PUBLIC SECTOR NETWORK

pwc

Cyber Security Executive Meeting Series 2021

Embedding Robust, Resilient and Proactive Infrastructure Security to Build Public Trust

10 – 26 August 2021

Sydney / Melbourne

Adelaide / Perth

Brisbane / Canberra

Cyber Security and Risk Management

Highlights of Keynote Sessions

Taking cyber security seriously

Protecting the integrity of computers and the data they hold has been part of the thinking of the IT industry since the beginning. As early as the 1960s, computer security was top of mind for agencies such as the CIA and FBI, but the technology was still in its infancy. Thirty years later computers were used by individuals in the home, not just in the office, whilst now, with the advent and prevalence of the internet, laptops, tablet devices and smart phones, the technology is much more advanced and convenient, and the threat to the security of the data is also much greater.

The Australasian region – once considered a remote backwater – can no longer sit back and wait to see what happens in the rest of the world. With the internet and the constant global transfer of information, we are as interconnected and therefore as integral to combatting the threat as any other world region. In fact, on numerous occasions, particularly since the start of COVID-19, the Australian government has said that the way Australia deals with the technological threats it faces will determine how it emerges from the pandemic. This is undoubtedly true of New Zealand and much of the rest of the developed world too.

The global cyber threat is now so pervasive and commonplace that most large enterprises and government departments not only have a chief information security officer (CISO), but an entire team to deal with digital security. Moreover, most Australian state and territory governments also have either a standalone department or an office within the Premier's department to deal with IT threats. Many global consultancies – particularly the 'big four' – are also heavily involved in dealing with the cyber threat and advising their clients how to best manage the impending risk.

This paper brings together a selection of the keynote presentations from experts across Australia and New Zealand as part of a Cyber Security Roadshow that was hosted in collaboration with PwC Australia and held mostly held virtually due to ongoing COVID-19 lockdowns in August 2021. Though each of the presenters came from different jurisdictions and a different perspective, it is remarkable that so many of their views were aligned and complimentary. Though, given the danger is universal, maybe that is not so remarkable after all. It might even be a lesson that if agencies can work together and collaborate on this issue, maybe they should cooperate on other issues too, and not just imminent threats.

The threat environment

Government agencies across the world are often attractive targets for cyber criminals because they hold vast amounts of communal and personal data that can easily be exploited or extorted for large sums of money. In Australia, the primary agency that monitors and aims to secure and improve the online environment is the Australian Cyber Security Centre (ACSC). **Jessica Hunter, the acting First Assistant Director-General of Cyber Security Services at the ACSC**, says that they are "continuing to see malicious actors repeatedly demonstrate their ability to take advantage of opportunities to cause harm to Australians, and in particular to governments." In fact, there has been "a shift in the threat environment on a national level."

Part of this shift is based on the fact that many people are working remotely or not in their usual way because of the pandemic. **Samantha Gavel, the Privacy Commissioner at the Information and Privacy Commission NSW**, says that "the onset of the pandemic has really accelerated trends that we saw were happening prior to the pandemic. This has led to much greater use of digital technology both in our personal lives and in our working lives." In many ways, these trends have "have brought us many benefits and have enabled us to work and learn remotely." But at the same time, they "have come with heightened privacy and security risks and incidents."

One of the reasons for that, as **Rachel Dixon, the Privacy and Data Protection Deputy Commissioner at the Office of the Victorian Information Commissioner (OVIC)** says, is because people are working from home but "not all agencies purchased laptops for their staff. This means that some computers are being shared at home and we have seen breaches where someone's family member inadvertently downloaded a Trojan or something similar." This is as true in Australia as it is in New Zealand. **Neville Bannister, the Senior Manager of IT Assurance at the NZ Ministry of Education**, says that "the number of cyber security incidents continues to soar as a result of our increasing internet presence, with a vast number of threats." It is very likely that "cyber-attacks will increase in frequency and in levels of sophistication."

Back at the ACSC, Jessica Hunter says that one of those threats is ransomware, which is "one of the most significant cyber threats currently facing Australian organisations." This is unsurprising given that ransomware is defined on the ACSC's website as 'a type of malicious software (malware). When it gets into your device, it makes your computer or its files unusable.'[1] Often cyber criminals demand payment in return for the files or threaten to destroy them. Ransomware can be particularly destructive because as Jessica Hunter says, "it requires minimal technical expertise, there's a low cost associated with it, and it can result in significant impact to organisations." In fact, because of many of these factors, **Phil Green, the Privacy Commissioner at the Office of the Information Commissioner QLD**, ominously predicts that "ransomware attacks are absolutely going to increase."

Ransomware is such a current threat that when surveyed at the start of the roadshow in each jurisdiction and asked what participants thought were the biggest threats that they needed to protect against, ransomware and phishing were

[1] https://www.cyber.gov.au/ransomware

identified as the two most popular responses. A total of 215 participants completed the survey across the seven jurisdictions, with 38% of them from state government departments in Australia, and a total of 73% from various tiers of government across Australia and New Zealand. Clearly ransomware is a concern for most of them, especially in the government sector.

In fact, **Jake Boyle, the Director of Cybersecurity & Digital Trust at PwC in the ACT**, who works closely with many government agencies, says that "across our work with government and industry clients in Australia and overseas, we continue to see ransomware impacting lots of government entities." In the context of government, as a majority of the participants acknowledged, "a ransomware attack would have significantly more impact and could potentially deprive citizens of critical and essential services." PwC's own data, in their annual CEO survey[2] also suggests, as Jake Boyle says, that "95% of Australian CEOs cite cyber as a threat to business growth." Such a high figure is partly due to the uncertainty associated with a return to 'COVID-normal', but it is also related to the fact that "although more CEOs are including cyber in their business decisions, much more focus needs to be brought to their organisation's cyber resilience."

