

DSD Technology in Government speech

- Thank you and it's great to be here today. I've been doing a few of these talks lately, but it's especially nice to be speaking to an audience in a slightly more technical context. I started my career at the Defence Signals Directorate as an engineer and I have been lucky to experience some amazing technology and be involved in some pretty funky operational activities during my time there.
- I don't really get to play around with that sort of stuff much these days, but I still love working in an organisation where it goes on.
- I'm here today to talk to you about the nature and scale of cyber threats to Government and what DSD is doing about it. I'll do this today with a focus on the technological aspects of cyber security. But it's good to keep in mind that cyber security does have a range of dimensions, and not all of these are technical.
- So I will be talking to you today against this broader context, and specifically, in the context of four key threads that my organisation focuses on. These are:
 - Intelligence
 - Technology
 - People; and
 - Policy

UNCLASSIFIED

- Before I start, though, I'd like to offer you my definition of 'cyber' and 'cyber space'. And DSD's role in relation to cyber. Like all hot topics, they have a range of interpretations, but I prefer a relatively simple one – "The internet, and everything connected to it".
- That's quite a wide definition too, when you think about it. 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 at around 12.5 billion. Or, to put it another way, roughly two devices per person on earth. CISCO predicts that there will be around 25 billion devices connected to the Internet by 2015.
- I won't go into the "internet is very big" stats today – I'm sure you've heard them before. But for anyone like me, who pre-dates colour television, the growth of the Internet has been amazing to watch. And even in the 16 years I've been at DSD, it's completely changed the way we do business.
- Most of you would know DSD as an intelligence agency. I spent most of my career there on the intelligence side. But it's with the growth of the Internet, that our other role – our role as a security agency – has changed almost beyond recognition.
- This is because the way we do business in government has changed, again, almost beyond recognition from when I first entered the public service.

UNCLASSIFIED

Government, and government agencies conduct business, recruit and correspond with their stakeholders through email and online, even through social networking sites such as Twitter and Facebook.

Government agencies are looking at Information and Communication Technology solutions like cloud computing services, to maximise service delivery within their budgets and to deliver efficiency dividends.

- Information and Communication Technology is also taking government business beyond the office, every day. A computer network is no longer contained in the perimeter of a building. It extends our 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 everything is online.
- Let me be clear – the internet is a good thing. And I am part of this business change. Recently, while I was overseas, DSD updated one of its flagship documents – 35 Strategies to Mitigate Targeted Cyber Intrusions.
- We wanted it to be ready to launch during last week's Security in Government conference. I used my iPad, my own iPad, to read and approve the document on the plane trip home, so we could meet our publication deadline.

- So technology works for me – and for my business. But it’s a double edged sword. The Internet was never designed with security in mind – it’s all about sharing information as widely and quickly as possible.
- This means that the benefits the Internet delivers to Government also come with much higher risks to our information. It’s now possible for people with bad intent to steal, destroy and manipulate information covertly on a scale that would’ve been unimaginable even ten years ago.
- I’m here today to tell you that the threat to our information is real and persistent. But I’m also here to tell you some of the things that we can do about it – both in a technology context and beyond.

The intelligence ‘thread’ and the cyber threat

- So, to my first thread, which is intelligence. DSD has a good understanding of the cyber threat from intelligence – both ours, and the work of other agencies in the intelligence community. But there’s still a lot more we need to know, and everyone in the intelligence community is working hard on this.
- I can tell you that the cyber threat comes from a wide range of sources, including individuals, issue-motivated groups, criminal syndicates and state sponsored hackers.

- Of these, the state-sponsored hackers give my organisation the most work. They have the resources to develop the most sophisticated tools and techniques, and to direct them against our networks on a very large scale. Having said that, cyber crime is also an increasing problem.
- While we don't have as much information on it, we do know that it is costing our economy big time – as much as a billion dollars every year, according to a recent report from the Australian Federal Police.
- And, as more malware and hacking techniques are shared over the Internet, the capability gap between the state-sponsored hackers and the criminals and 'hactivists' is getting smaller.
- I can also tell you that the state-sponsored hackers are not just looking for classified information. 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.
- We need to make sure that our systems are secure so that we can guarantee the integrity of the information and services we provide.
- And by 'we', I mean all of us in Government. DSD cannot tackle this problem alone. This is why I encourage all government departments to report cyber incidents to DSD. This ensures that we can help you, and it helps our understanding of the threat, and what we can do about it.

- Cyber security is not just an intelligence problem. If your organisation is connected to the Internet, then your information is potentially at risk.

The technology ‘thread’.

- So lets’ look at our second thread of cyber security – technology. Most people have no problem thinking of cyber security as a technical issue.
- But, and I hope to go into this issue a little bit more later, many people still do have a problem thinking of the technological dimensions of cyber security as something which concerns them directly. And this is something which needs to be addressed.
- At the heart of DSD’s technical response to the cyber threat is our cyber security operations centre, or CSOC. The CSOC has two main roles. First, it provides Government with a better understanding of sophisticated cyber threats against Australian interests. Secondly, it coordinates the operational response to the most serious of these threats.
- Since its opening in January 2010, the Cyber Security Operations Centre (CSOC) has identified over 2100 cyber security incidents. Approximately 500 of these incidents were serious enough to warrant a CSOC response.

