Speech for Australia-Israel Chamber of Commerce (WA):

"Secure and productive: industry's connected future"

Innes Willox, Chief Executive Australian Industry Group, Friday 3 November 2017 at EY, Level 5, 11 Mounts Bay Road, Perth WA

1. Introduction

Before I begin, I would like to thank our hosts, the Australia-Israel Chamber of Commerce, for inviting me to present to you about creating a secure and productive industry.

To be truly productive, industry first needs to be secure, both within itself and within its supply chains. As Australian industry becomes more international in its outlook, more integrated into the businesses of others offshore and more diverse in terms of its relationships and as the opportunities and the challenges become greater, the need for certainty of security is greater.

Also greater – and growing with speed – is the complexity and integration of business. Think of the increased use of big data, data analytics, automation, robotics and sensor technology as well as the use of the internet as a key distribution channel in the operations of businesses of all shapes and sizes. With that comes growing connectivity, the sharing of information and the use of the cloud.

It also means that businesses of any size, shape or sector need to be more aware of their security, not just their physical security but even more than that, their cyber security. What has been a forgotten or neglected component of the business risk equation by executives and boards, is now and must be a front of mind issue.

Business leaders are being asked more and more about what they are doing to tackle cyber security. The questions are being asked by partner businesses and by government. As business becomes more interconnected, perhaps like a rowing squad, you don't want to be the weakest link in the chain.

It is certainly something that keeps me up at night and a potential Black Swan event waiting to happen for any organisation – including mine!

The Australian Industry Group represents thousands of businesses around Australia, businesses of all sizes and covering many sectors, from manufacturing to construction, defence, labour hire, medical technology, communications and more.

While in many ways diverse, all our members have a common and indeed a collective interest in cyber security.

I think about it this way.

Businesses and individuals who do not take cyber security seriously are the ones that can bring down both themselves and anyone they do business with or hold sensitive data about.

They are today's biggest business risk factor, the weakest links in the supply chain and a potential anchor to business productivity.

So, today, I am here to discuss with you some of the key foundational areas that business leaders need to seriously consider around cyber security.

Now in May this year, a major global ransomware attack occurred: WannaCry – I am sure you have all heard about that.

Australia was not immune, with a few Australian based businesses hit by these attacks, disrupting business operations and productivity.

A month later, while companies were still reeling from these repercussions (and some are still recovering even now), another major global ransomware attack occurred: NotPetya.

And now four months after NotPetya, we hear of another incident – this time about a local defence subcontractor who was infiltrated by a hacker.

According to reports, this local company lost a significant number of commercially sensitive documents for defence-related projects including the Joint Strike Fighter program.

This incident had two particularly alarming features.

Firstly, the company was made more vulnerable by a combination of several poor cyber hygiene practices, including use of very basic default passwords and old unpatched software.

Secondly, and of most concern, is that the breach began in July last year, was not discovered until November that year, and only publicly reported last month (almost one year on).

This incident made worldwide news, due to the connections to the defence industry; however, what was stolen was commercial information that is now in the hands of potential competitors.

It may seem like this is old news (as the underlying incident occurred a year ago) and I am picking on a single unnamed business.

However, the company in question is a small engineering firm of about 50 employees, with just one IT staff member.

That could describe a great many Australian businesses.

This incident should set off alarm bells for many business owners.

They may have thought “my business is too small to attract the attention of hackers”.

That is a myth.

Small or large, everyone is a potential target and nobody can presume themselves safe.

This is not a new thing.

Ransomware has been around for almost 20 years, and other types of cyber attacks have been with us for even longer.

But the threats are growing.