Though there has been a shift in the threat environment, in some ways little has changed. Many of the current threats have been known about for a long time, but the shift has been in the brazenness of some of the attacks or attempted attacks. **Kim Valois, the Chief Information Security Officer at Flinders University** in Adelaide, says that "the TTPs" – the tactics, techniques and procedures – "of the threat actors are constantly changing and adapting, so we must change and adapt too. You need to know what your attacker might do against you and think about how that would impact your environment."

Jessica Hunter says that the TTPs "have evolved and are playing out in a much more public arena now." For instance, "some malicious actors have been publicly advertising their successful compromises," whilst others have "dropped the ransom note within the network" for it to be seen publicly rather than sending it by email, which was the previously identified method. "The threat adversaries have also pivoted to exploit public vulnerabilities within 24 hours. So the time window is ever decreasing." That means that organisations need to respond quicker than ever.

[2] https://www.pwc.com.au/ceo-agenda/ceo-survey/2021.html

Know what you've got

One way to be more cyber resilient and to ensure a rapid response is to know that more than likely, an incident will occur at some point, and to be prepared for it. Neville Bannister says bluntly that "unless we have the right protections in places, it's like walking down the main street of a city without any traffic lights and expecting not to get hit." In other words, as Samantha Gavel says, "the cyber threat landscape is such that it is a question of when an organisation will be impacted by an incident rather than if." Since holding organisations to ransom is one of the key ways that criminals operate, organisations and particularly government agencies should therefore "consider the information they hold, whether they need to collect it, how long it needs to be retained, how it is secured and stored, who has access to it, and what audits are in place."

Put another way, **Peter Bouhlas, the Chief Information Security Officer at Office at Digital Government WA**, says that "you're not going to be able to defend what you can't see. You need to have situational awareness and visibility over your threats, controls and vulnerabilities." Rachel Dixon meanwhile asks "how can you be certain that you won't be a victim of ransomware? You can't be." Therefore "it is important to know what you have. You really have to understand what you hold and the value of that information."

> **"Understand the data that you hold, understand what you've got and what could be at risk. If you don't understand where you are starting from then when a breach happens, you won't know what's been taken. If you don't actually know where you are starting from, it's very hard to get an accurate baseline."**
>
> **Rachel Dixon,**
> *Privacy and Data Protection Deputy Commissioner,*
> **Office of the Victorian Information Commissioner**

However, being cyber resilient is not only about a stocktake. Knowing what the data is and how it is held or stored is one thing, but as Rachel Dixon continues, "if a nation state wants to get access to your systems, they will get it. There is no protection against that." In fact, sometimes "you may not even know when you've been attacked."

Jake Boyle from PwC says it's also about "knowing your own supply chains." This means knowing where the data comes from or who has access to it. These days government agencies are "increasingly vulnerable to foreign ownership, control and covert influence." Current trends suggest that foreign actors are "constantly seeking to penetrate government, defence, academia and business to steal classified information, military capabilities, policy plans and sensitive research."

> **"Understanding your own supply chains is the only way in which you can really manage these increasing risks facing organisations"**
>
> **Jake Boyle,**
> *Director, Cybersecurity & Digital Trust,*
> **PwC Australia**

Peter Bouhlas says that "supply chain risk is a bigger considerations than just thinking if your password has the right number of characters." Increasingly, many of the foreign and even domestic criminals are using social media and other commonly used platforms to lure their victims. Jake Boyle says that "the pandemic has shone a light on the frailty of our global supply chains" and as a result, "we're increasingly seeing actors using LinkedIn and Twitter as targeting and exploitation platforms." Often these lures look authentic and are very effective. In fact, in one particular case, "a criminal actor was able to exploit a fault in the software that had apparently been around for over ten years without anyone noticing." They deployed their ransomware and caused havoc. This should be a lesson for everyone: all segments of society "need to consider if they are part of our critical supply chains and obviously take necessary steps to ensure they are not a weak link in that chain."

The importance of privacy

Individuals need to take personal responsibility to protect their data, but governments need to do the same as well. In some ways, as Rachel Dixon says, it comes down to the difference between privacy and security. "Privacy is an obligation that governments and companies have to individuals. Security is what they do to things. So just because you're keeping something secure doesn't mean that you're actually respecting privacy." This is important when it comes to protecting data against cyber threats and when it comes to governments gaining trust from their citizens. "While there may be privacy implications arising from data breaches, you can have breaches of systems that contain no personal data." For instance, if geospatial or scientific data was exposed, that would be a major breach with untold implications, though it would likely contain "data that isn't personal."

In the same way, whilst check-in apps during the pandemic have become ubiquitous, for the most part the public has accepted them because the technology behind them has been transparent and trustworthy. Phil Green says that though the federal government's COVID-safe app was "developed very hastily" and maybe didn't provide the "efficacy" that it was designed for, it was nonetheless "extremely well built and designed from a privacy and data security perspective." It was "almost unprecedented in an Australian history in terms of being transparent, and the government went further than any other government in the world at the time to protect privacy and to entrench privacy protections."

