the electronic marketplace.

In a secure environment, we can direct our energies towards creating opportunities for commerce and innovation.

Connectivity around the world is rapidly improving, but consumer and business confidence in the online environment is not keeping pace.

For example, in Australia every second person uses the internet to plan holidays, but only 14 per cent actually book and pay for their trips online.

It seems that low levels of consumer confidence in the security and privacy of transactions on the internet remain significant barriers to achieving the potential of the internet economy.

Last month at the OECD Ministerial Meeting on the Future of the Internet Economy held in Seoul, I committed Australia to supporting the Seoul Declaration.

Among other things, this sets out a shared vision for reinforcing a culture of security and promoting a global information society based on fast, secure and ubiquitous networks.

It specifies the need for policies to strengthen confidence and security, including those that:

- reduce malicious activity online through reinforcing national and international cooperation among all stakeholder communities,

- ensure the protection of digital identities and personal data as well as the privacy of individuals online: and

- encourage collaboration between governments, the private sector, civil society and the internet technical community to enhance the protection of children.

Protecting children online is an important priority for the Australia Government.

Earlier this year, at meetings of OECD and APEC Telecommunications and Information Ministers , I made clear Australia's determination to build a safer environment for children in the digital world.

I called on like-minded economies to work together on cross-border approaches to protecting children online.

Agencies with responsibility for child protection must share and expand their blacklists of illegal material such as child pornography.

Australia's e-security measures

Let me talk briefly about Australia's efforts to ensure online security.

Convergence is revolutionising the ways people are entertained, share information and conduct business.

Mobile phones with internet connectivity, for example are more and more like portable computers.

Organisations are connecting their computers and phones using a single IP network in order to reduce costs.

And we are also seeing the integration of systems that remotely control critical infrastructure services.

The internet and wireless links can operate and control power, water, transport and broadcasting.

With convergence, a compromised home, school or small business computer does not only represent a risk to the identity and personal information of the users.

Because of the access it can provide, it also poses a significant risk to the protection of critical infrastructure and government information systems.

Such compromised computers can be aggregated into huge networks capable of launching attacks on critical infrastructure and government IT systems.

The disruption of critical infrastructure systems by such malicious attacks has the potential to impact the public and private sectors and society as a whole.

The Australian Government recognises that the e-security landscape is constantly changing with the emergence of new and more sophisticated online threats and is delivering a range of targeted initiatives.

We are responding to some real threats.

According to the Australian Bureau of Statistics, in the financial year 2006–2007 Australians lost almost $1 billion as the result of phishing scams and ID theft.

More than 453,000 people lost money

In June this year, I launched the National E-security Awareness Week.

This event helps Australians understand e-security risks and educate home and small business users about the simple steps they can take to protect themselves, their families and their businesses online.

There were three key e-security themes:

- Securing your computer
- Secure social networking
- Securing your wireless connection

During the week, I launched various resources for home users and small businesses and these are hosted on the Stay Smart Online website (*www.staysmartonline.gov.au*).

One of these resources is a free subscription to an alert system. This will provide information to Australian internet users on the latest e-security threats and how to address them.

Another resource is a Small Business Self-assessment Tool.

This tool helps small business to assess their security requirements and adopt appropriate practices and measures to improve their online security.

The Australian Government is also developing an e-security education module for Australian primary and secondary schools which is scheduled to be launched in Australian schools during the first semester of 2009.

There are clear linkages between e-security and e-safety.

The awareness initiatives that will help young Australian protect themselves against e-security threats will also assist them in being safe online.

Therefore, adopting secure online behaviours and technologies assists in protecting against e-security and e-safety threats.

In this way, e-security has many synergies with the Government's comprehensive cyber-safety policy. This includes mandatory ISP filtering of illegal content, as well as international collaboration, research, law enforcement and educational programs.

International engagement

Given the borderless nature of e-security threats, the Government is mindful of the importance of working at an international level.

Effective, future-focused e-security measures are a global concern.

The Australian Government therefore participates in a range of International forums on this issue.