I recently visited the Australian Signals Directorate and they presented to us about these growing threats including the following:

- 75% of major cyber security threats facing large Australian businesses involve ransomware.
- Australia ranked second highest in the world for the number of ransomware detections in 2016.
- One third of Australian businesses have been subject to Distributed Denial of Service (DDoS) attacks.
- DDoS is also used in conjunction with ransomware.
- A recent ransom operation demanded 20 Bitcoins, (AU$97K) to stop DDoS against an email service.
- Cyber adversaries are increasingly stealing IP and conducting industrial and economic espionage.
- It is estimated that USD$700 billion in raw innovation is stolen from US companies each year.

These sorts of incidents are just the tip of an evolving cyber iceberg.

If businesses do not act, it is only a matter of 'when' and not 'if' this will happen to them.

And, sadly, cautionary updates on the latest victims have become a regular part of my speeches.

2. Why is cyber security important now?

There are a number of reasons why cyber security is becoming more important for businesses today than ever before.

Technological advances have created new points of vulnerability.

The **mobile revolution** has made digital technologies more ubiquitous in our society, both in our homes and workplace, enabling instant access to the internet while on the run.

It is almost now unheard of for anyone to leave their mobile phone at home – for some it has become their digital wallet.

While mobiles have helped increased business productivity, they also create a new attack vector for hackers.

The growing **Internet of Things** (or IoT) makes this an even bigger issue, as connectedness and data exchange grow exponentially.

There are currently more than 8 billion connected devices in the world, and for now at least this number is growing at a rapid rate.

Any one of them could be a point of failure in the security of a home, business, network or critical infrastructure.

The **Fourth Industrial Revolution** (also known as Industry 4.0 and the Industrial Internet) is seeing digital technologies converge with the physical world, bringing a new era for industry and society – and new forms of vulnerability.

Beyond technology there is regulation.

The new data breach notification laws due to commence in February next year will trigger another level of interest from businesses, if news about cyber attacks were not enough of a concern already.

Then there are **competitive** drivers.

Since the turn of this century, more than 50% of the companies that dominated in the Fortune 500 have either gone bankrupt, been acquired or ceased to exist.

This commercial disruption has been accelerated by the speed, volume and complexity of change enabled by digital disruption.

This has led to a mixture of anticipation, fear and skepticism from business leaders and workers.

No company, however invincible it seems, can rest easy.

Legions of startups are tirelessly plotting to displace them – and while most will fail, a few will change the world.

Cyber security becomes an important part of this competitive conversation and cannot be considered in isolation.

Poor security can help lose fortunes, but good security can help make them.

While there are evolving cyber security threats to manage to be secure and productive, there is immense value to tap into.

The global cyber security market was estimated to be worth US$75 billion in 2015, and is predicted to rise to US$170 billion by 2020.

It is also estimated that cyber crime costs the Australian economy roughly $1 billion dollars a year.

We need to help businesses and the community to embrace the opportunities without falling into the clutches of the cyber criminals.

Another key part of the picture is **skills**.

Attracting, developing and retaining skilled staff is essential for business to be competitive on cyber security.

The best digital technologies in the world will not deliver their full benefits without the best people with the right skills and the leadership to maximise their potential.

Companies succeed if they have strong leadership to set the right culture to drive change and create an adaptive and flexible workforce.

With the right skillsets in place, we will be able to cultivate a collaborative environment that encourages the development of innovative products, processes and solutions.

While internal skills are critical, this is not about tackling cyber security on our own.

Local and global partnerships are becoming critical – both in business and government.

In short there are many good reasons why an effective focus on cyber security is now fundamental to a successful business and a productive economy.

But before I delve deeper into the foundations for an effective cyber security response, I would like to outline current business attitudes towards cyber security.

3. Our findings

In a recently published survey[1] of 250 CEOs, Ai Group found that only 22% of businesses used cyber security technology – that is anything beyond the default protection bundled with their operating system or basic antivirus software.

Cyber security experts regard such default protections as the last line of defence.