Samantha Gavel agrees and says that "privacy issues have been a key consideration in many aspects of the NSW government's pandemic response." All over the world, governments have been acting faster than they otherwise would have as a result of the pandemic, and this increasing pace means that "government agencies and commercial organisations can now collect, store, use and disseminate significant quantities of information about their citizens." This means that there are more opportunities for breaches to occur, but generally citizens have accepted things like QR codes and check-in tools because they "are good examples of positive privacy practice to achieve an outcome that encourages public trust." Plus, they have been seen as "necessary for protecting the health and welfare of citizens." The question is, what will happen after the pandemic? One way of protecting data and ensuring it is safe is to "look at privacy-by-design."

> **"If you think about things like privacy and security threats early in a project and build them in, then you mitigate a lot of the problems that might occur later"**
>
> **Samantha Gavel,**
> *Privacy Commissioner,*
> **Information and Privacy Commission NSW**

In Queensland, Phil Green has "set up a Privacy Champions Network across state government departments," in part to build in that privacy early into a project. After all "it's critically important we get the culture right to support good cyber security practices."

Protecting your data

To truly protect the data of an organisation, it is not just privacy that needs to be built in, but as Jessica Hunter calls it, "cyber security needs to be embedded into the DNA of the organisation." Organisations and their management teams need to think about cyber security in the same way that they think about physical security and need to be "as literate in cyber security as they are in physical security." Peter Bouhlas gives an even more poignant example: "If your house is broken in to, do you start dusting for fingerprints? No, you call the police because you trust them and they are experts. It should be the same situation in cyber security. You need to know what to do about any breaches." In the case of WA, to ensure they are clued into all that is going on in terms of threats, they "work very closely with the ACSC and we're part of the National Cyber Security Committee (of the ACSC)."

One of the reasons why physical security is a good comparison with cyber security is because as Rachel Dixon says, some years ago there was a breach at Sony. "That was in part a result of poor physical security and machines were left unguarded so random people were able to walk in and steal data." It is very important therefore to ensure that offices are secure, "to know who visits your office and to mandate that everyone lock their screens at all times when they are away from their desks." Some of these are very simple measures but are highly effective at stopping breaches.

Some of these measures are also aimed at preventing human error. For instance, "one of the biggest issues that we see in terms of breaches is emails being sent to the wrong person." Part of that is related to the "autocomplete feature, so if you can disable it, you should." Samantha Gavel says that according to a report of the Office of the Australian Information Commissioner for the second half of 2020,[3] "human error accounted for a little over one third of data breaches." As Peter Bouhlas says, "cyber-attacks affect humans and the way they behave."

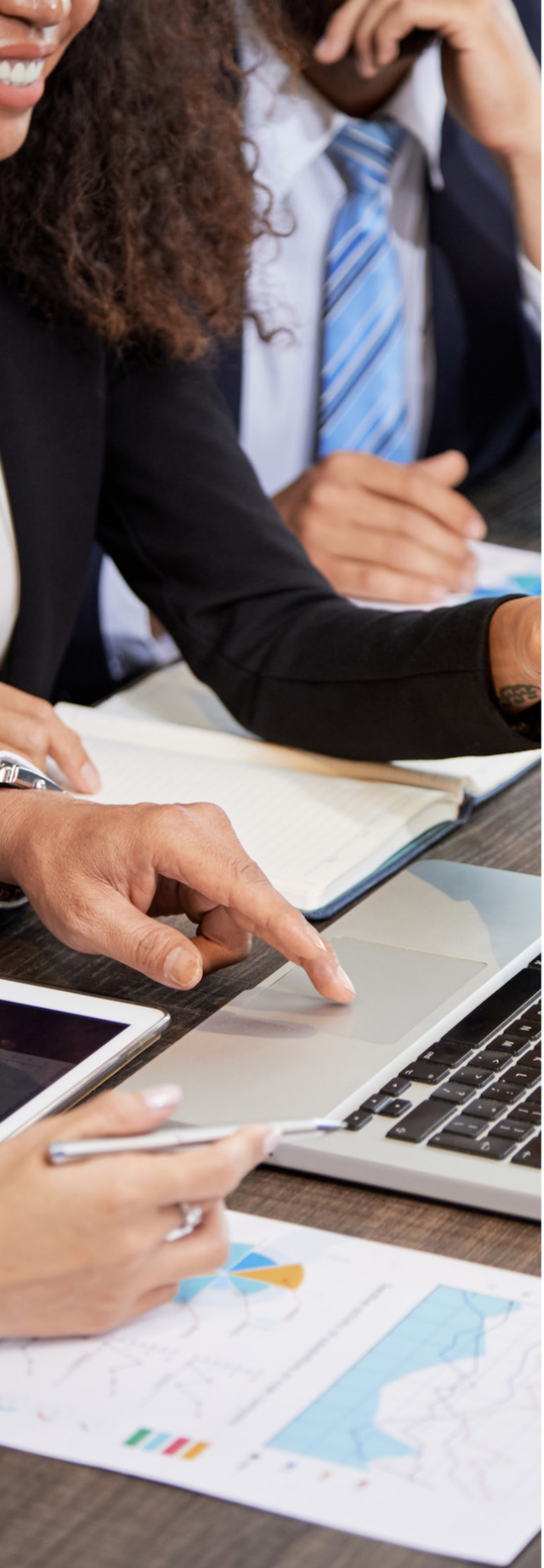
This human element can either make or break an organisation's cyber security capabilities, regardless of the sophistication of its security technologies. Attacks are becoming increasingly sophisticated and, as a result, a paradigm shift is needed to improve current risk-reduction techniques and practices. PwC Australia's latest article, ***A cyber-savvy workforce offers one of the best protections against cyber threats***[4], delves into the behavioural tools and techniques for understanding decision-making and prioritises the actions business should take when raising cyber security awareness and supporting cyber-safe behaviours.