Australia is an active participant on e-security issues in APEC.

Earlier this year I attended the APEC Telecommunication Ministers meeting in Bangkok.

This work is recognised by many economies.

For example, Australia is working with the United States in leading an awareness raising program within the APEC region.

As I mentioned earlier, I have also recently returned from the OECD ministerial meeting hosted by Korea last month.

This was the first meeting of OECD Ministers in ten years.

The OECD is leading the way in collaboratively addressing e-security risks and threats.

It is a forum that enables international organisations to work together on the global issue of cybersecurity.

One area that requires coordinated international action at in the Asia-Pacific region is the fight against spam.

Spam is a major impediment to participation in the information economy for the nations of this region.

About 70 per cent of all email traffic is spam.

The sheer volume of it threatens to overload Pacific networks.

Spam is also increasingly a vehicle for other major e-security threats, such as viruses.

And, as it erodes trust and confidence in the use of ICT, spam further increases the digital divide.

Australia's anti-spam legislation is considered world's best practice.

With the support of AusAID, the Department is undertaking anti-spam legislative projects in Niue, Samoa and Vanuatu.

These projects build on recent, similar work in Tonga and the Cook Islands.

It seeks to maximise the opportunities for Pacific Islanders to participate in the global information society by reducing the impediment to participation posed by spam.

This activity has a number of interrelated objectives:

- to improve the capability of Pacific Islands countries to engage in e-commerce

- to maximise the potential for a consistent legislative and regulatory approach developing in the Pacific region

- to enable Pacific nations to act against spam both domestically and internationally, and

- to reduce the potential for the establishment of spam havens in the region that undermine global efforts to minimise it.

ITU workshop

This ITU workshop today brings together experts to discuss both international and national approaches for improving cyber-security and critical infrastructure protection.

My Department—the Department of Broadband, Communications and the Digital Economy—has worked closely with the ITU to develop the Forum agenda.

Such international engagement not only ensures we have access to international best practice, but that we contribute to the work that supports global efforts in e-security.

The OECD's work on e-security will assist the ITU to access international best practice.

It will help the ITU to contribute to global efforts.

The ITU is uniquely placed to support developing countries that are in the initial phases of formulating cybersecurity strategies.

PacCERT announcement

I want to turn now to an initiative that I can announce at this event.

As we know, collaboration between government, industry and users is crucial when developing strategies to deal with e-security threats that undermine confidence and trust in the online environment.

The borderless nature of the internet means that this collaboration must be global.

A key part of an effective e-security strategy is informing key stakeholders in the ICT community about the latest e-security threats.

Computer Emergency Response Teams—or CERTs—are a crucial aspect of a broader e-security strategy.

CERTs provide a coordinated approach to informing key stakeholders of the latest cyber-threats and assist in developing coordinated responses to these threats.

My Department and the Attorney-General's Department have held, over the past 12 months, a series of informal discussions with key stakeholders in the Pacific ICT community.

We were keen to learn how best to support them to set up a Pacific-based CERT.

It became clear that one way we can help is by undertaking a study to determine the best path forward.

I can announce today a scoping study into the creation of a Computer Emergency Response Team in the Pacific.

This is a result of Australia's contributions to the ITU and collaboration with AusCERT.

It is important that all countries, including countries in the Pacific region, are able to access computer incident prevention, response and mitigation strategies.

Only then can they respond in a timely manner to threats affecting or involving their telecommunications networks.

The success of a CERT for the Pacific region will depend greatly upon agreed protocols and standards and a commitment by all participating nations to maintain and enforce them.

Conclusion

It is clear to all of us, I am sure, that success in the digital economy requires more cooperation—not less.

The benefits of the digital economy will flow only to those nations that embrace its potential for establishing access and commonality in purpose.

This does not mean relinquishing national identity or sovereignty.

Rather, it requires engagement in the global marketplace on terms that inspire trust and confidence and in international forums such as this.

This meeting is a firm step down that path and I thank you for your contributions.

Thank you.