# Cyber resilience

www.afr.com | Wednesday 21 June 2017

*Edited by Jason Clout: jcloutfairfaxmedia.com.au*

# Many businesses at risk from hackers

**Strategy Companies need a collaborative approach, say experts.**

**Ian Grayson**

Awareness of the severe risks posed by cybercrime is increasing within Australian organisations, yet many remain unprepared for an attack, experts have warned.

While incidents such as the recent WannaCry ransomware attack have focused attention on the need for effective IT security, the rising sophistication of cyber criminals means the threat landscape is constantly changing.

"Cybercrime is the number one threat that the business community is facing, and the cost is conservatively put at $1 billion a year to our economy," says Dan Tehan, Minister Assisting the Prime Minister on Cyber Security. "The business community has to be aware that the threat is going to continue to evolve."

According to the latest MaturityScape Benchmark report on IT security from research company IDC, more than 60 per cent of Australian businesses are taking only a basic or reactive approach to security issues.

As a result, they could find themselves challenged if the target of an attack.

IDC analyst Lydie Virollet says while corporate awareness has been strengthened by the recent high-profile incidents, Australian companies still lag their counterparts in the United States and Europe.

"The threat landscape is shifting from high-volume 'spray-and-pray' techniques to more targeted attacks, many of which come via email," she says. "Australian companies don't necessarily have the skills they require in-house [so we are] seeing an increase in use of managed security services as a result."

Security experts agree there is a role for government as well as the private sector when it comes to improving Australia's cyber security readiness. The launch of the federal government's national cyber security strategy in 2016, which featured 33 initiatives together worth $231 million, is widely seen as a positive move.

IBM security solutions business unit executive John Vine Hall applauds the establishment of the Australian Cyber Security Centre but says there is also a role for companies to work more closely together to meet the rising challenge.

"What's key is collaboration," he says. "The bad guys are very good at sharing their knowledge and methods of attack, but we don't have the same level of collaboration and knowledge sharing between companies."

Vine Hall says it is key to make sure that any cyber events that occur within one organisation are understood by others.

"We need to shift from the point of view that a cyber event is something that should be swept under the covers and hidden to one that allows us to learn from each other's mistakes and improve our security position as a country," he says.

Companies also need to recognise that cyber security is no longer something that is handled in isolation by the IT department. Simply assigning a team of technicians to the problem is not the most effective approach.

"We are seeing a change in the level of accountability," says Vine Hall. "Boards are taking a more active role in security, but more education is still needed."

"More companies need to shift from the mindset that if they spend a certain amount of money on cyber security the problem will go away. The more prepared they are, the better the outcome will be."

Microsoft Australia's chief technology officer, James Kavanagh, says while awareness of cyber security threats is certainly increasing at senior management levels, there can sometimes be a challenge in how an organisation responds while also balancing demands for innovation.

"Security approaches that support and enable business demands while informing risk-managed security controls will always be the most sustainable and effective in the long run," he says. "And Australian organisations, both in government and enterprise, still would largely recognise they've some way to go in establishing that kind of balance."

Dan Tehan, Minister Assisting the Prime Minister on Cyber Security, says the cost of cybercrime on the economy can be conservatively put at $1 billion a year and businesses must realise that the risks continue to evolve. PHOTO: ANDREW MEARES

Kavanagh says in many cases it is not a matter of businesses allocating more spending to cyber security initiatives. Instead, taking a different approach to the way in which technology infrastructures are built could deliver a better outcome.

"Some government organisations and businesses are actually spending more than they should, maintaining security of legacy applications and technology platforms that could be better secured by moving to the cloud or modernising their applications," he says.

**The bad guys are very good at sharing their knowledge and methods of attack.**
John Vine Hall, IBM

"It's interesting to note that the Essential Eight [a set of security controls recommended by the Australian Signals Directorate] puts the greatest emphasis on controls that really don't require additional layers of technology or any new tools or services, just modernisation and patching."