As the survey at the start of the roadshow showed, apart from ransomware, phishing was identified as the other most pressing threat because as Samantha Gavel stresses, cyber-attacks very often "rely on a person clicking on a phishing link." Like ransomware, they often look very authentic but "this confirms that email vulnerability is still one of the greatest risks to information security facing organisations." In fact, Jake Boyle says that the pandemic has only exacerbated some of the attacks. "COVID-19 makes up a significant portion of the phishing lures, as we see cybercrime actors targeting governments and educational institutions with highly targeted emails covering things like geopolitical headlines."

This makes such institutions particularly vulnerable and as Samantha Gavel says, "in May 2020 Service NSW suffered a cyber incident phishing email attack. It compromised the email inboxes of 47 staff members. A deep forensic assessment of the incident to work out what had occurred and what information had been breached was conducted. Personal information of 100,000 customers and staff was exposed in the incident." This is just one example but is indicative of what can occur, though as Jessica Hunter says, "I'm sure that no one would like to be part of that learning curve."

[3] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2020

[4] https://www.pwc.com.au/government/government-matters/cyber-savvy-workforce-offers-best-protections-against-cyber-threats.html

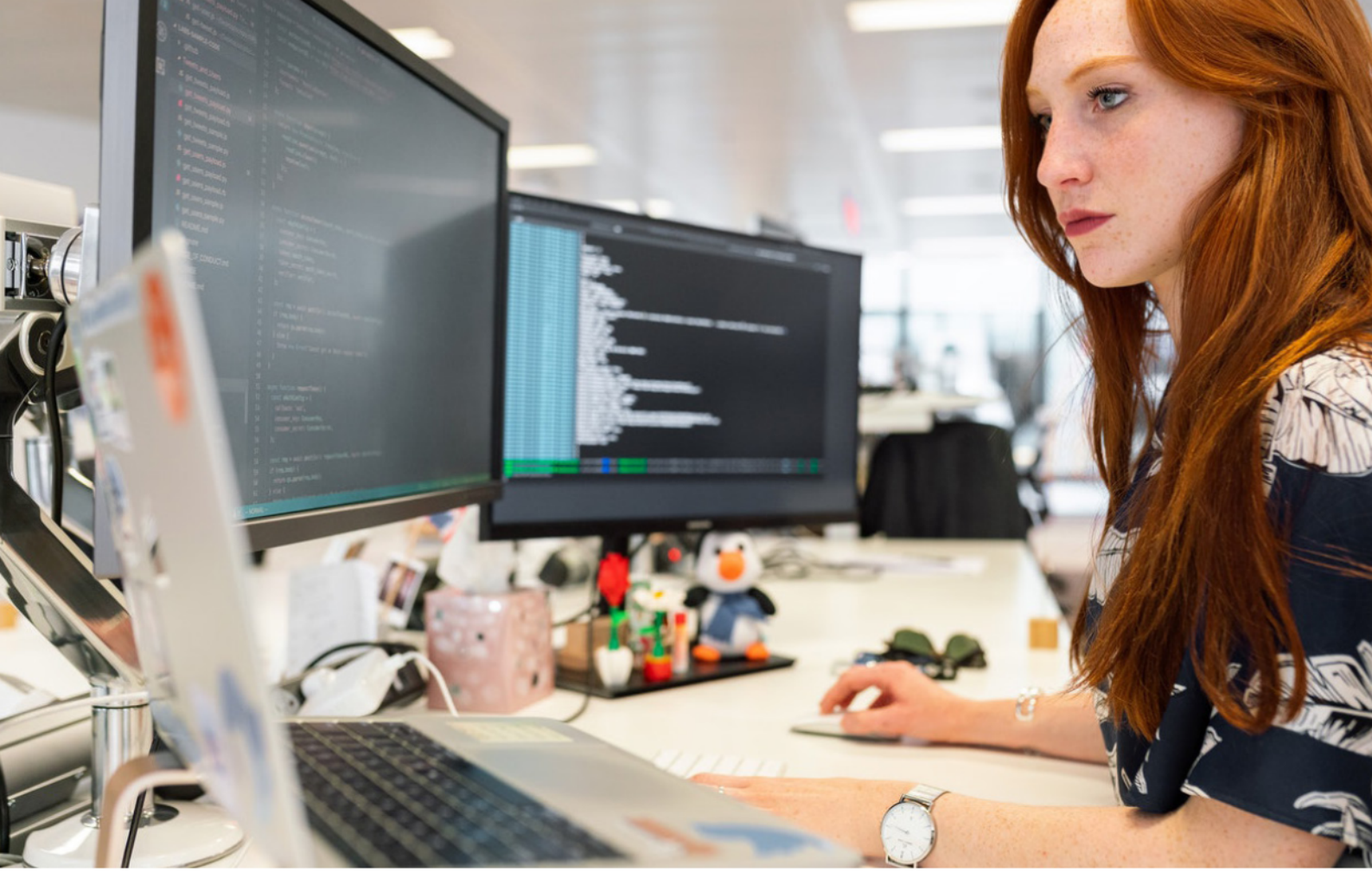


The collective role of the CISO

Each jurisdiction and in fact each organisation is different and often at a different level of maturity when it comes to cyber protection and mitigation. Many institutions and even states now have whole-of-government departments or teams to deal with cyber threats, often headed by a CISO. Whilst having a CISO in an organisation is not new, the role has evolved. Jessica Hunter says "what I'm starting to see across the community is the challenge for any CISO in explaining the risk of cyber security in terms of impact." In other words, the threats are greater and thus the role of the CISO is greater, though sometimes the work of the CISO is not aligned to the work of the organisation. "We've found that the decisions currently being discussed at the CISO level don't always have the full support of the organisation."

