Special Report

Cyber resilience

In partnership with ACS

www.afr.com | Tuesday 21 August 2018

Edited by Jason Clout: jclout@fairfaxmedia.com.au

Too many businesses ignoring risks

Strategy Maintaining data security has never been more important.

Ian Grayson

Despite the growing number of internet-based attacks against businesses and public sector organisations, most Australians remain unaware of the need for effective cyber resilience, experts have warned.

With an increasing proportion of economic activity being handled electronically, ensuring transactions and data stores remain secure has never been more important. However, many people are either ignorant of the risks or indifferent about the consequences of such breaches.

At the roundtable discussion conducted by *The Australian Financial Review* in partnership with ACS, participants agreed awareness of cyber security issues is alarmingly low and urgent steps are required to encourage more people to take pre-emptive action.

Fergus Hanson, head of the International Cyber Policy Centre, said the relaxed attitude of many people towards cyber security stems from their perception of a lack of risk. For example, if an individual has their credit card details stolen, they know their bank will make them whole again and so they do not see a need to be concerned.

"Or perhaps it's a data breach of personal information and it gets on the dark web," he said. "No one hangs around on the dark web, so they think, 'it doesn't really bother me. I'm not interacting with that problem face-to-face'."

Other discussion participants say that often, even if there is awareness of the challenge posed by cyber attacks, many people are unaware of the steps they need to take to boost their resilience.

Simon Ractliffe, head of cybersecurity at Singtel Optus, says: "I think, unfortunately, a lot of the population takes a view that [cyber security] is too hard, they don't understand it and so, therefore, there's nothing they can do. I think they have a fog. There's generally a technology fog or a confusion fog that prevents them from feeling like they can be part of the solution."

Maria Milosavljevic, chief information security officer for the NSW government, agreed many people are failing to act and believes this failure is stemming from feelings of fear. She said many people feel they do not understand anything about technology and worry they will be bombarded with advice they are not going to understand.

"So it's about breaking through that barrier and making people understand that this is actually about business risk," she said. "It's really not about just technology, it's about what can happen to you."

John Dewar, vice-chancellor at La Trobe University, said there is a requirement for a "huge shift of awareness" when it comes to cyber security and the importance of effective resilience measures.

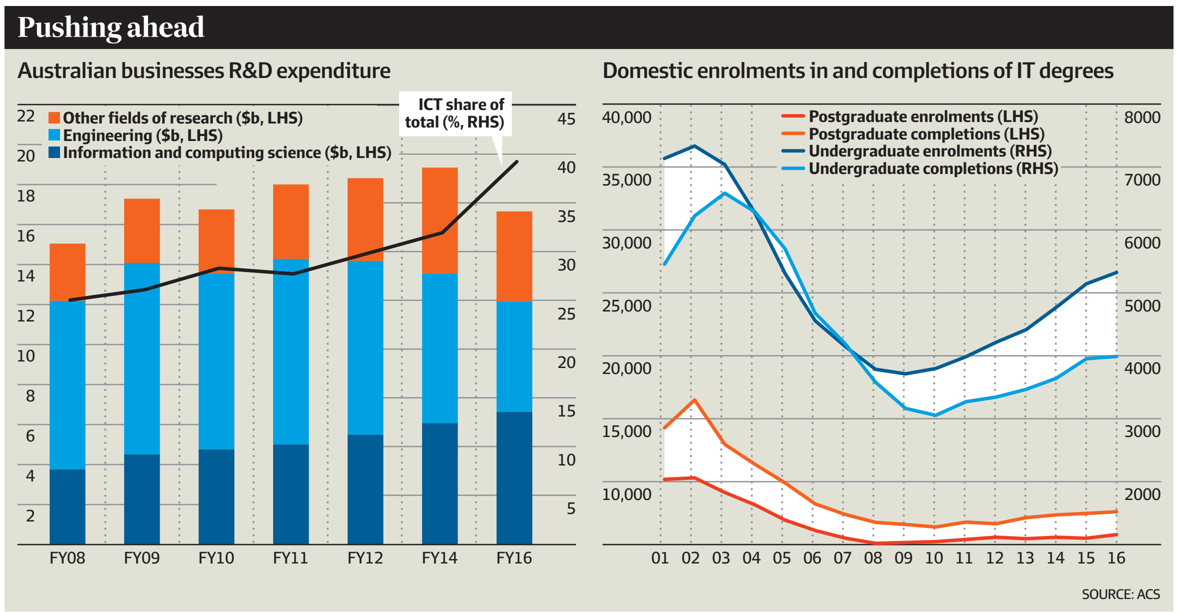
"People have grown accustomed to trusting the internet [as a means to] exchange data," he said. "What this now requires is for people to become distrusting, and I think that's something that is quite difficult to achieve."