- These responses cover a wide range of activities. Sometimes direct action, like a visit to the compromised agency, or specific advice initiated from the CSOC, was needed. In a very few cases, the incidents were serious enough to need intensive, long-term activity by the CSOC, including the deployment of CSOC staff to affected sites.
- A lot of the time though, the CSOC response will be less hands-on. The incidents we see inform the generic advice we publish, for example our electronic alerts for particular types of activity, or advice on the trends we see in spear-phishing techniques. It also feeds back into the advice we give to Government on how best to protect our networks from targeted intrusion attempts.
- The CSOC is a formidable resource for government. It has a critical mass of very experienced technical staff that can, and frequently do, detect evidence of sophisticated cyber intrusions.
- It also includes staff from agencies across Government with a key stake in cyber security. We have people from other areas of Defence, the Attorney-General's Department, the Federal Police and ASIO sitting in the CSOC, multiplying its effectiveness and making it part of a truly nationally coordinated response to cyber security incidents.

- I'm not saying the CSOC is perfect. We can, and will do more for Government as we grow our capability. But in the 18 months it's been operational, the CSOC has kicked some important goals for Australia in terms of protecting our networks.
- The CSOC is also not the only answer to improving cyber security. We cannot do this alone. Cyber security is a shared responsibility across Government. And I mean everyone in Government, from senior leadership through to the people out on the floor.
- This is why DSD is investing heavily in the messaging and communication side of our business.
- A couple of weeks ago, we re-issued our flagship document, 35 Strategies to Mitigate Targeted Cyber Intrusions.
- This 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 CSOC responded to in 2009 could have been prevented if agencies had implemented the top 4 of these 35 strategies. Today, with the release of the revised strategies and the advances in ICT security by industry, we estimate it to be at least 85%.

- You don't have to take my word for it, either. The SANS institute recently posted a review of the update on its website, where it described these strategies as – and I quote – “the best hope for stopping or mitigating the targeted attacks”.
- While new strategies have been introduced, the top four strategies remain unchanged, indicating that they are still paramount to achieving good cyber security. I'm sure you're aware of them, but just to refresh, the top 4 are:
 - Patching your applications promptly
 - Patching your operating systems promptly
 - Restricting admin privileges on your network to the folk who really need them, and only allowing them to undertake administration tasks, i.e. not surf the web or access email; and
 - Not allowing unapproved applications to execute on your network – we call this application whitelisting.
- We did make a change to the order of the top 4. Patching applications is now the number one strategy, where it was once 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.

- The important thing about the top 4 though, is unchanged, and that is their proven effectiveness when implemented fully as a package. We know that they hit a sweet spot in terms of network defence-in-depth.
- We realise that the implementation of these strategies isn't a trivial undertaking. But the evidence that they are worth it is too strong to ignore.
- I encourage you to visit the DSD website and download a copy so that you can start a conversation in your organisation about improving cyber security.

The people 'thread'

- Now, I'd like to move to the third thread of my talk, which is people. Again, this is a message which I hope you've heard before, but it bears repeating. People are a key strength in your cyber security.
- DSD is an intelligence agency, and we know, as an intelligence agency, that technical and even operational expertise is only one part of the picture. Obtaining information by stealth often depends on exploiting peoples' behaviour as much as it does on Gucci technology.
- I have spent most of my time at DSD on the intelligence side, and some of the most successful operations I was involved in certainly used innovative technology.

- But these operations depended equally on our targets doing silly things or not thinking about security. Like using really simple passwords. Playing video games or visiting really dodgy web sites on the work computer.
- The hackers know this too, of course. And their approaches are getting more and more sophisticated. We're seeing a huge increase in the sophistication and frequency of phishing emails. These are not your average Nigerian bank scam emails.
- They might appear to be from someone you know, even a boss. They will have convincing looking commercial logos and signatures on them. And they will target specific interests, both professional and personal.
- This is why, on the 35 Strategies, 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. For example, DSD used to recommend that you educate your users on spear phishing emails, we have now extended this to a number of other areas:
 - Selecting stronger passwords and not re-using these passwords across systems.
 - Thinking about the websites you visit at work; and
 - Not using USB devices and other media not corporately supported.

- I'd actually like to take this one step further and suggest that the users we educate need to know how their information can be stolen. I'm not talking about giving every worker in your organisation a crash course in computer programming.
- But just as we expect the people we recruit these days to be able to at least turn on a computer and use Microsoft Office, we should expect them to have a basic understanding of the risks to their information and what they can do about this.
- Cyber security is not something that should be delegated to the helpdesk to deal with. The technological dimension of cyber security affects everyone, simply because nobody can do their daily business without recourse to technology.
- User education, like any of the 35 mitigation strategies, is not a silver bullet.
- In any organisation there will be a user who double clicks on a malicious email attachment or hyperlink. However our experience tells us that sometimes another user receives the same email and understands the threat enough to report it.
- Technical controls, such as the higher ranked mitigation strategy of performing email content filtering, can help users avoid making a wrong security decision.

