

## **DSD Security-In-Government speech**

### **'Cyber Security – Beyond the Firewall'**

- Thank you Joe and my thanks also to the Attorney-General's department for incorporating a cyber security stream into this year's Security in Government conference.
- The word cyber is used a lot today and we see many definitions of cyberspace. At the Defence Signals Directorate we prefer a simple definition of cyberspace and that is "the Internet and everything connected to it".
- The title of my talk today is "Cyber Security- beyond the firewall".
- So what does this mean? Well, for me, it means that cyber security has a range of dimensions, and not all of these are the obvious, technical ones.
- So today, I'll set the scene, providing some context for cyberspace and the cyber threat. And I will discuss cyber security in the context of four key threads that my organisation currently focuses on. These threads are;

Intelligence

Technology

People &

Policy

- Cyber security is a field that demands collaboration and while the Defence Signals Directorate has a lot to offer, we cannot possibly tackle the cyber security challenge alone.
- If you leave here today with only one message, I hope it would be that while the cyber threat is real, there is something we can all do about it.

## **Introduction**

- At DSD we are both a poacher and gamekeeper. I like to tease my colleagues on the intelligence side of our business by saying that the security role is way more difficult than intelligence.
- But it's actually true. In intelligence, you only have to be successful once to deliver a moment of success. In security, it is very difficult to know how successful you've been.

- We've been a security agency for over 60 years, but in the last decade especially, this role has changed quite dramatically. To understand how, and why, you only have to look at the advances in technology and the growth of the Internet.
- In understanding the cyber threat, we need to think about the context. Just look at the Internet. At the end of 2000, there were around 361 million users worldwide. That figure is now well over 2 billion and growing.
- In 2003, according to Forrester Research, there were approximately 500 million connected devices worldwide.
- At the end of last year, Cisco estimated the number of connected devices increased to 12.5 billion. To put that in perspective, that is the equivalent to roughly two devices per person on Earth.
- It is important to note that the 12.5 billion devices we're talking about here go far beyond devices we hold in our hands. This is about device-to-device and "machine-to-machine" communications including everything from RFID tags attached to cattle or shipping containers.

- This also includes air traffic control systems and wireless sensors now being deployed as we build out Smart Grids to distribute energy more effectively.
- And Cisco predicts there will be 25 billion devices connected to the Internet by 2015.
- Today, over 80 per cent of Australians have access to the Internet, 40 per cent of them own more than one mobile phone, and more than half of them use their phone for email and web browsing.
- Social media is also changing the way we work, play and communicate, and the incentive to share more personal data on the internet is increasing. People are demanding more flexibility in their working arrangements – they want to work remotely and they often use their own devices.
- For Government, and for the private sector, this means that they want to remotely tap into networks, most of which contain a great deal of information that needs to be protected.

- All of this illustrates the evolving nature of the Internet and computer networks. A computer network is no longer contained in the perimeter of a building – it extends out over the Internet, to a range of mobile devices, and it can access information physically stored almost anywhere in the world. Almost everything is connected and is online.
- Let me be clear – the internet is a good thing.
- But – and you knew that there would be a ‘but’ – there is potential for harm. People with ill-intent, cyber criminals, issue motivated groups and foreign intelligence services now have the means to disrupt or steal information covertly on a scale that we could not have imagined 10 years ago.
- We see new reports of hacking in the media every day. In April this year, the SONY PlayStation Network was hacked, resulting in the theft of the personal information of 77 million account holders. I was one of them – my son uses the SONY playstation network. SONY now faces a class action lawsuit for the loss of personal information. I’m not picking on

SONY, but it is one of many examples of what is happening today around the world.

## **The Intelligence Thread**

- So let's look at our first thread of cyber security – intelligence.
- We have a very good understanding of the cyber threat from intelligence, but there is still more we need to know. And we are working that hard.
- The cyber threat comes from a wide range of sources, including individuals, issue motivated groups, organised criminal syndicates, as well as state-based hackers representing a broad range of skills and varying levels of sophistication.
- It is reasonable to assume that information held on Australian networks is attractive to intelligence services of foreign governments and organised criminal syndicates.
- We don't have as much information on the cost of cyber crime in Australia, but one recent Australian Federal Police estimate put it at over a billion dollars every year.

