Partnering for a cyber secure Australia
ACSC Co-coordinator Speech to ACSC Conference 2015
0920 – 1040, 22 April 2015
National Convention Centre, Canberra

Introduction

Whilst we have been gathering ourselves to meet here this morning … chances are … there has been at least one attempt by a state actor to penetrate Australian Government networks.

There will have been several attempts against some of our nation’s biggest companies… and many times that again by serious or organised crime to penetrate our banking and financial sectors.

That is why we need the Australian Cyber Security Centre.

Our task … and my responsibility … is to defend and assist others to defend against this threat.

I want to talk to you this morning about how we are going to go about achieving that. But let me start with some observations about the threat.

Threat Update

Malicious cyber activity will endure as a threat to Australia’s economic prosperity and our national security.

We are an attractive target because:

- A substantial amount of the business of Australians … and we are amongst the wealthiest of peoples … is done on-line.

- We have some significant bilateral relationships and alliances.

- We have valuable intellectual property in some specific areas of research.

- Just down the road from here, in Sydney,… for example … some CSIRO scientists developed what we now call WiFi.

- And then there is the strategic importance of our resource wealth.

Australia is a target rich environment for malicious cyber actors.

But our detailed understanding of the threat across Australia is still developing.

Specifically … our metrics are nascent. We want to work with industry … and citizens … to remedy this.

The metrics we do have are pointing to some trends that we expect over the next year or so:

- The number of state actors and cyber criminals with a capability will increase.

- Although quality code writers are a finite resource … so the available tools are unlikely to increase at the same rate as the number of cyber criminals.

- For those actors already in the game their sophistication will increase. This will make detection … and if you do find them … attribution, more difficult.

- A diplomat … not here in Australia … sent an email from his government system to colleagues in a number of other nations embassies inviting comment on an attached paper.

- Two hours later they all received another e-mail from him … this time he said with the correct paper attached … except it wasn’t from him. Unfortunately, none of the recipient’s knew that. That is an example of increased sophistication.

- Spearphishing will continue to be the most popular but waterholing will increase … and both these techniques will target software vulnerabilities … which will be subject to expanding research and publicity.

- 2014 was a big year for ransomware … we expect 2015 to be the same.

- We commonly view the threat through cyber as largely one of theft … the theft of money, identities, intellectual property and of national security information.

- Less commonly realised is the threat of destruction. If you can get access to steal then you have access to destroy.

- Significantly the attack on Sony late last year included a destructive element. We expect an increase in actors with this capability and, possibly, in incidents with a destructive element.

- We expect there will be an increase in electronic graffiti … web defacements, social media hijacking and the like … to grab a headline.

The ACSC

Can I now turn my remarks to the new Australian Cyber Security Centre.

The ACSC … as we call it … was officially opened by our Prime Minister last November.

It brings operational cyber security capabilities from across the Australian Government together into a … new … single location.

Those agencies are on the screen …

There has been some confusion about the difference between the ACSC and the former Cyber Security Operations Centre … CSOC.

As you can see the CSOC has been subsumed by the ACSC.

The CSOC was a Defence capability that hosted a few liaison staff from other government agencies.

The ACSC brings together all of the government's operational cyber security capabilities in one place … it has approximately three times the number of staff that the CSOC had.

So … we have been open for business for six months … what have we been doing?

First of all … the contributing agencies have been getting to know each other much better.

This is changing the cultures and the way we do business … which is exactly what was intended. If all we do is change our street addresses then we will have failed.

Earlier this year a member of the team … from one of the contributing agencies … mentioned he would be meeting with industry … and delivering a speech.

He said it would be good to have someone to come along to represent the ACSC.

This was a head scratcher for me. I said to him, brother you are the Centre … ah … yes was the reply. The change journey will take a little while yet … but it has started.

The next priority activity for us has been to develop our strategy for partnering with industry. Our strategy has been informed by industry … let me tell you a little about it.

It is based on the premise that public-private partnership on cyber security is essential for Australia's overall national security and economic prosperity… if we don't get this right… we will lose.

We want to collaborate to provide targeted and actionable information that can be accessed and used by those who need it … be that the private sector or government.

And we want to develop longer term assessments that can be shared more openly.

To achieve this we are going to need to open the doors of the Centre to industry.

We see our industry partners in three broad groups:

- infrastructure providers, telcos and ISPs
- sectors that are targeted by cyber actors, and
- cyber security vendors.