Understanding that this might be the case and partly because of the evolving threat of cyber security, Peter Bouhlas says that in WA, "the Office of Digital Government was stood up in July." Previously, in terms of dealing with cyber security, "agencies were largely working in silos and independent of each other and with no central coordination to help provide leadership and guidance to improve their standards and practices." The role of the Office and specifically the Cyber Security Unit is to coordinate and support a whole-of government effort and to "protect the WA government's information, assets and service delivery from cyber threats." As part of the unit, a new Cyber Security Working Group was also established, which "now has representation from over 40 agencies and is very collaborative and constructive." Part of the reason for needing such an office, a unit and a group is to "try to define the boundaries of the threats and the role."

> **"Most agencies have never been attacked, have never had an incident. Some however were having thousands a day, whilst other didn't really know what constituted an attack. It was never really defined. Now that the Office of Digital Government has been set up, the main objective for all of us is probably to prevent any loss of information or data and to ensure that we can continue to provide our services and our operations"**
>
> **Peter Bouhlas,**
> *Chief Information Security Officer,*
> **Office of Digital Government WA**



In New Zealand, Neville Bannister says that the notion of cyber security "didn't exist pre-2010. It was a big fat zero." As it was in much of Australasia, the prevailing view for a long time was that "bad things do not happen in our backyard." Obviously there were occasional breaches, but collectively little was done about it. "No one really cared until their machine was affected. Staff and customers got annoyed but then it was fixed and concerns soon faded." Then when it was clear that something needed to be done, partly to keep up with the rest of the world, "things changed rapidly, starting in 2019." But even then there was little enthusiasm from management for things to change. At the Ministry of Education for instance, the IT people used to say "that we just need a good crisis for us to capitalise on. Sometimes you get what you wish for because the pandemic hit, and bingo. We now have that opportunity. The responsibility is therefore now on us to come up with appropriate solutions."

When the change came to the Ministry of Education, the vision of the Ministry was updated. Amongst other things, the purpose now is to have "an education system that delivers equitable and excellent outcomes," and that this should be achieved in a way "that family and students are confident and secure to thrive in a digital world." In other words, the cyber security of the organisation needs to be strong even though "we have a big, broad organisation with a number of different siloed areas, and we're not always well connected."

Drilling down further, even individual institutions like universities also need protection. Kim Valois says that Flinders University in Adelaide "is a big place. We have over 6,000 staff, over 25,000 students and actually another 10,000 on top of that pursuing other forms of study." A single incident could have significant ramifications, especially because even before the pandemic, much of the work was conducted online. "Even a lot of the research that has traditionally been done in a lab has now gone online." For the IT department and the CISO, "this is creating a unique set of challenges in terms of awareness," especially because until also about 2019, "cyber security was not looked after seriously."

Improving your security posture

Jessica Hunter says that to ensure that cyber threats are heeded, and to mitigate the risk, the ACSC has produced the Essential Eight Maturity model,[5] updated regularly with eight steps to help organisations protect themselves. Many organisations have great tools and "monitoring capabilities, but it's the interpretation of that data and being able to translate it that's really critical. Essential Eight starts to take us into that space." One of the difficulties for many organisations is that "there's an equal need to invest in prevention, and also in the management of a crisis." Numerous ACSC and other tools are designed to assist in doing that. But across the rest of the region, there are other challenges and issues.

Western Australia

Peter Bouhlas says that initially "you need to establish very strong incident response capabilities." In WA and across much of the country, this means creating or enhancing the risk profile to know what a threat or an attack looks like, and to know what to do about it. For an agency like Digital Government WA, this means establishing good partnerships. "You can't do this on your own. You can't have an effective cyber security program on your own." And particularly in WA, "we are highly dependent on the other states." For instance, "we need to know what's going on in other jurisdictions. If there's an incident elsewhere, we need to be alerted so that we can get the indicators of compromise and can put them into our networks to better protect ourselves."

Back in their own territory, the Office of Digital Government WA realised that they simply can't "tell agencies what they need to do. You actually have to lead and do something yourself." So they created a Top 5 cyber security control report, which is "essentially a subset of Essential Eight." It assigned a score to every agency, from zero to five. It was only recently implemented, and of the 120 or so agencies under the umbrella of the Office of Digital Government WA, "69% of agencies are still at zero. What we're trying to do now is to shift agencies from zero to one."

They also initiated "a student intern program. We trained students and sent them to the various agencies." As much as the agencies wanted to change and improve their security postures, they generally didn't know how and didn't have the resources to implement any changes anyway. "So we started providing services at no cost, which really gained momentum." The students looked at the controls, the vulnerabilities, the passwords and many other factors, and were able to begin the process of engagement and improvement. This was also designed to lift the capacity of agencies and shift the dial.

Victoria

Rachel Dixon says that agencies like OVIC and the cyber security team at the Department of Premier and Cabinet have been set up to assist when a breach occurs, and to help agencies arm themselves for better protection. The important thing is to "notify either of us. There is no wrong door in that regard." In fact, not only is it a recommendation, but according to the Victorian Protective Data Security Framework V2.0,[6] it is a requirement for "each agency to submit a plan to us every two years." However, "it is not just a checklist kind of thing. It's a risk-based approach to security" based on very strict standards that need to be signed off by the CEO.