Urgent steps are required to encourage more pre-emptive action.

Encouragingly, Professor Dewar said cyber resilience awareness levels tend to be higher within academic circles as students are taught about the importance of securing their online activity.

"Obviously, we're huge users of the internet and data and Australian universities are the home of very high-speed internet," he said. This means attention is constantly being placed on making such links and interactions as secure as possible.

Gavin Matthews, practice director, cyber security and risk, at GHD, said there needs to be a mindset shift from people assuming that other parties will take care of their cyber security to one where they feel personally responsible.


Pushing ahead

Australian businesses R&D expenditure

Domestic enrolments in and completions of IT degrees

SOURCE: ACS

"In the US and Europe, there's a lot more focus from an individual perspective in particular and, especially with their boards, around social media protections and executive profile protections," he said. "There's a lot they're doing in that technology space, and companies are a lot more focused with regard to their executives. Here in Australia, we just don't seem to have that focus."

When it comes to the role of government, politicians are faced with putting in place policies and regulations that not only promote cyber resilience but also protect the data held by departments and agencies. Discussion participants recognised that, in this area too, there is much more that needs to be done.

"I think it would be naive to assume that awareness within the general community was high," said Philip Dalidakis, Victoria's Minister for Trade and Investment, Innovation and the Digital Economy.

"I think it would be a bit like an iceberg – 20 per cent are probably very aware, and there's probably about 80 per cent that have absolutely no idea or knowledge of anything that's going on around them. From a public policy point of view, it's the stuff that keeps me awake at night – making sure that, even at a state sub-jurisdictional level, we have our own policies in place to protect data. And we, as a state government, have huge amounts of data from

Continued next page

Maria Milosavljevic says of getting the message across: "It is really not about just technology, it is what can happen to you." PHOTO: JEREMY PIPER

Boards need to take more responsibility

Professor Jill Slay says Australian business is well behind the US and Europe in terms of cyber security. PHOTO: JEREMY PIPER

Leadership Action must be taken to ensure greater security.

Mark Eggleton

Australian business needs to work a lot harder to build its cyber security capability because at present not enough is being done to prevent a cyber attack that potentially could undermine confidence in the whole economy.

This was a clear message to come out of the Cyber Resilience roundtable hosted by *The Australian Financial Review* in partnership with ACS in Sydney.

Director of enterprise security at Micro Focus, Chris Casswell, likens the current environment to the aftermath of the September 11 attacks in 2001.

He says at the time everyone was talking about disaster recovery.

"Everyone was going to spend money on disaster recovery but it didn't happen. Every company just put it off."

Unfortunately, the big cyber security attack is probably still to come and Casswell suggests it is really up to the government to think about its place in helping organisations to recognise the cyber security threat and the implications it can have on the broader economy.

The looming threat is quite massive as Lloyd's revealed in a report it undertook last year with Guidewire Cyence, a cyber risk analytics modelling firm. In the report, *Counting the cost: Cyber exposure decoded*, it was revealed the potential economic impact of a malicious hack that just takes down one cloud service provider would cause losses of $53 billion.

By comparison, Superstorm Sandy, the second costliest tropical cyclone on record, is generally considered to have caused economic losses between $50 billion and $70 billion. Yet despite reports indicating mammoth losses, which could shake confidence in whole sectors and the broader economy as a whole, roundtable participant Professor Jill Slay, who is the director of cyber security at ACS, says Australian boards seem to have no clue about what they need to do.

Professor Slay, who has worked closely with government and defence around the world on cyber crime and is the Optus chair of cyber security at La Trobe University, said she had been working with governments since 2003 on cyber security and has basically seen nothing happen.