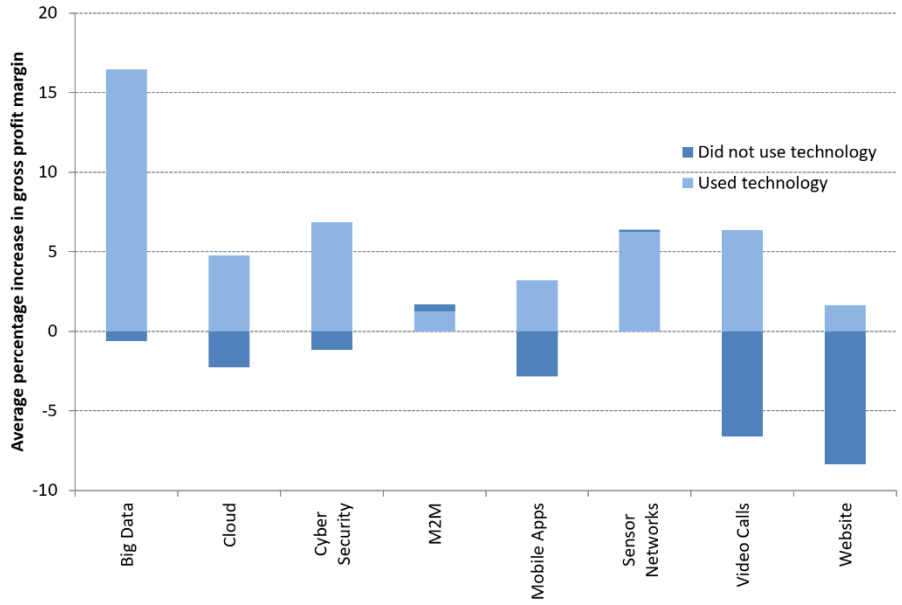
We also found that just 13% of businesses considered cyber security to be an inhibiting factor for business investment in digital technologies.

This goes against trends overseas, as reported by The Boston Consulting Group and McKinsey Digital.

This low business priority suggests to us that there is an underlying lack of organisational appreciation of the importance of cyber security.

The combination of low investment and low concern suggests a dangerously unfounded confidence that things will be okay.

But there is also good news in our findings.



If you would like to know whether digital capabilities and investment can drive revenue growth, including in cyber security, then my simple answer is yes, as you can see in the chart.

[1] Ai Group (May 2017), *Business Beyond Broadband*.

Our survey results showed a close association between digital investment and higher business performance.

- Businesses that maintained investment showed increasing revenue (5%), as did those that increased investment (4%).
- Businesses that did not invest in digital technologies saw an average 3% decline in revenue.

While our analysis suggested a link between digital investment and revenue growth, there was still a disconnect amongst business respondents in realising these opportunities and implementing strategies to achieve growth, as well as addressing risk.

This leads on to my first foundation for a more cyber-secure and productive industry: **boardroom focus**.

4. Cyber leadership and culture

A modern mantra in the business world is that cyber security is a boardroom issue.

But what does that really mean?

One of the best analogies that I have heard is to Occupational Health and Safety.

Businesses initially viewed OH&S as a compliance matter, with concerns about over-regulation.

OH&S eventually evolved into a risk management consideration but it took businesses about 20 years to get there.

Hopefully it will not take this long with cyber security.

While the forthcoming mandatory data breach notification law has good intentions behind it, we suspect that many businesses will likely treat this as a compliance issue.

That would be a pity.

Rather than mere compliance with an inscrutable mandate, companies would do better to take cyber security seriously as a business discipline.

Like OH&S, if you treat cyber security as an internalised management discipline rather than merely as a compliance task, you stand a better chance of making it part of your organisational culture.

And there are good business grounds for doing so – I will offer three.

Firstly, **poor cyber security costs money**.

When a cyber attack occurs, a company's operations could be disrupted, leading to lost time in production, repairs, potential regulatory fines, legal costs, and insurance premium increases.