Although incidents such as the WannaCry attack, which infected more than 230,000 computers across 150 countries, capture significant attention, security experts emphasis ransomware does not actually represent the largest threat.

Australian organisations are more likely to fall victim to phishing attacks where criminals target small groups or even individuals with emails that appear legitimate but actually contain rogue code or a link to an infected website.

"The incidence of malware and credential theft through phishing emails is greater in volume and the consequences of an advanced attack on business or government is probably more damaging, but certainly ransomware is a significant and growing threat," says Kavanagh.

# Brace for next ransomware strike

**Solutions Building effective barriers must be led from the top.**

Ian Grayson

The increasing complexity of business IT systems is causing growing challenges for the teams tasked to manage them.

Responsible for everything from corporate data centres and cloud platforms to mobile devices and networks, many teams are struggling to ensure their infrastructures are secure enough to ward off cyber threats.

"This can mean that basic steps such as applying software patches may be overlooked," says Jack Chan, network and security strategist at cyber security specialist Fortinet.

"In an ideal world, if everyone applied patches, the recent global WannaCry ransomware outbreak would not have happened."

The high-profile WannaCry attack exploited a known vulnerability within Microsoft's Windows operating system for which an update patch had been issued. Unfortunately, many organisations had failed to apply it.

Businesses and their IT departments are facing cyber threats on a variety of fronts, and one of the most challenging is around usage of mobile devices. As well as ensuring the devices, such as phones, tablets and laptop PCs are secure, the connections they use to access centrally stored data and applications must be carefully managed.

According to the most recent Threat Landscape Report produced by Fortinet, the proportion of malware targeting mobile devices rose from 1.7 per cent in the fourth quarter of 2016 to 8.7 per cent in the first quarter of this year. The report found about 20 per cent of all organisations have detected it within their IT infrastructures.

Chan says it is important to be aware of the security threats posed by mobile devices as they become more widely used by staff. Just because problems have not been seen yet does not mean an infrastructure is secure.


Organisations around the world like this South Korean monitoring centre are gearing up to deal with the next ransonware attack even as businesses and their IT departments face cyber threats on a variety of fronts. PHOTO: YONHAP

"There is a famous quote that says there are only two types of organisations," he says. "There are the ones that have been hacked, and ones that are going to be hacked."

Another area of focus for security teams is the increasing usage by their organisations of cloud platforms and services. This is requiring a rethink of security strategies and areas of investment. "If you think about how security has been architected over the years, it's tended to be on the premise that someone was sitting inside a building and connecting to a server in the same building," says Christopher Campbell, director, solutions product marketing – security at technology company VMware. "The security solutions in the industry were therefore designed to address that scenario."

**It is important to be aware of the security threats posed by mobile devices.**

Campbell says that, now businesses are moving workloads and data storage into the cloud, a new approach is required. If a decision is taken to retain some IT resources in-house and shift a proportion to the cloud – known as a hybrid cloud architecture – the security challenge becomes even greater.

"In a lot of cases businesses don't have competency to do this internally," Campbell says. "They will have to increase their budgets and leverage experts to help them do this."

To achieve the best outcomes when it comes to IT security, many organisations are going to have to rethink how the area is managed, adopting a top-down rather than bottom-up approach.

Campbell says a business might have someone responsible for cloud platforms, another for the data centre and others for applications and mobile devices.

"We have found that you have to take this up to a higher level in the organisation," he says. "Those who are successful are doing it from the board level. They have the authority to lay down a strategy to ensure all these parts will work with each other."

By rethinking their approach to management, businesses can be better placed to have a resilient barrier around their IT systems and resources.

# Our right to privacy threatened

**Digital identity**

Mark Eggleton

Australians may need to find a whole new way to communicate in the digital age if we do not want to completely lose the right to privacy, suggests Professor David Lacey, one of the nation's leading cyber security experts.

A Professor in Cyber Security at the University of the Sunshine Coast and managing director of national identity and cyber support company IDCARE, Lacey says the community is at year zero when it comes to cyber security and we are well behind where we need to be.