She said Australian business is well behind its counterparts in the United States and in Europe because the government will not enact any real legislation or regulations with teeth when it comes to cyber security.

According to Professor Slay, whenever she suggests Australia follows the lead of another nation, such as the US, the usual response is: "We're not like that, that's the Americans. We don't regulate. We persuade industry."

The upshot of all the industry persuasion is "we're still having the same conversations of 15 years ago".

Head of the International Cyber Policy Centre at the Australian Strategic Policy Institute, Fergus Hanson, said Australian board directors basically consider cyber security an IT issue.

Hanson said most company board directors just do not know what to do because the language of cyber security is impenetrable.

"We use coded language and jargon when the issue at hand is not that different from what would happen in a normal business. Basically, if you smash a window in a shop, you patch it up," Hanson said.

Understanding how best to patch things up means individual businesses need to get a better understanding of where their exposures are for a start, said Maria Milosavljevic, who is the NSW government chief information security officer and ACS cyber security technical committee chairperson.

She said if you do not understand what information you have, what services you provide, and what the impact is of a cyber attack "on people and on other organisations when they're taken offline or destroyed or corrupted, you can't prepare and you can't respond and then you'll never be cyber resilient.

> **There's a lot of work to be done on creating a cyber security culture.**
> Professor Jill Slay, ACS director of cyber security

"Step one is you have to ask those fundamental questions and don't stop at information.

"It's also about services, critical or otherwise, and when you're thinking about information, don't stop at personal information – it's intellectual property, your finances and everything you own," she said.

For Milosavljevic, organisations need to know how they will respond all the way down the line and have a solid plan in place because trying to plan when something inevitably goes wrong will just cause panic.

"Who's going to do what when something goes wrong? You have to have a play book. It's just like if we have a massive bushfire, we have all sorts of things in place that we do and we step up and we just execute. It's not just about putting the fire out but actually knowing how to recover from the harm. For example, if you've got personally identifiable information, and now your customers are at risk because their information could be sold, what's your responsibility in minimising that impact for them?"

Head of cyber security at Singtel Optus Simon Ractliffe agreed getting the response right was vital. He said organisations can myopically over-focus on protection but we need to accept that all protection systems will fail, so getting the response right is critical.

For Hanson, determining how you prepare centres around whether you are a small business or large business. He suggests small businesses have to have a more modest plan but whether you are large or small the two most important things to think about at a strategic level is the response and communications plans. Of those two, having a solid communications plan in place will have a huge effect on the future of your business.

"When an attack happens, how are you going to relay that to your customers, the public, if you're a public-facing brand and that's a piece where a lot of people let themselves down," he said.

For Professor Slay, this means getting the administration processes right in an organisation like having a central corporate information security committee with the mission statement given by the CEO.

"Committees across the organisation where you pull everybody together to understand the risk from different perspectives. There's a lot of work to be done on creating a cyber security culture. Figuring out how you're going to run the ship from the bottom up with internal training and external training and once you've got all those into place, you've got some kind of assurance for a board that you are actually building a set of controls."

Practice director of cyber security and risk at GHD, Gavin Matthews, said it was pretty simple to figure out how critical building a strong cyber security capability was to a business.

"You have insurance for your physical assets. Cyber security is insurance for your digital assets."

Integrated approach required for security

Protection

Ian Grayson

Achieving an effective level of cyber resilience requires organisations to adopt a holistic approach to security that extends far beyond the IT department.

Participants in the round table discussion, hosted by *The Australian Financial Review* and the Australian Computer Society, agreed a new approach is required to ensure security issues and tactics become embedded in all areas of business activity.

Jill Slay, director of cyber resilience initiatives at the ACS, says that – all too often – cyber security is viewed by boards and senior managers as a technical issue that needs to be solved. This attitude needs to change if Australian businesses and public sector organisations are going to withstand the growing range of cyber threats causing problems around the world.

"We haven't treated information security or cyber security as a multidisciplinary issue," says Slay. "We haven't had generations growing up who understand law and policy and technology.

"You can't solve the problem unless you actually understand what it is you're protecting and how you'll protect it. Until we've come to grapple with that a bit more, I don't think we're going to solve the problem."

Maria Milosavljevic, chief information security officer for the New South Wales government, agrees that a broader approach to cyber security is required within organisations of all sizes.