But there are other very real costs that can be overlooked – customer reactions, reputational damage, management time and focus being diverted, and psychological impact affecting employee morale and productivity, leading to absenteeism and turnover.

A single serious cyber incident can cost enough to threaten the existence of many companies.

When making the hard-nosed decision about whether it is worth the money to elevate cyber security as a company priority, it is important that the full range of financial risks to the company are assessed.

There is another emerging financial implication of cyber security too: the ability of companies to raise capital.

Investors increasingly look at the corporate social performance of companies – will cyber security be a new measure of ethics, risk and management competence for investors?

Consider the recent Equifax data breach as an example.

Equifax is a worldwide consumer credit reporting agency, with almost 120 years of history, and their lifeblood is data.

In July, there was a data breach through Equifax's website, with reports of over 140 million people, mainly in the US, being affected.

It was not until September that Equifax announced this cyber incident.

While it remains to be seen as to whether this is a temporary setback for Equifax, its share value plunged by 24% and wiped out approximately 18 months of share price growth.

So significant was this breach and the subsequent criticism of Equifax's response that a number of senior executives including their CEO have departed the company, with talk of further regulatory action and lawsuits.

The second reason to make cyber security core business is the increasing role it plays in **supply chain selection**.

In short, could good cyber security practice be promoted by companies as a point of differentiation against their competitors?

What we are increasingly observing is that cyber security is becoming a key selection criteria of business partners in contracts and tenders, locally and overseas.

This is most obviously the case in suppliers to the defence sector, but it is becoming commonplace among large primes in many fields.

Finally, the cyber security record of a firm or indeed an industry may become increasingly important for their **social licence to operate.**

Companies or industries with an indifferent attitude to cyber security incidents may increasingly find that this does not win fans among consumers or politicians, particularly if there are privacy breaches to explain.

Will they receive less policy sympathy in times of economic trouble because of bad cyber security practices?

Will they be subject to customer boycotts, amplified by the power of social media?

To go back to the Equifax case, the entire credit data industry is also now subject to more regulatory scrutiny.

So I think there are strong business grounds for companies to see cyber security as an integral and natural part of both corporate strategy and good management.

And it is no coincidence that these grounds for cyber security are similar to previous points made for OH&S.

Learning from the OH&S experience, businesses do not need to take 20 years to reach the same conclusion for cyber security.

If businesses can put the right leadership culture in place, the second cyber foundation they need is **workforce capability**.

5. Cyber education and skills

The first skills issues that usually springs to mind in this context is the need for the IT skills to understand what cyber security technology and services are relevant to the business.

But cyber security is more than just the IT department, and we are only as strong as our weakest link.

This means good cyber hygiene across the organisation.

It starts at the top, from the Boardroom and senior management, but it has to be practised by every employee in the organisation.

Again OH&S provides a model.

Workforce cyber education should be considered in any new employee induction program and applicable to everyone in the organisation.

This is why, as a first step, we regularly run cyber security awareness events for member businesses, drawing on the expertise of members like Cisco.

A more skilled workforce will underpin good organisational cyber hygiene across all Australian industries.

And there is plenty of material to draw from to get started and to keep up to speed.

The Australian Signals Directorate have developed Strategies to Mitigate Targeted Cyber Intrusions in support of the Australian government and also industry partners.

And as a start they recommend the implementation of the Top 4 mitigation strategies as a package to prevent at least 85% of targeted cyber intrusion incidents.

The ASD have a wealth of information and guidance for businesses available on its website.

There is also an opportunity for Australia to build a more innovative and competitive industry in cyber security itself.

As you know, AustCyber (also known as the Australian Cyber Security Growth Network) has been tasked with this responsibility.

But this industry's success will be hamstrung without access to strong technical and foundational skills in cyber security.

That ultimately means ensuring our youth has the necessary skills, which is fundamental to industry success in the long term.

In our schools, Science, Technology, Engineering and Maths (STEM) education is a prerequisite for cyber security.