Some years ago "we had a review of the standards done for us by PwC. We asked if getting the CEO to sign off on this a good thing or not and almost universally, everybody said it was one of the single best things in the framework because it forced the senior executive to actually pay attention to cyber security within the organisation." Part of this reasoning was because "you can't have one rule for your senior executives or Secretary, and then another rule for everyone else."

Data is generally seen as a good thing because it gives organisations information. But it can also be "a liability if it is not well governed or looked after." Therefore, having an up-to-date "business impact chart and risk register is a good idea." Knowing what shouldn't be in the system is critical because "somebody may already be in your network." Not every criminal actor is involved in ransomware or malware. Some may simply "modify your data in such a way that a system runs poorly, produces poor results, or destroys confidence in the agency that's holding the data." Sometimes this can be more destructive and cause more long-term pain than malware.

Having a plan and having things like multi-factor authentication (MFA) is important, but almost more important is to "test the plan, to do regular audits because there are always software updates, and to do everything you can to try to make your agency a less attractive target." If it's too hard to get in or if the data is too well secured, criminals "may move on to try to find another target."

[5] https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

[6] https://ovic.vic.gov.au/data-protection/framework-vpdsf/

New South Wales

Samantha Gavel says that as part of a larger commitment to improving the quality of digital interactions across NSW, "$2.1 billion has been provided as part of the Digital Restart Fund." Within that, "there is also a provision for funding to improve cyber security practices across government and to ensure that Cyber Security NSW is appropriately resourced."

However, improving the security of organisations is not only about funding. Partly as a result of the breach that occurred at Service NSW, a public interest direction was enacted in August 2020 for six months. This allowed the "collection, use and disclosure of personal information for a time limited data exchange process between the databases of other agencies. The purpose was to provide Service NSW with up-to-date contact details of customers impacted by the cyber incident. The breach has provided important lessons and learnings."

In fact, though it was first discussed in 2018, "a mandatory notification data breach scheme for NSW government agencies will be introduced into state parliament either later this year or early next year." The consultation process featured presentations by Service NSW based on their breach, and the scheme "will include the requirement to notify both the Privacy Commissioner and the affected individuals," which has not typically been the case. This an innovative Bill, and "while we might be the first of the states to introduce such a scheme, I don't think we will be the last."

Queensland

In fact, Phil Green says that although a similar Bill is not being proposed in Queensland, "we desperately need our Information Privacy Act to be updated." It was first passed in 2009 and "has no notification scheme at present." Many other states also don't have notification schemes, whilst "the Commonwealth's Act is also under review." Updating the Privacy Act might seem trivial, but it has major ramifications. A small agency may not feel the need to report a breach and might feel that they can deal with it. "But what happens if Brisbane City Council has a breach, considering that it is a larger institution than the Tasmanian government? I'm hoping that Queensland will shortly have an updated, contemporary legal framework." This is currently in train largely because of the pandemic, and if changes happen, "then COVID wasn't such a bad playbook in that regard."

One of the issues is that there is a "skills shortage" in terms of cyber security and privacy knowledge. At Queensland Health for example, in 2020 there were "1,200 notifications of unauthorised access to patient information." Not all of the access was malicious and most of the breaches were very minor, but "education and awareness training was lacking" and that was the result. In the first half of this year, with improved education, "notifications have so far come down to 400." In general, when it comes to improving cyber security "training is critical, and it needs to be tailored and done repetitively to make sure people have current, up-to-date training and awareness."

NZ Ministry of Education

Neville Bannister says that now that they are taking the cyber threat seriously, they are taking "a proactive, smart approach." They've come to the realisation that "not all vulnerabilities are born equal." Some criminal actors get into systems surreptitiously whilst others send emails to individuals. The important thing is that they now have a "risk management tool that gives us an assessment on an apples-for-apples basis, so that we can then recommend to the executive where our efforts and resources should be best spent."

One of the problems previously was that management didn't understand the jargon in the reports. "Now we've simplified it and got it all into plain language. You've got to talk to people at their level and keep the language simple." Another issue previously was that "there was never a view across the whole organisation. Now with our simple risk management tool in place, we can see all the risks and vulnerabilities." Much of the work of the Ministry and other ministries across New Zealand in this space is informed by "frameworks like the Essential Eight and other ACSC resources." But even still, "there's a little bit of triage required at the outset to make sure that we're targeting areas that affect us." The most important lesson is to continuously move forward.

> **"Just get moving, take small steps and build the foundations. If you don't have the foundations or the fundamentals in place, such as good policies and standards, then you'll be in trouble. The environment around you constantly changes so keep your assurances going. Keep double checking and testing everything"**
>
> **Neville Bannister,**
> *Senior Manager, IT Assurance,*
> **NZ Ministry of Education**

Flinders University (SA)

For Kim Valois, the cyber protection of the university comes done to one question: "What does good look like? That is what drives me." In late 2019 when the CISO role at the university was created, Kim was tasked with looking into a cyber-attack that occurred at ANU in Canberra just a few months earlier to determine if something similar could happen at Flinders. "I was asked to tell the board if something similar happened here, what we would do about it." At about that time, a report was released by ANU that detailed what actually transpired. "I spent a fortnight picking apart that report and that attack. Then I briefed the board with 15 recommendations of things that we needed to do. There's not only 15, but that is the number I chose. It was about understanding our weaknesses, being honest about them, and trying to make them better."