- I can tell you that a lot of this activity has an economic focus, looking for information about Australia's business dealings, its intellectual property, its scientific data and the government's intentions.
- As you know, cyber security is a national security priority for government and that's not just about classified information being accessed. We need to make sure that our systems are secure so that we can guarantee the integrity of the information and the services which we provide.
- But we can't do this alone.
- For example, I encourage all government departments to report cyber incidents to DSD. This ensures, we can help you, further develops our understanding of the threat and more importantly what we can do about it.
- While intelligence is important and our understanding of the cyber threat is critical, cyber security it not just an intelligence problem.

## The Technology Thread

- So let's look at our second thread of cyber security – technology.
- Most people have no trouble thinking about cyber security as a technical problem – and this is where the Cyber Security Operations Centre comes in. The Centre has two main roles:
  - provide government with a better understanding of sophisticated cyber threats against Australian interests, &
  - coordinate and assist operational responses to cyber events of national importance across government and systems of national importance.
- The Centre's operations also complement DSD's other information security activities. It identifies malicious activity conducted by sophisticated foreign hackers by using advanced analytic capabilities and techniques. Our workforce includes staff highly trained in computer information technology and analysis.

- This, together with DSD's high powered computing resources, ensures the centre is able to process large volumes of data to identify cyber threats. Our people work very much in that slim area between the difficult and the impossible.
- Our technical specialists in the Centre can detect evidence of sophisticated cyber intrusions and they frequently do. My people work with agencies whose networks are at risk to improve their security stance, and they also work with agencies whose networks have been compromised to help mitigate cyber intrusions.
- So, while the threat is real, the good news is, we have a number of technical measures to mitigate the risk.
- Last Friday DSD updated the 35 Strategies to Mitigate Targeted Cyber Intrusions.
- The update is based on our operational experience.
- Like the previous version, the strategies are listed in order of effectiveness.

- Over 70% of the incidents that the centre responded to in 2009 could have been prevented if agencies had implemented the top 4 of the 35 strategies. Today, with the release of the revised strategies and the advances in ICT security by industry, we estimate it to be closer to 85%.  
That's a technical fact.
- I was pleased to read a post about our update on the SANS website, and I quote “an updated list of 35 mitigations that are the best hope for stopping or mitigating the targeted attacks”. So don't just take my word for it.
- While new strategies have been introduced, the top four mitigation strategies remain unchanged, indicating that they are still paramount to achieving good cyber security.
- Some changes I'd like to highlight include: User education has moved up from number 31 to number 8. This reflects how important user education is in the fight against cyber intrusions. With this change comes a more holistic approach to cyber education.

- Where once it was recommended that you educate your users on spear phishing emails we now recommend education in a number of areas:
  - Selecting stronger passwords and not reusing these passwords across systems;
  - Thinking about the websites you visit at work; and
  - Not using USB devices and other media not corporately supported.
- Patching applications is now the number one mitigation strategy. It was number two. This change was made to highlight the increased exploitation of applications such as PDF and Flash Player as opposed to patching operating systems such as Microsoft Windows.
- We have some copies here today at DSD's Booth in the Exhibition Hall – but I encourage you to visit our website and download a copy so you can start a conversation in your organisation about improving cyber security.
- We have also begun to produce supporting documents to help organisations effectively implement the top four mitigations strategies. These documents include detailed technical information on application

whitelisting and minimising the number of users with domain or local administrator privileges. And a supporting document on patching is under development.

- Technology and technical solutions are really important but, cyber security is not just a technical problem. Incidentally, I used to be an engineer, so you can imagine that I needed therapy to be able to say this out loud.

### **The People Thread**

- So let's look at our third thread of cyber security – people.
- Technical and even operational expertise is only one piece of the picture. DSD is an intelligence agency. And we know, as an intelligence agency, that obtaining information by stealth often depends on exploiting peoples' behaviour as much as it does on Gucci technology.
- I spent most of my career in DSD on the intelligence side. Some of our most successful operations have used great, innovative technology.

- But these operations depended just as much on our targets doing silly things or not thinking about security. Using really simple passwords. Using the same disk to transfer information back and forth between different networks. Playing video games or visiting dodgy websites on their work computer.
- The hackers know this too, of course, and that's why one of the things we're seeing is a huge increase in the sophistication and frequency of phishing emails. These are not your average Nigerian bank scam emails.
- The emails might appear to be from someone you know, even a boss. They will have convincing-looking commercial logos and signatures on them. Or they might target a specific interest of yours.
- The hackers are researching you online – your profile, your profession, your personal interest and your family – to see what sort of information you might be interested in.
- The starting point dealing with this is the understanding that we all share the risk. Last year we spent a lot of effort helping people understand that

the “threat is real”. This work continues, but this year we also working to help them “comprehend the risk”.