We need more coordination of STEM activity with greater industry participation and a bigger workforce of qualified STEM teachers.

Those teachers in turn need to work from a more engaging school curriculum and with pedagogy developed to attract students to STEM.

At the higher education level, our research suggests that improved practices around work integrated learning (WIL) for both undergraduate and research students, and closer connections between universities and business will better equip graduates.

We have also found that partnerships in WIL can lead to greater support for collaborative innovation, which I will discuss shortly.

The VET sector needs to be part of the government's innovation initiatives.

All VET qualifications will need to be re-examined for their capacity to incorporate both STEM and higher order skills that may provide a pathway to higher education and a career in cyber security.

We are piloting this approach in our partnership project with Siemens and Swinburne on the Industry 4.0 Higher Apprenticeships Project, which includes cyber security as one of its units.

This leads on to my final foundation for cyber security: **collaboration**.

6. Collaboration and partnerships

We hear a lot about collaboration and innovation – they are certainly not new concepts.

For our early ancestors, it was a matter of collaborate and innovate to survive.

While not as dramatic in today's business world, collaboration and innovation can mean the difference between financial sustainability and oblivion.

In the context of cyber security, collaboration is important for sharing information about threats, as well as building an innovative industry.

On the first point, traditional forms of regulation have been criticised for being inflexible and slow to respond to rapidly evolving threats.

Governments tempted to over-use these regulatory sticks need to consider a different approach.

In responding to modern cyber security threats, it is critical that collaboration is encouraged in a safe environment where businesses can share threat information without being punished.

Cyber crime is also a global issue, requiring governments to work together more frequently – while managing their different values and approaches to issues like privacy and national security.

The fast pace of technological change also forces companies to rethink their business models.

Some businesses realise that they may not be able to offer everything the customer requires in-house.

Developing new capabilities themselves can be expensive and risky; partnering can be an attractive alternative.

Successful partnerships create trusted relationships and networks, locally and globally, that should not be undervalued.

And in cyber security, the value of trust is amplified even further.

It is therefore essential that businesses and their networks are strengthened and secure.

In Ai Group's surveys of Australian CEOs and leading Australian innovators, we have found that Australian businesses are collaborating to innovate more frequently than is often recognised – but that we are still well behind most OECD countries on this front.

Governments can play a role by improving the incentives for collaboration in public sector research funding, and maintaining stable support for innovation overall.

Researchers can help bridge the cultural divide with business and ensure their approach to IP encourages partnerships rather than undermines them.

But the clearest path to better collaboration is for businesses to learn the practices of those who already collaborate well.

As our research shows, these businesses make collaboration a process that is carefully considered and iterated for success.

Their practices include clear eyed awareness of their own strengths and weaknesses; careful selection of partners that complement their capabilities; shared development of a business vision for mutual benefit; and a commitment to learning from the experience of collaboration.

Ai Group is encouraged by evidence of progress on the foundations I've outlined today.

You may be aware that the Federal Government has recently launched its International Cyber Engagement Strategy.

We are pleased to see global issues like digital trade and cyber crime included as priorities in this Strategy.

An important message in the Strategy is about partnerships, which are critical in a rapidly evolving area.

Israel is a case in point.

Israel has long been recognised as a leading nation for innovation, with a thriving hi-tech community, including in cyber security.

Australia shares a lot of common interests with Israel.

We may be separated by vast distances, but digital trade and cyber security threats are not constrained by borders or oceans.

The agreement between our Australian and Israeli Prime Ministers last year to expand business and trade ties, including to collaborate more on cyber security, was a good start.

It is now up to industry to make that happen.

I believe that taking action on the three cyber foundations discussed today (cyber leadership and culture, education and skills, and collaboration and partnerships) will help industry take the next step.

So with these thoughts, I look forward to your comments and questions.

And I also look forward to our joint defence industry delegation trip to Israel in May next year and hope to see you there.

Thank you.