No specific money was provided by the executive to implement the recommendations, but "with some good will from my boss, we were able to move some projects around and delay others so we could pay for this one. Most importantly, it was about having control and developing visibility." One of the recommendations was about the deployment of MFA across the board. "We're not at 100% yet but we're working quickly to actually fix that so that we deploy MFA for everyone." MFA is not a silver bullet; threat actors can still sometimes get around it and "are constantly advancing and adapting their activities. But it does buy us time, and to combat the threats, we need time."

Some of the other recommendations were still being worked through when the pandemic hit. "We had to set everybody up to work and study from home." In some ways, the pandemic was a blessing because it ensured that many of the processes set up for remote learning could be controlled by the university. "Across all universities in Australia and New Zealand, cyber security is still a threat and has been one of the top three challenges for the past few years at least, but we are hustling and trying to mitigate the risks as much as possible."

Creating a multi-disciplinary approach

Overall, across all jurisdictions, it is clear that the best way to combat the threat of cyber-attacks is not simply by having a CISO or even an IT department, but by embedding the practices of the team across the whole organisation. As Rachel Dixon says, "IT security in this day and age should be something that everybody in the organisation is responsible for." Jessica Hunter takes it further and says "while security controls will absolutely help mitigate and are critical in this space, it is not solely technical decisions alone that come into play."

> **"End users need to appreciate that they're part of the cyber security journey. It's no longer just looking at the technical controls and technical language. Now it's about an emphasis on policy and decision making for everyone. It's truly a community that allows us to manage this challenge, and often we find that sharing that knowledge and some of the challenges helps the community grow"**
>
> **Jessica Hunter,**
> *acting First Assistant Director-General, Cyber Security Services,*
> **Australian Cyber Security Centre**

On top of that, for large organisations or departments, working with media and other partners is also important. "It's very important to bring media in at the beginning." The ACSC often only gets involved in an incident when the media calls asking questions. This is not ideal. "It's very easy to bring a cyber security culture into an organisation if you've lived through an incident that's gone public, but cyber security is actually about more than that."

Phil Green agrees and says that to truly combat the cyber threat, "you do need your media and PR people on side to explain what is going on and to develop trust and transparency. You also need the legal people involved, and you obviously need the tech and engineering people." In other words, "you really do need a multi-disciplinary team approach, with safety, security and privacy built into the DNA of any developments."

> **"Having a supportive culture with the right people and the right skills is more important than even the best technological controls"**
>
> **Phil Green,**
> *Privacy Commissioner,*
> **Office of the Information Commissioner QLD**

Samantha Gavel says "we all share and have a role in contributing to a strong cyber security environment. It cannot be left to one team or one individual." In fact, across NSW, "managing the cyber security environment of agencies requires a whole-of-government and collective approach. It is not just for the technical staff within the agencies to deal with, but the executives, risk and audit committees and other agency teams also need to be involved." Kim Valois takes it one step further, and says "everybody has a role to play."

> **"For me, cyber security is about having one foot in strategy and governance, and the other in the fast-paced world of threats and mitigation. If I could co-opt everyone with a computer to be part of the larger cyber security team then I surely would."**
>
> **Kim Valois,**
> *Chief Information Security Officer,*
> **Flinders University (SA)**

Moving forward

The threat landscape has changed, and the approach to mitigating it must change too. Moving forward, it is important to understand the environment and the vulnerabilities that organisations face, and what to do about them. Jessica Hunter says that the ACSC has plenty of tools, guides and plans "where we provide you an indication of your internet-facing capabilities and where there may be vulnerabilities." But combatting the cyber threat is not just about having the right plans. In fact, Rachel Dixon says that "everybody has a plan until they get punched in the face." In other words, it is critical to exercise that plan and be constantly prepared.

> **"Just like a fire evacuation drill, you need to be involved in regular and constant organisational cyber security exercises, whether that's a planning exercise, an incident exercise or a backup exercise."**
>
> **Jessica Hunter,**
> *acting First Assistant Director-General, Cyber Security Services,*
> **Australian Cyber Security Centre**

But even before that, Kim Valois says that the language needs to change. "When I talk about cyber security, it sounds one way to me in my head but it often sounds foreign to somebody else. That's because it is technical and complex. We really have to simplify it and make the messages a lot simpler and more straightforward."

As part of keeping things simple, Peter Bouhlas has very realistic and cautious aspirations for his uplift program. Whilst most agencies are still languishing at the bottom of the table, "my immediate objective is just to get them off zero. I don't need them to have a score of two or three just yet. There's no point in helping an agency that already has a score of two or even one and spending money and time on them. For now, we want to make sure we don't leave anyone behind and focus on those that potentially don't have the appropriate resources."

In very simple terms, Neville Bannister says that cyber security is really about "creating a vision for your organisation and embedding the improvements." Or as Samantha Gavel says, "agencies need to focus holistically on good cyber security protection, reducing risk, and having processes and procedures in place to manage a cyber security breach."

At the end of the day, Jake Boyle says that a 'big four' company like PwC is "proud to be working with both government and private sector organisations, helping them better understand where they may be vulnerable in their supply chains. But more importantly, we are providing practical and meaningful advice to address these vulnerabilities and reduce the likelihood and impact of a compromise." That, after all, is the purpose of cyber security.