The Policy Thread

- This brings me to my fourth and final thread of discussion, which is 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 freely confess that messaging isn't something that my division has always been consistently good at. We're really good at the ones and zeros, but we aren't going to achieve as much as we can with them if we don't translate this into language that is meaningful for everyone.
- But we are changing. My favourite example comes from a few years ago, when some of my technical specialist 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 technical measures 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 document called "35 Strategies to Mitigate Targeted Cyber Intrusions, which DSD 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 big, technically detailed document that forms the basis of our ICT security advice to Commonwealth and other stakeholders.
- Its good advice, but I'd be the first to admit that the manual is never going to make the New York Times bestseller list.

- The thing is, though, that the 35 strategies document speaks 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 a really simple statement which says 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 strategies, to our Secretary, he took it to his colleagues, who took it to their CIOs. As a result, we've seen a lift in cyber security across government. That's good policy, and it's effective messaging.
- The next edition of the information security manual will follow up on this trend. It will give people the "why" behind its technical advice, by spelling out the policy principles behind this advice. It will include an unclassified threat assessment.
- And above all, it will include an executive summary which will be directed at the senior managers who make decisions about resources and people in their organisations.
- Most importantly, for the first time, the draft of the ISM has been made available for comment on OnSecure, DSD's online security portal, before it comes through people like me for sign-off.

- Policy is also always more effective when it acknowledges the business drivers for the people who are applying it. And that's where DSD is also changing its mindset on security.
- Traditionally, information security, like physical security, has been informed by a conservative, prescriptive mindset. We tend to focus on the "Noes". You can't do that. You mustn't do that. You shouldn't do it like that. You're doing it **WRONG!!!**
- This year, I have often used a phrase coined by Ray Griggs, who is now our Chief of Navy, during his work on the Strategic Reform Program. Ray used to talk about the challenge of moving from a mindset of "We can't do that because" to a mindset of "We can do that if".
- This is exactly the mindset I want us to apply to cyber security. DSD can't be in the business of telling people that they can't take advantage of new technology.
- We can't keep saying to seniors "No, you can't have an iPad at home to look at your protected information. We harm our reputation by this, and in the long run, we do no good because we can't prevent people from using the latest technology.
- What we can do, though, is enable them to use it in the least risky ways. This is why, for example, we published a technical hardening guide on the iPad this year. It's not a certification of the iPad to store and transmit national security classified information. This is still coming, and we are working hard with Apple on

achieving certification of the iPad for use up to PROTECTED level. But the guide does enable you to significantly enhance the security of the iPad to protect sensitive information. And this is important. Like I said at the beginning of this talk, a lot of the information being stolen off Australian networks does not have a security classification. All types of information are potentially at risk.

- This is also why DSD revised the ISM's restrictions on user-owned devices connecting to government networks. Now, you can use your own devices – including your iPads – to connect into networks to read your email and browse your intranet remotely, as long as you use a trusted operating system.
- While I'm on tablet devices, we have already evaluated the Blackberry Playbook and certified it for use at PROTECTED level. I've got one of these as well, and it is a good option for business as a secure tablet device.
- So I think DSD is doing well on delivering solutions, as well as advising people of the risks in information security. But we can do better. We can pre-empt questions and start delivering answers about new technology. One of the examples where I think we've been especially successful in this way is our recent Cloud Computing Security Considerations paper. Cloud computing is fraught with security risks for government – but at the same time, it offers potential cost efficiencies that we cannot ignore. So instead of saying “don't touch it with a barge pole” or even “hang on and wait for a few months until we know more”, we're actually

encouraging agencies to embrace cloud computing services – but with their security eyes wide open.

- The paper has been a huge success, both within government agencies and the private sector, and I think it's for two reasons. First, it delivers the “can if” message rather than the “can't because” message. Secondly, it does so in a way which everyone can understand.

Conclusion

- To sum up what I've said today:
- The internet is a great thing. It has changed the way we do business in government, and greatly for the better.
- I want people to embrace this great thing, and the wonderful technology associated with it. I want everyone to use it to the maximum effect in delivering better business results for their organisation.
- But – and of course there is a but – I want everyone to make good decisions when they use this technology.
- The starting point for this is 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 will continue in 2011, but this year DSD is putting a lot of effort into improving everyone's understanding of the risk, and what they can do about it.

UNCLASSIFIED

- Finally, I would like to underline what I said to you earlier about technology, which is that it is a critical aspect of our response to the cyber threat. But it is much more effective when used with the other dimensions of cyber security that I have spoken to today – intelligence, people and policy.
- Thank you.

UNCLASSIFIED