Industry participation within the ACSC will be at the invitation of the ACSC and … for the time being … we will focus primarily on owners and operators of systems of national importance.

With the endorsement of the Board that oversees the Centre, I have written to seven Telcos/ISPs inviting them to join us in the Centre.

These providers were selected based on the size of their customer base as well as those who have customers that are of national interest.

Targeted sectors

The second group … targeted sectors … includes industries and companies most targeted by malicious cyber actors.

Because our organisational capacity is not able to deal with everyone at the same time we have had to prioritise the sectors to work with.

Priority will be given to sectors who are strategically important to the nation, the attractiveness of the sector to malicious cyber actors, and whether the partnership would be of value to both the sector and government.

We will give preference to sectoral representatives over individual company representation. We are finalising a plan for engaging with sectors to build partnerships.

The key risk we see … at the moment … is whether industry sectors are organised in a way that allows us a sensible partner.

We know some are… but some are not.

If businesses in a particular industry are not organised into something akin to an industry group … our approach will be to work with the key two or three players in a sector and see if we can develop a suitable forum.

Cyber security service providers

To the third group, cyber security service providers … and I know there are a good number of you in the audience today … you are, and will continue to be, crucial partners for the ACSC.

We want to continue to collaborate with you … but we will not be offering a permanent seat in the centre ... for the foreseeable future.

What we will consider is providing a pass for a provider to access the centre to work collaboratively on short term projects.

I acknowledge that we need to do more thinking about how to further develop the Centre’s relationship with cyber security providers. We will do this … and I would welcome the community’s ideas.

Those individuals selected to represent sectors or organisations within the ACSC are required to hold and maintain a Top Secret Positive Vetting security clearance.

We will advise and approach potential industry representatives once we have firmed up our arrangements with Telcos and ISPs and can free up some organisational energy.

So what else have we been doing?

We have continued on our journey of awareness raising activities … this conference is part of that effort …

You may have seen our latest video production on YouTube … "Recognise report".

Getting our message out there is key. We have not been afraid to stand up and be noticed … and this video has been plenty noticed.

It is not aimed at educating the cyber security community … rather it is intended as a tool for you to use to help educate others.

We have also released authoritative security advice to our website on cloud computing … which I think is a world class effort.

And around the middle of the year we will release our first … unclassified … national cyber threat report. It will provide an overarching view of threat actors, what they want, and how they go about getting it.

The target audience is not so much the cyber security community … though we hope it will be a useful resource for you … but rather boards, management and SMEs.

Now, whilst one or two of the agencies in the Centre are used to producing unclassified reports … it is not true for most of us. It will probably take us a couple of iterations to get it right.

All hands to the pump

Let me turn to my final idea.

We, Australians, sometimes look overseas for thought leadership, when we should be doing it … or at least contributing … ourselves.

Often we do this because other nations have been looking into a particular endeavour for a very long time … there are efficiencies to be had by learning from those who have been at it for a while … sometimes it makes sense to follow.

I do not think cyber fits into that category.

When I first took up my appointment I did some horizon scanning for best practice in cyber security.

I saw much that was good.

The Netherlands had combined their capabilities into one organisation.

The US and Canada had some terrific technical capabilities – Canada especially in the area of automated monitoring.

The UK had put a great deal of effort into their partnerships with industry and academia.

Australia does these things as well … with varying levels of success.

However, in my scanning, I did not see anyone who was obviously out in front … I did not see a bright light out ahead to follow. … I did not see anyone with a better, across the board, approach than us.

We have a reasonable picture of the threat to us here in Australia.

We do not focus on just one avenue to mitigate the threat … we take a holistic approach to the problem.

In fact I have noticed we have a point of difference … a strong focus on prevention.

And we know that the solution is as much about people … as technology.

Our mitigation strategies and advice are extremely effective. And the results that we are achieving are good.

So I invite you not to search for some bright light out ahead away from home … there is none out there.

While we must stay abreast of what other nations are doing … we need to roll up our sleeves and make our own contribution … we can, and should, stay at the leading edge of thinking about cyber.

To do this we need to harness the collective IQ of the nation … across academia, industry and government. I intend that the Centre play a pivotal role in helping to achieve this.

One of the ways we can do that is to continue to gather together in forums such as this.

Please enjoy the conference… it is a significant contribution towards partnering for a cyber secure Australia.