First Assistant Secretary Cyber and Information Security (FASCIS) Speech for Parliamentary Library Guest Lecture Series

15 August 2012

"Cyber Security"

Introduction:

- Good afternoon. I am pleased to have the opportunity to speak to you today about cyber security.
- In the short time I have, I'm going to talk about the cyber threat and go through some things we can all do to help manage it.

About DSD:

- But before I begin, I would like to tell you a little bit about the Defence Signals Directorate. We have two missions. One is collecting foreign intelligence by interception. The other is information security - working to stop other people doing the same to us. So, we are both a foreign intelligence and information security agency and these functions are defined in the *Intelligence Services Act.*
- Given those two functions, you can see that DSD is both the poacher and gamekeeper of information. Hence our mission statement: reveal their secrets, protect our own. It is the 'protecting our own' mission that I will talk to you about.
- DSD was established in 1947 to exploit foreign communications and be responsible for communications security in the Australian Defence Force and government departments.
- In its first 50 years, DSD's focus on information security was to protect the nation's secrets, primarily for Defence, our diplomats and our intelligence agencies.
- While DSD still protects the nation's secrets, the landscape in which we operate has dramatically changed in the last 10 years. Advances in technology have transformed the way we work and live, and our role has broadened to assist government agencies to protect sensitive information and to help other government agencies help the private sector.
- So, what is sensitive information? It can be of strategic, economic, commercial, or personal value. Such information requires protection, and it is because of this reason that cyber security is one of Australia's top national security priorities.

- Cyber intrusions on government, critical infrastructure and other important networks are a real threat to Australia's national security and have the potential to undermine public and international confidence in Australia as a safe place to do business.

National Security Priority of Cyber security

- At DSD, a common response we hear at all levels is "my information is not classified – no one would be interested in it" or "I'm not that important, it would never happen to me".
- Well, in some cases, this may be true, but I can assure you that from our experience, that is an unwise assumption to make. Someone out there is generally interested in our information, and perhaps not in a good way.

Scope, nature and trends the cyber environment

- But let's take a step back and look at cyberspace – what does the environment we all operate in look like?
- Cyberspace is where the world conducts its business.
- Earlier this year, CISCO estimated that by 2016, the number of people connected to the Internet will be 4.5 billion. Global IP traffic has increased eightfold over the past five years, and will increase nearly fourfold over the next five years.
- CISCO also reported that by 2016, the world's 19 billion global network connections will generate 1.3 zettabytes of data.
- In fact the number of devices connected to IP networks will be nearly three times as high as the global population by 2016 – that's our kindles, our tablets, our laptops. By then too, the gigabyte equivalent of all movies ever made will cross the global internet every three minutes.
- According to the Australian Bureau of Statistics, there were 11.6 million Internet subscribers in Australia at the end of last year
- Today, governments, industry and the public alike all rely on communications technology in their everyday lives.
- Many of our everyday services are now being conducted over the Internet as a matter of course. Technology, such as the growth of smartphones, makes it easier for us to access information on the run.
- Online has become a primary means of interaction. We just have to look at the rapid uptake of Facebook, Twitter and LinkedIn to see the prolific nature of online communications and impact of social media.

Defining the threat

- We can all agree - the internet is a good thing. But – and you knew there would be a ‘but’ – advances in technology can be a double-edged sword.
- Australian computers – whether government, commercial or personal – are facing an unprecedented level of cyber intrusion activities.
- The cyber threat comes from a wide range of sources including:
    - individuals (doing it for profit or fun);
    - issue motivated groups (who do it to protest or for propaganda);
    - organised crime syndicates; and
    - state-based hackers.
- State-sponsored intrusions are the biggest threat to networks, which makes sense when you think about the resources they have available.
- In practice, a least 65% of cyber intrusions on Australian computers have an economic focus. Actors are looking for information on Australia’s business dealings, its intellectual property, its scientific data and the government’s intentions.
- The most common method used to gain access to your information is socially engineered emails.
- These contain malicious attachments or web links, which are increasingly tailored to appeal to you personally, and a specific interest of yours.
- Unbeknownst to us, hackers are researching us online – our profiles, our professions, our personal interests and our families – to see what sort of information we are interested in. They will then tailor content to entice us to open a malicious attachment or follow embedded links to malicious websites.
- Once that attachment is opened, or the link is clicked on, an attacker can install malicious software, such as putting a back door into your computer or mobile device.
- We hear reports of hacking in the media every day. Almost all government and large private sector organisations have been affected by cyber security incidents. In 2009, the Cyber Security Operations Centre was established to address this threat. The centre is located within the Defence Signals Directorate and also comprises staff from DIO, ASIO, the AFP, and CERT Australia.

  In 2011, the Cyber Security Operations Centre received reports and identified 1259 cyber security incidents.

- 313 incidents were considered serious enough to receive heightened assistance from the Cyber Security Operations Centre.
- But before I go into detail about the Centre, let's talk about what you as a user can do to protect yourself.

What can you do about it?