He says the vast majority of Australians are naive when it comes to issues of cyber security as we happily share a treasure trove of our personal details online. What's more, organised crime networks know the best place to misuse personal data is online.

"We're already seeing a huge amount of misuse. At IDCARE we have recorded over one million scam calls alone and one major telco reported to us the number might be more than 10 million," Lacey says.

Part of the problem is the cyber environment is influenced by a handful of players and while they are delivering great service to consumers, their actions (when it comes to collecting personal data) are overt on one hand but not so overt in the way they handle the data.

"The great irony is we all focus on China or Russia potentially hacking into our systems but we don't bat an eyelid when it comes to giving information to public companies," Lacey says.

Many people still do not understand that the nature of the internet means we are giving up a large part of our right to privacy. Lacey points out that while the right to privacy is a legal right it is increasingly becoming an impractical right in the modern world as we conduct more of our lives online.

For Lacey, creating better knowledge of cyber security is a shared responsibility. While the pressure seems to fall on business and government, he says the community needs to better educate itself and this has to start in schools and move beyond.

"We have to be innovative in how we educate people and it has to cross generations."

The managing director of cyber safety specialists Family Zone, Tim Levy, agrees there needs to be a drastic increase in education around cyber security in schools and in business.

"People don't understand cyber safety and there are many stories about people who traded away their privacy to get more access online. The internet is designed to target our base instincts. It's like a slot machine, it's designed to be intoxicating," Levy says.

His company works with schools and business to try to build a cyber culture in each organisation through education and a technology solution.

"In the past, schools would suggest their responsibility stopped at the fence but they now understand their duty of care, when it comes to cyber safety, extends far beyond the fence especially as the issue gets worse."

Levy believes things are only going to get worse, especially among young Australians who often no longer make a distinction between their online and offline world.

Ideally, he says families and business should be able to create a "virtual walled garden" so they can protect their privacy and data.

For Professor Lacey, that "walled garden" is going to be increasingly hard to create.

# More skilled staff needed all around

**Training Australia has to react to the growing requirements.**

Joshua Gliddon

Australia faces a severe shortage of qualified cyber security personnel. According to some estimates, the nation needs between 9000 and 11,000 qualified people to meet the security challenges of the internet age, yet we are training only a handful.

"We do not have the people, we do not understand what cyber security means, what a cyber security professional is, or how they should be trained," said Professor Jill Slay, director of the Australian Centre for Cyber Security, in Canberra.

Research done undertaken by the Australian Computer Society (ACS) indicates the average cost of a cyber attack to an Australian business is about $276,000. Globally, cyber attacks cost as much as $500 billion a year.

"Demand for cyber security professionals has grown 57 per cent in the last year," says an ACS representative in a statement. "Australia is already facing a critical shortage of skilled ICT professionals, which makes meeting demand a significant challenge."

Yet there is more to this skills shortage than meets the eye. Not all cyber security professionals are created equal. It is not correct to state that Australia needs 11,000 high-level hackers; what's needed are professionals from across the cyber security spectrum.

"We are definitely not on track to deliver 11,000 new professionals in the next three years," Slay says. "We have also been very slow to respond to the growing need for security professionals."

The US and UK identified the need for a massive increase in cyber security professionals many years ago. More to the point, they put in place programs to address the skills shortage, something Australia has failed to do.

"If we look at what the US, UK and China have done, they have put together public policy with education policy and they have invested in cyber security," Slay says.

There is an increasingly coordinated approach to IT training in Australia, similar to programs found overseas.

She laments that until recently, successive Australian governments have identified the shortage of cyber security professionals as a problem, but done little about it.

That could be changing, with the government releasing its Cyber Smart Action plan in 2016, which hopes to address "the shortage of cyber security professionals in the workforce through targeted actions at all levels of Australia's education system, starting with academic centres of cyber security excellence in universities".