"If you get an electrician to fix the wiring in your house, you don't have to have a safety person with them – they know safety, and they were trained on safety," she says.

"But we've still got graduates coming out of universities who can code, but they don't know how to code securely. We've got to reframe what a professional looks like in this space."

Simon Ractliffe says cyber security is all about timing. PHOTO: JEREMY PIPER

Milosavljevic points to the evolution of motor car safety as the type of path that needs to be followed when considering cyber security and resilience. As cars become faster and more powerful, risks increased and more controls and safety features were added to reduce risk of injury.

"We've evolved and adapted and said, we're not prepared to tolerate that risk, and so how do we minimise that risk to something that we think is actually tolerable. It's about finding that balance."

Acknowledging the approach taken by car manufacturers, Singtel Optus head of cyber security Simon Ractliffe says that when it comes to cyber security, the challenge is one of timing.

"There needs to be sense of urgency," he says.

"To train an architect to think as a security architect [and ensure] everything is cyber secure by design is going to take some time to evolve – I'm not sure we have that much time."

Gavin Matthews, cyber security and risk practice manager at GHD, agrees, saying the threats facing Australian companies are growing at an increasing rate. "We're up to a major breach every fortnight, so the reality is we've got to get better at this," he says.

"In organisations here in Australia, boards and C-level executives need to understand the questions to ask. Taking that information and doing something with it, that's the key thing."

From previous page

Too many businesses ignoring risks

people that use our public hospital networks, to our staff, to our students within our public education system."

Chris Casswell, director of enterprise security at Micro Focus, said it is important for individuals and organisations to understand their responsibilities when it comes to guarding against cyber attacks. It is not sufficient to simply expect that someone else will do the heavy lifting.

"The reality is that you can't outsource risk," he said. "And, as much as organisations and governments want to have a third party take on a little risk for them … the reality is you can't. It's the responsibility of the organisation to secure its own data, its own access and the identity of the individuals that are accessing that data."

Participants agreed a consistent, long-term approach is required to ensure Australian organisations develop the level of cyber resiliency that will be needed in coming years. Any failure to do this could have significant negative ramifications for business and individuals.

Personal data the most targeted by attackers

Privacy Healthcare information is simply not secure enough.

Mark Eggleton

Australians are completely unaware as to how susceptible their personal information is to a cyber attack, according to most participants at *The Australian Financial Review* and ACS roundtable on cyber resilience.

Furthermore, just as the federal government continues its roll out of its My Health Record digital health scheme, it is the one sector continuing to see the most data breaches here and overseas. According to the Office of the Australian Information Commissioner, out of a total of 242 breach notifications from April 1 to June 30 this year, 49 were reported by the health sector.

This was also reflected in Chubb Insurance's global claims data report that tracked the number of cyber incidents over the past decade.

Chubb's report found 38 per cent of cyber incidents occurred in the health sector with professional services second at 16 per cent.

Head of the International Cyber Policy Centre at the Australian Strategic Policy Institute, Fergus Hanson, said healthcare was the single most sensitive type of data we have in the whole country, including intelligence sources.

"Yet it's the most targeted as we know now, and it's the most state-based and yet we don't have the resources to put into securing it," Hanson said. "Reason being is if you ask the hospital if they're going to allocate funding to the emergency ward, or to some security system – it's a no brainer."

Practice director, cyber security and risk at GHD, Gavin Matthews, said it is the most valuable data of all to criminals. "It's 10 times more expensive than credit card data on the dark web," he said.

Away from the health sector, vice-chancellor of La Trobe University, Professor John Dewar, said the tertiary sector has had to change its mindset. In the past universities have all been about openness and sharing but "it's clear now that we're being breached".

"There are people who are interested in research data and in the various data records we hold about staff or students.

"We are big organisations so we have to make a big shift from one of openness and transparency and accessibility to one where we're much more aware of the risks of being breached and compromised in various ways," Professor Dewar said.

For Hanson and Matthews, the key is for organisations to be held more personally responsible for data breaches.

Unfortunately, at present it is mostly left to the individual and when their data's out there on the dark web, it is the individual who has to cancel their licence and credit card or something more drastic to avoid exploitation.