JESSICA HUNTER
acting First Assistant Director-General, Cyber Security Services,
Australian Cyber Security Centre

SAMANTHA GAVEL
Privacy Commissioner,
Information and Privacy Commission NSW

RACHEL DIXON
Privacy and Data Protection Deputy Commissioner,
Office of the Victorian Information Commissioner

PETER BOUHLAS
Chief Information Security Officer,
Office of Digital Government WA

PHIL GREEN
Privacy Commissioner,
Office of the Information Commissioner QLD

KIM VALOIS
Chief Information Security Officer,
Flinders University (SA)

NEVILLE BANNISTER
Senior Manager, IT Assurance,
NZ Ministry of Education

JAKE BOYLE
Director, Cybersecurity & Digital Trust,
PwC Australia

PUBLIC SECTOR NETWORK

About
Public Sector Network

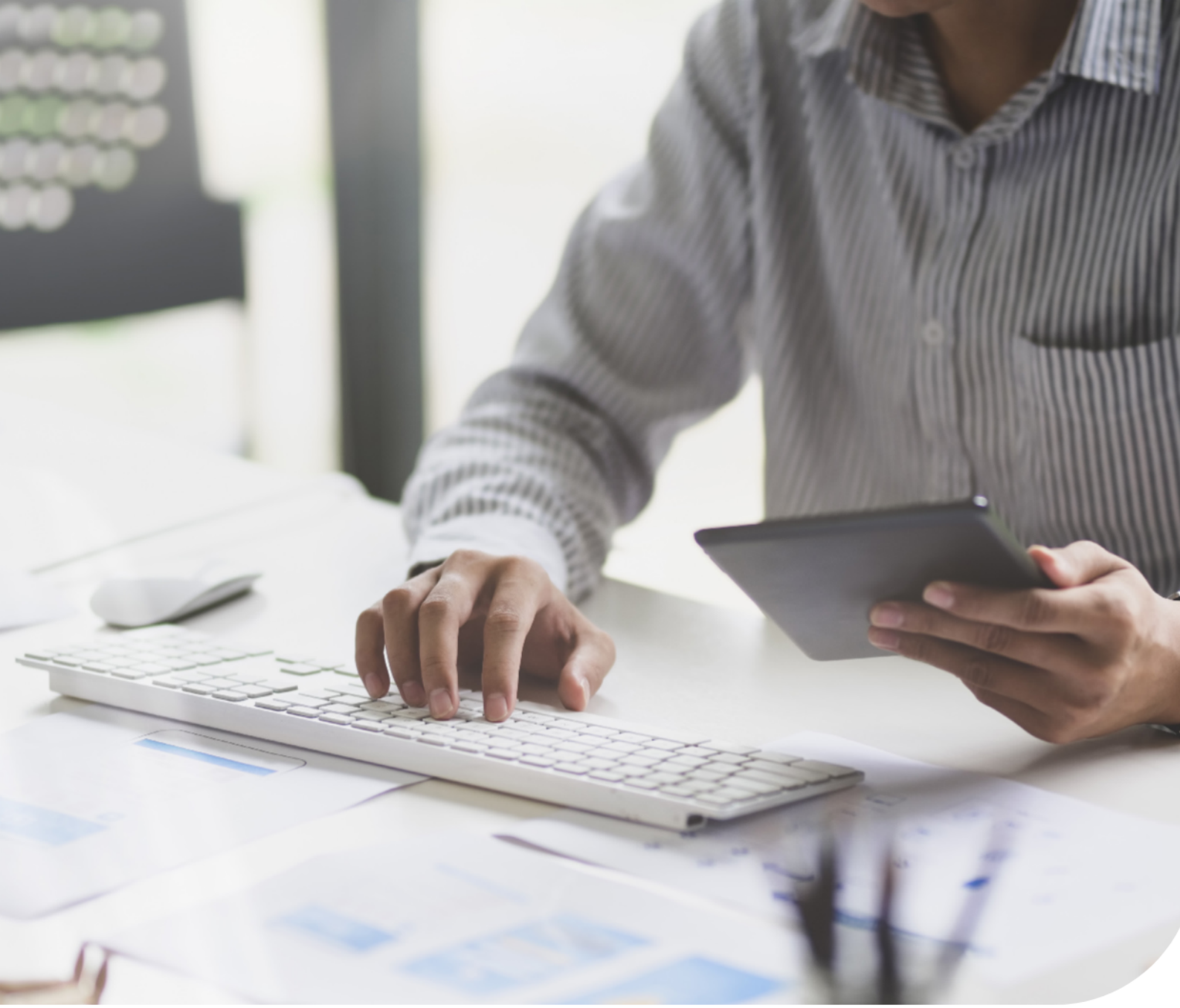
Public Sector Network is a research company that represents public sector professionals across Australia, Canada, New Zealand, and the USA. We develop research, roundtables, events, and webcasts to suit current areas of interest to government agencies and their suppliers.

The public sector consistently faces shrinking budgets and growing expectations, forcing them to be one of the most innovative and resourceful industries in the world.

Regardless of department, agency, level of government or geography, public sector employees are all striving to tackle similar challenges and priorities.

Join Public Sector Network's communities of practice to share ideas and insights, and to access to the latest research.

www.publicsectornetwork.co



PUBLIC SECTOR NETWORK

Certified B Corporation
This company meets the highest standards of social and environmental impact

CONNECTING GOVERNMENT
WWW.PUBLICSECTORNETWORK.CO

AUSTRALIA / NEW ZEALAND
P +61 2 9057 9070
E info@publicsectornetwork.co

USA / CANADA
P +1 (647) 969 4509
E contact@publicsectornetwork.co

Public Sector Network (Australia) Pty Ltd
ABN - 46 617 870 872

Level 22, 56 Pitt St,
Sydney NSW 2000, Australia