The Australian government has also invested in the establishment of the Australian Cyber Security Research Institute (ACSRI), which is a coordinated research and education effort between government agencies, the private sector and researchers.

"Overall, with the Cyber Smart Action plan and the legislation regarding breach notifications, I think that we are on the right track and generally doing the right thing" Slay says.

What's clear, however, is that making up the skills shortfall is not the work of a moment. "We are generally good at what we do in this area," she says. "And I don't think [the skills shortfall] necessarily makes us more vulnerable."

The chairman of the Australian Cyber Security Research Institute, David Irvine, says the real threat to cyber security is that methods of attack are changing every day. PHOTO: LOUISE KENNERLEY

# Defences improving but still vulnerable

## Networks Solutions are always having to play catch-up.

Mark Eggleton

Australia still has a long way to go when it comes to cyber security – several senior sources inside and outside of government say there are enough issues of concern around to make us potentially vulnerable to a large-scale cyber-attack.

One major issue is while we blithely talk about cyber security and the meddling of the Chinese or Russian governments on a geopolitical front we tend to ignore how cybercrime is broadly based against everybody. Its very nature means we cannot really make a distinction between state and non-state activity.

The reason is the same tools available to most state actors are also available to a wide variety of individuals and groups. This combination of threats makes it an issue for government, business and the individual.

So, while the federal government's Cyber Security Strategy ticks all the right boxes when it comes to formulating an integrated solution involving training, innovation and outreach by government, the big question inside the intelligence community is whether the strategy is being implemented or is there a long way to go?

According to the former head of ASIO and chair of the Australian Cyber Security Research Institute, David Irvine, the government's strategy is a great step forward but there still is a long way to go, although, he says we are on the road to developing a cyber industry in Australia.

For Irvine, the real threat is the nature of cyber security and the fact it is always moving.

He says it is going to be a constant for industry and government for a long time, and will never be solved all in one hit.

"It's essentially a new vector for committing old crimes. A new way to rob an old lady or conduct espionage and organised crime is tumbling over itself to develop ways to extort money among other things," he says.

Irvine says the issue is hugely complex but we need to develop cyber expertise in Australia as a matter of urgency.

"You have to remember a whole lot of people are putting a huge investment into the area such as the Chinese, Israeli and Russian governments as well as inside technology hubs like Silicon Valley.

What's more in countries such as China, Israel and Russia, the governments offer a lot of support to their homegrown cyber sectors and when the government steps back, industry steps forward, says Irvine.

> **It's hard to see when we're going to get ahead of the curve.**
> Craig Davies, Australian Cyber Security Growth Network CEO

"Israel has built an entire ecosystem around cyber security."

Chief executive officer of the Australian Cyber Security Growth Network (ACGSN), Craig Davies, agrees we need to have a viable industry here as there are many things that need addressing – and soon.

"The federal government's strategy is to build the sector here and they're pushing it really hard so we're starting to see some good momentum but how do we go faster? The attacker always has the advantage just because of the core design of the internet. It's open source so security is always going to be retrofitted," Davies says.

"It's hard to see when we're going to get ahead of the curve so the key now is to ensure Australian business understands the whole problem."

According to Davies the good news is Australian business is beginning to get a better grasp on the matter.

"In the past, the knowledge at board level was virtually non-existent but this is improving as boards are starting to ask questions. What we need to do now is build the security sector here and ensure we end up with a strong sovereign capability," Davies says.

"The Department of Prime Minister and Cabinet are working hard and being very proactive in building Australia's capability quickly."

Without doubt the department is building on Australia's already considerable cyber expertise in the government sector.

In organisations such as the Signals Directorate, ASIO, the national Computer Emergency Response Team (CERT) and the Australian Federal Police we have made a good start but the business sector really needs to step up to the plate.

More often than not their business models take preference over cyber security risks.

In many ways, it would make sense for business to shoulder more of the load when it comes to cyber security as a social responsibility. A good example is the global response to money laundering where many governments abdicated their responsibility to the banks.