Bearing this in mind, Australia will not be on the right path towards building cyber resilience "until the companies and boards and owners are actually held personally liable for breaches as they are in other parts of the world," Matthews said.

For Hanson, getting it right might mean changing the way of thinking where organisations gather personal data under the auspices of getting to understand their customer better.

He says a new model might involve pushing data out into the hands of multiple stakeholders rather than it being held in one place representing a single point of failure, such as a single cloud service. What worries Hanson is that the way we are collecting data is increasingly disempowering people.

"We're taking away rights and people are getting their privacy stripped away. For example, health records used to be stored in your local GP's office. The chances of somebody breaking in and stealing your personal files was very remote, and the chance that some other doctor being able to get access to your GP's file was just too much hassle, and so it would never happen.

"Now we've got a honeypot of data where it's all suddenly available and it's actually going to be at some point breached."

He said governments and business needed to just put the citizen back in the driving seat so individuals control their data. "It's a total change of mindset from what we do at the moment."

Fergus Hanson says resources are lacking to protect medical data. PHOTO: JEREMY PIPER

> **Now we've got a honeypot of data … and it's actually going to be at some point breached.**
> Fergus Hanson, Australian Strategic Policy Institute

We don’t do enough to keep systems safe

Philip Dalidakis worries an attack on the apparatus driving the Victorian digital economy will hit confidence. PHOTO: JEREMY PIPER

Digital economy Threats put our economy at risk.

Mark Eggleton

When the alleged Chinese Intelligence Services breach of the Australian Parliamentary computer network was discovered in 2011, reports at the time suggested the breach had been ongoing for up to 12 months or more.

Seven years later and ACS director of cyber security, Professor Jill Slay, says we are fighting a war right now and many people in business and government have no idea of the nature of the battle.

Professor Slay, who has worked with governments around the world on cyber security issues, said at the Cyber Resilience roundtable in Sydney hosted by *The Australian Financial Review* in partnership with ACS that Australia’s lack of cyber resilience is a huge problem of vital national importance.

She said it is about keeping our critical systems safe, but we are not doing very much about it.

NSW government chief information security officer and ACS cyber security technical committee chairperson Maria Milosavljevic agreed and said there is life and health at risk.

“Our financial position is at risk. Our entire national economy is at risk,” Milosavljevic said.

Professor Slay said there is no doubt a state-based actor using something as simple as a laptop can spin a generator and take out a whole state’s worth of electricity.

“I have no doubt that they can do it and if we close our eyes to this, there is a huge risk we’re not managing. I would expect the government to take notice of this and do something about it because at least the Americans have had a go, at least the British have had a go but I’m not convinced we’ve had a go,” she said.

Victoria’s Minister for Trade & Investment, Innovation and the Digital Economy, Philip Dalidakis, said he cannot do anything to stop a state-sponsored actor from getting any information they want.

“I work off that basis every day of my life. I work off the basis that my phone is being listened to whenever I’m on it,” he said.

“I work off the basis that anything that I do, somebody else is seeing. Unfortunately, that’s the world that I live in. About 99.9 per cent of the community do not work off that basis, nor do they have those fears.”

What worries Dalidakis is how an attack on the apparatus driving the Victorian digital economy will impact confidence and people’s ability to use the system.

“If you’re trading through access of the internet, if you are dealing in terms of internal and external communications using the web, if you are using cloud-based systems that you don’t understand but you have been sold, all of this contributes to the digital economy, and you can, with very little effort, destroy people’s confidence to be able to use it whether they are doing their banking, whether they are doing their payments, whether they are purchasing, whatever the transaction is and that will be one of the largest, most challenging things for a government to get across.”

If we close our eyes to this, there is a huge risk we’re not managing.
Professor Jill Slay, director of cyber security, ACS

For Dalidakis, it is community confidence around everything we do that poses the biggest threat because it could cripple whole communities “in terms of their behaviour and what they do and how they function”.

Milosavljevic agreed there is a real problem in regard to crumbling community confidence in institutions because of constant cyber security issues.

She drew attention to the ongoing Robert Mueller investigation in the United States concerning alleged Russian meddling in the 2016 presidential election as there is “all this fear and uncertainty around electoral fraud because the Russians hacked democracy”. “They hacked people. They hacked social media. They targeted people’s confidence in democracy.