- When I’m briefing senior execs on this, I always ask them to start with some fairly basic questions about the value of their information, and the consequences of a major data loss or spill. And whether their staff understands how they might be targeted.
- My point is that you should never assume that information about you or your work is of no interest to anyone, and if the computer that holds that information is connected to the Internet, then it is a potential target for cyber intrusion.
- I’m not trying to be alarmist or defeatist in telling you this. And DSD is not in the business of telling people that they can’t take advantage of technology. That is not an option, and in any case, I wouldn’t want to.
- Security is an intrinsically negative business, but instead of telling people what they can’t do, I prefer to concentrate on telling them that they can do good things with this technology.

- But, they need to make good decisions when they do so. And they need to understand that it's not just a problem for their IT staff.
- It's not just our stakeholders who need to change. DSD is changing its own mindset on security. Traditionally, information security, like physical security, has been informed by a conservative, prescriptive mindset. We tend to focus on the 'No' – you can't do that, you mustn't use that, you shouldn't do it like that.
- This year, I have often used a phrase used by Ray Griggs during his work on strategic reform. 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".
- One example of this change is our recent Cloud Computing Security Considerations paper where we encourage agencies to embrace cloud computing with their "security eyes" wide open.
- This is exactly the mindset that I think we ought to be applying to cyber security. And it's not like we really have a choice about this. We can't always say no. We can't keep saying to seniors "No, you can't have an

iPad at home to look at protected information.” We harm our reputation by this, and in the long run, we do no good anyway.

- We can't stop people from using the latest technology. What we can do is enable them to use it in the least risky ways.
- Of course, cyber security is not just a people and behaviour problem.

### **The Policy Thread**

- So let's look at our fourth and final thread of cyber security – policy.
- If you think about what policy is, it's really just a formal record of how most people think we ought to do things. But if you don't get the “why” message out there, and if you don't frame it in a way that most people can understand, then the policy isn't going to be as effective as it ought to be.
- I confess messaging is not something that we've always been consistently good at, which is probably pretty inevitable when you have a critical mass of highly introverted, technically talented people concentrating on the ones and zeros. Speak geek, or get out of the server

room, seemed to be the dominant mindset, at least it did in the circles I moved in.

- But we are changing. My favourite example comes from a few years ago, when some of my technical staff responded to a major security incident. When my technical director sat down with the network operators, the first thing he was asked was “what can we do to stop this?”
- My tech director wrote down a list of things to do, right here, right now. In fact, I think he initially wrote it on the back of a coaster.
- Eventually, this list became a flagship document “35 strategies to mitigate targeted cyber intrusions”, which DSD first published in early 2010.
- Now, everything in the 35 strategies actually maps back to technical advice that DSD has already published in its Information Security Manual, which is a detailed document that forms the basis of our ICT security policy.
- The thing is, though, that the 35 strategies document appeals to a much wider audience than we could hope to do with the Information Security

Manual. Because it basically takes these technical solutions and turns them into really simple statements which say that there are things you can do, right here, right now, to improve your network security posture.

- When we took the 35 strategies, coupled with the 70% effectiveness of implementing the top four to our Secretary, he took it to his colleagues who took it to their CIOs. As a result, we have seen a lift in cyber security across government. That's good policy. That's effective messaging.
- And effective messaging is where it really is about going beyond the firewall. DSD has invested very heavily in its messaging function. The 35 strategies is only one of a number of documents we've produced on everything from travelling overseas with a laptop, through to security considerations on cloud computing.
- This is why, for the first time, our next release of the Information Security Manual will be available for comment on OnSecure, DSD's online security portal, in early August for three weeks. This will allow agencies time to provide feedback on the document before its next update.

- Our new version of the ISM will feature a principles based document aimed at senior decision makers. The idea behind the principles based document is to focus on providing agencies with a better understanding of the threat environment and a rationale to assist agencies to develop IT based policies within their agencies.

## **Closing**

- As I said at the start today. The word cyber is widely used and we see many definitions of cyberspace. I prefer a simple definition - “the Internet and everything connected to it”.
- The Internet is a good thing.
- At the Defence Signals Directorate, we are currently focusing on four key threads of cyber security;

Intelligence

Technology

People &

Policy

- Our response to the cyber threat and our attention to these four threads of cyber security are critically important.
- Cyber security is a field that demands collaboration. Defence's Cyber Security Operations Centre and the Defence Signals Directorate have a lot to offer, but we cannot possibly tackle the cyber security challenge alone.
- I leave you with one final message today, while the cyber threat is real, there is something we can all and must do about it.
- Thank you.