Australia's own Anti-Money Laundering and Counter-Terrorism Financing Act 2006 imposes obligations on business to identify and report transactions of a suspicious nature to the appropriate authority. Similar laws exist around the world.

Bearing this in mind, what would be the difference in any of the social networks developing software to recognise terrorist websites (for example) and block them?

As Irvine says, cyber security is a constantly mutating threat and it is hugely important we get it right.

"It's changing every single day and [at the moment] the solutions are running behind the problem."

# Industry Insight

Industry comment by
**Anthony Wong**
President of the Australian Computer Society

**This content is produced by The Australian Financial Review in commercial partnership with the Australian Computer Society (ACS).**

We are finally at a place now – thanks to widely publicised attacks that occur on an almost weekly basis – where awareness of cybersecurity is at an all-time high.

We've even seen how the best-laid plans can fall short, as demonstrated by the DDoS attack of the Australian Bureau of Statistics eCensus website last year.

But being aware and taking action don't often go hand-in-hand. We are notorious as a species for thinking it always happens to someone else (until it happens to us) and for putting in place rules and regulations after the damage is done, thinking it will prevent future occurrences. But this doesn't work for cyber: the goalposts are constantly moving. Current threats evolve and new ones appear on a daily basis.

Gemalto's latest Breach Level Index revealed that 1.4 billion data records were compromised last year, an 86 per cent increase over 2015. In Australia alone, in the last financial year, AusCERT (Australian Computer Emergency Response Team) responded to 14,804 incidents affecting Australian businesses, 418 of which involved systems of national interest and critical infrastructure.

It is now an accepted truism that no system, no network, is impenetrable. It is not possible for a company or organisation to guarantee a breach won't occur, or that it can prevent personal data being stolen or its business processes being interrupted.

A cyber incident at your workplace then is not an if, but a when.

And when it happens, the cost can be measured in a lot more than red faces – according to the latest ACS Australia's Digital Pulse 2017 report, the average cost of a cyberattack to an Australian business is around $419,000, up from $276,000 two years earlier.

Cyber resilience, then, is now a critical business process. It is the practice of being prepared. Having policies and procedures in place to deal with the inevitable breach as well as clear steps on how to minimise the impact, mitigate consequences, and getting the business back online. The calibre of your organisation will be measured by how it responds.

A good cyber resilience framework is built upon two pillars:

**Education:** At all levels, from boards and C-suite management to the receptionist at the front desk. Some of the most damaging breaches use social engineering or the manipulation of people to gain a foothold. All it often takes is an innocently clicked email link to put an entire organisation at risk. If you hold a position of authority, it falls on your shoulders to ensure your organisation or your department has a cyber resilience plan in place.

**Skilled professionals:** There can be no cyber resilience without the knowledge capital and skills of trained ICT professionals able to build cyber solutions to protect your systems and to carry out best practice in the event of a breach. This itself builds upon recognised certification and professional ethics.

> *We are notorious as a species for thinking it always happens to someone else (until it happens to us).*

The good news is that as an industry, we are growing rapidly – 40,000 ICT jobs have been created in the last two years alone. According to SEEK, ICT roles were the most advertised jobs in 2016.

Going forward, Australia's Digital Pulse 2017 also identified that cyber presents a significant growth opportunity, with the potential to create an uplift of 5.5 per cent in business investment, a 2 per cent increase in wages, and the employment of an additional 60,000 people by 2030.

Bearing this in mind, ensuring your organisation has a solid cyber-resilience framework in place underpinned by skilled ICT professionals isn't just good for your business, it's good for Australia too.


Hackers are becoming more active all the time. Current threats to businesses and organisations evolve and new ones appear on a daily basis.

# No one immune from hack threat

## Counter measures
**There is a constant need to adapt to risks.**

James Dunn

When one of Australia's richest people, mining billionaire Andrew Forrest, went public in 2015 with the admission that he had been cyber-hacked, it was a stark reminder that no one was safe, Despite the tycoon presumably having state-of-the-art cyber-security measures in place, hackers managed to rip off $615,000 as it was being digitally transferred between accounts.