- Typically, I get asked the same three questions every time I am asked to speak on cyber security.
- *Number 1, socially engineered emails*. What do they look like, and what can we do about them?
- Successful cyber intrusions are as much about exploiting people's behaviour as they are about exploiting technology.
- One of the best defences against social engineering is for users, like you, to be alert and aware and take some basic precautions, because if technical measures fail, you are the last line of defence.
- So be suspicious of unsolicited phone calls or emails asking you to do something. Do not follow instructions from someone who rings or emails you to tell you that your computer has 'technical problems', unless you can prove they are from your internet service provider.
- You should also check out an email before you open it or click on any attachments or links. Look for signs that an email may not be legitimate, such as:
    - The language used. Is this what you would expect from the sender?
    - Are there inconsistencies in the grammar, spelling, or punctuation (or a combination of all three)?
    - Does the email seem suspicious or from someone you don't know?
- A malicious document, such as an attachment or a website that has no, little or unexpected content, attachments that flicker or flash when opened; or dialogue boxes that close before you've had a chance to read them, may all be indicators of a virus or malicious software.
- These may just be spam, or they might be trying to install a virus or malicious software on your computer. If someone has sent you an email that you think is a bit strange, consider deleting it before you open it.
- But if you think you may have accidently opened a malicious file, there is something you can do about it.

- If you're using a work device, report it to your organisation's IT security staff. If you are using your own personal device, delete the email and run anti-virus software to scan for possible viruses or Trojans.
- The second most common question I am asked is, can I use webmail for work purposes?
- DSD strongly advises against using webmail, such as Hotmail or Gmail, for work. The use of such services may bypass some of the security measures that have been put in place to detect, and respond to malicious activity.
- And finally, *mobile devices*. I get a lot of questions about mobile devices.
- If you want to use mobile devices such as tablets (iPads), smartphones (Android or Apple), for business purposes, or to connect to your corporate network, please talk to your organisation's IT security staff first.
- And what about using mobile devices when travelling overseas? Like you would with your passport and credit cards, special care should be taken in protecting these items.
- Don't underestimate the lengths that foreign intelligence services and other actors will go to, to get steal your device and the information that it may hold. It's a treasure trove of information on you, your work, your life and your contacts that they can use to target you back in Australia or anywhere you go.
- If you choose to take a mobile device overseas, we advise you do so without storing sensitive information on it, unless absolutely necessary.
- If necessary, we would then strongly recommend that you not let your phone or device leave your control, just like your credit card, or always ensure it is handled by someone you trust.
- And finally, you should always assume that someone is able to listen in on your calls while you are overseas.

The role DSD plays

- So, we've spoken about the environment, the threat and what you can do about it. Let me now move on to the final piece in the cyber security puzzle – the Cyber Security Operations Centre at DSD and what we can do to help you.
- The Centre has two main roles. The first is to provide government with a better understanding of sophisticated cyber threats against Australian interests. The Centre identifies malicious activity conducted by sophisticated foreign hackers by using advanced analytic capabilities and techniques.

- Our workforce includes staff who are highly trained in computer information technology and analysis. We also have technical specialists in the Centre who can detect evidence of sophisticated cyber intrusions, and they frequently do.
- This, together with DSD's high-powered computing resources, ensures the Centre is able to process large volumes of data and identify cyber threats.
- The Centre's other function is to provide advice and assistance regarding cyber events across the Australian government and systems of national importance. CSOC staff work with external government agencies to improve the security stance of their networks. They also work with agencies whose networks have been compromised to help mitigate against further cyber intrusions.
- Traditionally, DSD's information security advice was informed by a conservative and prescriptive mindset. We tended to focus on "no – you can't do that, you mustn't use that, and you shouldn't do it like that".
- But we can't always say no. It is not in line with current thinking on this issue.
- I'd like to think that the new underlying principle of DSD's information security mission is to empower - instead of telling people they can't take up advances in communication technology, I would rather encourage good decision making when they do so.
- We can't stop people from using the latest and greatest. What we can do is enable them to use it in the least risky way.
- Now, I often use a phrase by the current Chief of Navy, Vice Admiral Ray Griggs, during his work on the Defence Strategic Reform Program. Ray used to talk a lot about the challenge of moving from a mindset of "we can't do that because" to a mindset of "we can do that if".

Conclusion

- In closing, cyberspace is a 24 hours a day world. This is one of the great benefits of modern technology – cyberspace is always open for business. But this also brings great challenges to those of us who guard our electronic information.
- The best piece of advice I can leave you with is that while there is a threat out there, there are things we can all do to help minimise it. Everyone has a part to play in protecting information.
- If you are using your work device, remember to use your organisation's IT security staff as resources when you're unsure of something.

- On your personal devices, remember to update your operating system and applications frequently and install reputable anti-virus software and set it to update regularly. And if you have concerns, call the vendor’s customer support number, your ISP... and if all else fail, call the 1300 CYBER1 for assistance.
- DSD has further information on the points I’ve raised on our public website (www.dsd.gov.au). I would encourage you all to have a look.