“That’s what they were actually trying to do, and that’s what we have to stop and also ask ourselves, how should we respond and whose responsibility is it?”

The head of the International Cyber Policy Centre at the Australian Strategic Policy Institute, Fergus Hanson, said it is a global problem requiring a concerted global solution.

“Currently, the logic of the nation state level is to say, ‘Let’s protect Australia enough so that they go after New Zealand instead’. And that’s essentially the logic that we are buying into, of helping ourselves and making sure they go after somebody else.

“The way that we’ve been approaching cyber crime is a broken model. What we do at a state level is we invest in state-based police forces who then get the reports and they send them down to local area command and they triage against their open books, they say we’ve got a break-in, we’ve got a car stolen, someone’s been assaulted, and we got somebody who lost $20,000 to some country. Let’s triage that out of existence and close the case.

“And that is essentially the model we currently have when it is an international problem so at an international level we need to change the way we approach cyber crime and realise we cannot just be Team Australia and understand who our partners are in this, and ask how do we make a serious dent in this problem.”

Internet of Things could be most vulnerable point

Hacking Malicious actors can get into the most common devices.

Mark Eggleton

More than 90 per cent of malicious botnets are driven by IoT, says Gavin Matthews. PHOTO: JEREMY PIPER

When Russian President Vladimir Putin handed a football to US President Donald Trump just after this year’s World Cup a few alarm bells went off in the United States as the ball had a transmitter embedded in it.

While the transmitter was completely innocuous and was part of the manufacturer’s marketing efforts, the alarm was raised because there may have been potential for an external actor to hack the transmitter.

The football incident brought into focus the essential weakness of the Internet of Things (IoT) and how easy it is for malicious actors to hack into devices ranging from phones to internet cameras and more.

At the Cyber Resilience roundtable hosted by *The Australian Financial Review* in partnership with ACS, practice director, cyber security and risk, at GHD Gavin Matthews said well over 90 per cent of malicious botnets are being driven by IoT.

Part of the reason is IoT devices are cheap and when they are connected to the internet they are impossible to secure. Professor Jill Slay, who is the ACS cyber security director, said there is no way of updating them and we will never be able to secure them. Moreover, quite a number of people have figured out how to use them for a targeted attack.

Professor Slay said we are importing these cheap Christmas stocking-stuffers from around the world and we are actually allowing people to attach them to workplace computers and critical infrastructure and, unfortunately, despite assurances from government and business “we cannot secure IoT”.

For Matthews, the problem with IoT security is it is only going to escalate, especially as cyber crime becomes much easier to perpetrate.

It is only going to escalate as cyber crime becomes much easier.

“It is going to be worth $6 trillion by 2025 so when it’s outstripping the global drug trade by double the amount, criminals are going to be doing things the easiest and cheapest way possible. They’re just like any other corporate organisation and with IoT we’re just making it easy for them,” he said.

NSW government chief information security officer and ACS cyber security technical committee chairperson Maria Milosavljevic suggested no business or government department should allow IoT devices in the workplace but it is very difficult to police.

“Even if you say your company is compliant and it’s Essential Eight compliant [as specified by the Australian Signals Directorate] there’s always certain parts of a business or government department that thinks it can do something better so they’ll go and use an outside cloud service or buy an IoT device.

“I’ve even had a situation where people went down to a local electronics store, created their own server and then connected it to my network. Basically government (in particular) should not buy IoT devices,” Milosavljevic said.

For Matthews the horse has already bolted and “there is no security perimeter, it has disappeared”, in terms of IoT usage. He said the best we can hope to do now is to mitigate against further breaches by building more layered defence mechanisms and protecting the core parts of a business or organisation you cannot do without.

Fellow roundtable participant Singtel Optus cyber security chief, Simon Ractliffe, spoke of a new phenomenon termed “living off the land” where a malicious organisation might break into your environment and “actually use all of your tool-sets to propagate their own needs”.

“So, they’ll use your architecture, your tool-sets, your software distribution tools to run their own agenda within your organisation.

“Organisations just need to do the basic stuff and certainly one of the great services that we’ve seen is the Australian Signals Directorate disseminate the Essential Eight and if organisations simply heeded those things, they would find themselves immune to so many of the real threats of today.”