Last year, information security company Dell SecureWorks said Australia was the third most targeted country of 17 examined in a report on banking "botnets", which refers to computers that maliciously launch repetitive tasks to damage information systems. And according to the security company Kaspersky, Australian banks were among those targeted by the Carbanak campaign, which was discovered in 2016: over a period of 18 months, cyber criminals targeted 100 banks in 30 countries, stealing a reported $US1 billion ($1.3 billion). Carbanak used the "spear phishing" technique, which encouraged some high-level staff to download the malware, which then moved into the bank systems to issue transfers – and even order some ATMs to start dispensing cash.

More recently, the "WannaCry" ransomware attack in May – believed to be the world's biggest online extortion attempt – struck more than 100,000 organisations in 150 countries, including British hospitals, German rail operators and Chinese universities. Britain's National Health Service had to turn away patients after WannaCry locked up hospital computers, forcing the closure of wards and emergency rooms. WannaCry is believed to have emerged from North Korea.

Cyber-security is "a constant game of cat-and-mouse," says Graeme Speak, founder and chief executive officer of BankVault Cyber Security. "Whatever protections a bank puts in place today, the hackers work on that and find a way of cracking it, and then the bank has to work on leap-frogging them again."

Speak says Australian banks, particularly the big four, are "very good" about cyber-security in terms of their internal processes, but the "unavoidable problem" is that their customers' systems may not be secure. And because everyone wants to do their banking online,

Andrew Forrest was the target of a cyber attack a few years ago. PHOTO: PAUL JONES

that is a recipe for problems. "The bank systems are safe – the problem is always the end-point device that the customer uses. Take your PC: the bank has no control over who you share that computer with, or what other software you've installed on it, and quite simply, no one can ever guarantee the integrity of that interaction."

Nor is the smart phone – on to which digital banking is increasingly moving – safe.

Earlier this year, in Germany, hackers managed to drain customer bank accounts not by hacking the banks themselves, but by exploiting a long-known weakness in a global telephony protocol known as Signaling System 7 – a set of international telecommunications protocols – to redirect the text messages the banks used to send one-time passwords. The hackers used the mTANs – or "mobile transaction authentication numbers" – sent over the O2 Telefonica mobile network to transfer money out of the accounts.

"Previously hackers have targeted your PC using traditional malware to steal people's online banking credentials and break into their accounts, but effectively they've impersonated them," says Speak. "With the new technology they have, they don't have to impersonate you."

BankVault has just launched its SafeKeyboard product, an "invisible keyboard" that builds a pristine virtual machine at a randomised remote internet address, and runs completely independently of the customer's device.

"It allows the bank to control the security of that end-point for the time their transaction is happening, for a few minutes – that's all they need," says Speak. "It's effectively a safe window, within which it is impossible for hackers to intercept or see or use passwords, or see anything else they shouldn't."

While something like this "lifts the barrier again," maybe for five or even 10 years, inevitably "the hackers will eventually get around it," he says.

Banks must keep adapting to the ever-changing environment, and can "never afford to rest on their achievements," says Lynwen Connick, chief information security officer at ANZ Banking Group. But she adds that it is not just about managing the risks, there are opportunities as well.

"We're going through a digital transformation at ANZ and developing an enhanced customer experience through things like voice biometric security, digital wallets and our BladePay merchant device, and we are also developing improved cyber-security. The two go hand-in-hand."

Connick sees cyber-security as a "key enabler" of innovation and digital transformation. "We're working with a range of partners to promote innovation in security. Embedding security culture will ensure we can safely make the most of the opportunities the online world offers.

"There is also a broader opportunity to develop the right skill sets in our employees, and help develop cyber-security skills more broadly," she says. "There is a worldwide shortage of such skills and we are doing what we can to build them for the future."