Australian Government

Chief Scientist

DR ALAN FINKEL AO

National Fintech Cyber Security Summit

Cyber Security: Challenges and Opportunities

Tuesday 3 May, 2016

The Ivy

Sydney

My new car… our big challenge

I have a new car. In fact, it isn't a car – it's a computer on wheels. A magnificent, fast, comfortable computer on wheels that, so far, I have had to reboot three times.

A testament, perhaps to the incredible complexity of this mobile computer.

It controls the brakes. It controls the electric motor. It even controls an autopilot capable of steering, cruising and parking.

So you can imagine that, in the wrong hands, access to my computer on wheels could be very concerning indeed. And not just for me. Did I mention how fast my car can accelerate?

Now I tremble to imagine the consequences of a large scale attack on our future traffic system.

Just think – in 30 years from now we are all using automated cars. We've solved the problems of traffic congestion and parking.

We've eliminated traffic lights and our city fleet of 2 million cars is cruising, blissfully efficient, around Sydney. Suddenly, at 5 pm, a successful cyber-attack results in the entire fleet crashing or screeching to a halt.

Of course vehicle designers are thinking of these scenarios now and will plan an effective defence. But recent news articles suggest to me that the security is far from perfect.

Access to vehicles has been gained through mobile apps for BMW, Mercedes-Benz and Fiat Chrysler cars, with the most prominent example leading to the recall last year of 1.4 million Jeep Cherokees after hackers showed that they could control the car though the online entertainment system.[i]

Most people think of cyber security in terms of the big players; the military, the government, or big business. The organisations in the news when websites are hacked or customer data compromised.

But with the growth of the Internet of Things, everything is coming online, from watches, to whitegoods, to children's toys. And each of these networked devices creates a new opportunity for attack.

So is now the time to panic?

I don't think so. It's time to rise to the challenge and opportunity that cyber security presents. We can do this – as a nation.

When I was discussing Operating System security with Adrian Turner this week, he likened future self-defending algorithms to the body's immune system. And in many ways, this is an excellent analogy.

It is a community responsibility to be vaccinated if you can.

And, in the same way, it is each person's responsibility to ensure that they are doing what they can to defend against cyber-attacks.

If we want to enjoy navigating a free and open internet we need to contribute to preventive health rather than treatment after the fact.

We all need to ask ourselves, whether we're a business, a government, a university or an individual – are we doing enough?

Threats today

Now I am not a cyber security expert, but I don't think you have to be to take a very keen interest. The global cyber security market is currently worth more than US$71 billion and is growing at around eight per cent a year.[ii]

Governments overseas are clearly focussed:

1. The UK published their cyber security strategy in 2011. Since then, their cyber security sector has almost doubled from £10 billion to £17 billion with employment now at 100,000 people.
2. The US has issued Executive Orders, created the NIST Cyber Security Framework and continues to lead the way on cyber security policy.
3. And Israel has cemented its dominant position for cyber security entrepreneurialism.

The launch last week of the Australian Government's Cyber Security Strategy reflects the commitment on all sides of politics to defend and advance our own critical interests.[iii]

And we do have tools and strategies to fight back. The Australian Signal Directorate's *Top 4 Strategies* are estimated to mitigate at least 85% of the intrusion techniques to which the Australian Cyber Security Centre responds.[iv]

But what about the other 15%? What about securing new devices, and countering the emerging attack techniques?

At a summit such as this, we can look to these aspects of cyber security as an incredible opportunity.

First, it's an opportunity with an identified local market.

There is a clear economic imperative for cyber security capability in Australia. We have digitally advanced industries – including banking – that demand comprehensive cybersecurity capability.

According to a recent KPMG report, there are 10 Australian companies in the top 100 list of global FinTech Innovators.[v] These and their contemporaries will demand increased cyber-security capability as they grow.

Why wouldn't we innovate to meet this demand locally?

Second, it's an opportunity with breadth.

We would be mistaken to think that cyber security is the exclusive realm of IT companies. Or only for the military. Or government. As we move towards a data-driven future, all industries will be underpinned by the capability and security of their IT systems.

And large companies know this. As just one example, the Commonwealth Bank has partnered with UNSW to the tune of $1.6 million in an effort to boost Australia's stock of cyber security professionals.[vi]

A step that seems warranted in an industry where job advertisements have grown by more than 57 per cent in the last year.[vii]

Third, it's an opportunity with depth.

Cyber security is not just about mitigating vulnerabilities, improving secure coding practices, developing products to automate intrusion detection, or increasing user and community awareness. It is about ALL of these things and more.

In an increasingly automated and connected world, it is also about the translation of research, about collaboration between small and large enterprises, between government and industry, and between international partners.

And fourth, it's an opportunity that aligns with much of Australia's future needs.

The development of Australia's cyber security capability will require the same considerations as *all* of our grand global challenges:

- Well-trained scientists, mathematicians, engineers and ICT workers,

- Well-established collaborative relationships between research, industry and government, and

- A scientifically literate community capable of engaging in a challenging national conversation.

Obvious questions that will arise in this national conversation include:

How do we reconcile security with efficiency?

Are we clear about the difference between privacy and security?

Can we embrace cyber security as an obligation we share, to achieve immunity for the digital herd?

And importantly – can we recognise the magnitude of the risk, without forgetting that the opportunity on the other side is just as large?

Looking ahead

I am extremely heartened to hear examples of Australian companies growing in this space. Companies like NUIX[viii] - an internationally respected, Australian data analysis and cyber security company with hundreds of employees and more than 1000 customers – a company that is growing at an incredible rate.[ix] A company that sprang forth from an Australian university.

And there's much more coming. Through its partnership with CSIRO's Data61, Stone and Chalk will encourage other emerging companies in this space.

From my viewpoint, cyber security is a critical, growing field with enormous potential. Potential that will only be realised with commitment, collaboration and innovation. And that's where you come in.

By your presence here today you are the ones who see the potential.

I encourage you to seize the opportunity by investing in your own proprietary approaches, investing in skills development, and creating exciting and important contributions to the Australian business landscape.

Thank you.

---

[i] http://www.nesta.org.uk/blog/cyber-security-and-future-driverless-cars#sthash.vrzgtVMs.dpuf

[ii] http://www.innovation.gov.au/page/cyber-security-growth-centre

[iii] https://www.pm.gov.au/media/2016-04-21/australias-cyber-security-strategy

[iv] http://www.asd.gov.au/infosec/mitigationstrategies.htm

[v] http://fintechinnovators.com/

[vi] https://www.commbank.com.au/about-us/news/media-releases/2015/commonwealth-bank-and-unsw-confront-chronic-cyber-security-shortage.html

[vii] http://insightsresources.seek.com.au/seek-employment-trends-australia-spotlight-information-communication-technology

[viii] NUIX

[ix] http://www.forensicfocus.com/c/aid=76/interviews/2014/jim-kent-ceo-emea-nuix/. https://en.wikipedia.org/wiki/Nuix.