PUBLIC SECTOR NETWORK

Certified B Corporation

Cyber Security and Risk Management Roadshow 2022

Adapting for a More Resilient Enterprise in the Next Normal

September 2022

Sydney / Melbourne
Brisbane / Perth
Adelaide

Sponsored by

pwc

The importance of enhanced cyber security is making headlines as rising international tensions have reiterated the need for improved resilience across the nation. Security leaders have been told to strengthen their defences as attacks on networks and data continue to rise.

Government organisations are facing new threats daily and are racing to stay ahead of bad actors, who are employing more sophisticated methods to successfully breach systems. It is imperative new methods and emerging technologies are combined with improved practices and good cyber hygiene to protect the nation from widespread threats.

This series shines a light on how to mitigate risk and learn through collaboration. By sharing best practices, agencies can employ stronger cyber defence strategies and implement them throughout their organisations. They can educate their workforce on understanding the need for vigilance and how following company policies can help uplift resilience and improve overall cyber security across the country.

Highlights of Keynote Sessions

A changing landscape

For more than two years much of the world has been in chaos or in some kind of disruption as a result of the pandemic. Many former office workers suddenly found themselves permanently resigned to their makeshift home offices, still working remotely, and many companies and organisations are still trying to come to terms with their predicaments. Whilst the pandemic accelerated some practices and altered many others, in many cases it also vastly changed the IT landscapes, causing many systems to be re-built or greatly re-developed. For the most part, a lot of these early changes were conducted hastily and without much warning and thus opened the door to greater cyber threats and vulnerability. But as things stabilised and systems and operations found some kind of normalcy, the initial havoc gave rise to more permanent changes, pathways and journeys that are only now being realised and implemented. Cyber security has always been a central tenant of any institution with IT or internet access, but the last few years have shown how important it is to be ever vigilant, and what happens when there is a sense of chaos. Now, though the threat actors are just as brazen and active as ever, since the immediate dangers have been minimised, it is time to mitigate impending risks in innovative ways.

Threats and risks

When it comes to cyber security and cyber threats, the main changes of the last few years according to **Jaynesh Narain**, one of the Directors of the Cyber Security and Digital Trust at PwC, are not the types of attacks necessarily, "but the scale and the impact."

"Ransomware continues to be the most significant cyber security threat faced by all organisations irrespective of industry sector or location."

Jaynesh Narain, *Director, Cyber Security and Digital Trust,* PwC

This is based on PwC's data and the impact can be so severe that it can be "felt across organisations' supply chains and can affect civil society." However, ransomware is but one of many threats and risks that organisations can face and need to be aware of. One of the other related big trends at the moment is "supply chain compromise, and we as organisations need to see a continuing focus and emphasis on protecting our supply chains and third parties. We have to manage them better. We have to better understand the vulnerabilities in our supply chain and in our whole ecosystem and how that impacts our assets." Another development is "commercial offensive tooling, which continues to be a primary driver in the cyber security market." This isn't new, but especially in the last few years it has become "a lot easier to access these tools, especially when it comes to malicious access online." The tools can be "targeted to a particular organisation or industry," so much so that across much of general society, "we're seeing a lot more intelligence and information gathering."

In just one Australian state for example, **Charlotte Wood**, the Director of Policy, Awareness and Research at Cyber Security NSW, says that according to their 2022 snapshot, "data including credentials and personal or other sensitive information, was exposed in 71% of incidents, whilst 24% of incidents involved employees conducting actions that caused or contributed to the incident." On top of that, "over half of reported incidents were discovered by someone external to the entity." In a public service like NSW – or any other jurisdiction – these kinds of numbers are frightening and unacceptable.

Across the country, at the start of the roadshow, a survey was conducted where each participant was asked to nominate two or three things as the biggest threats in their organisation. Figure 1 (below) shows unsurprisingly, that on an average national basis, just like it is elsewhere, ransomware is one of the biggest threats, along with phishing and other similar risks.

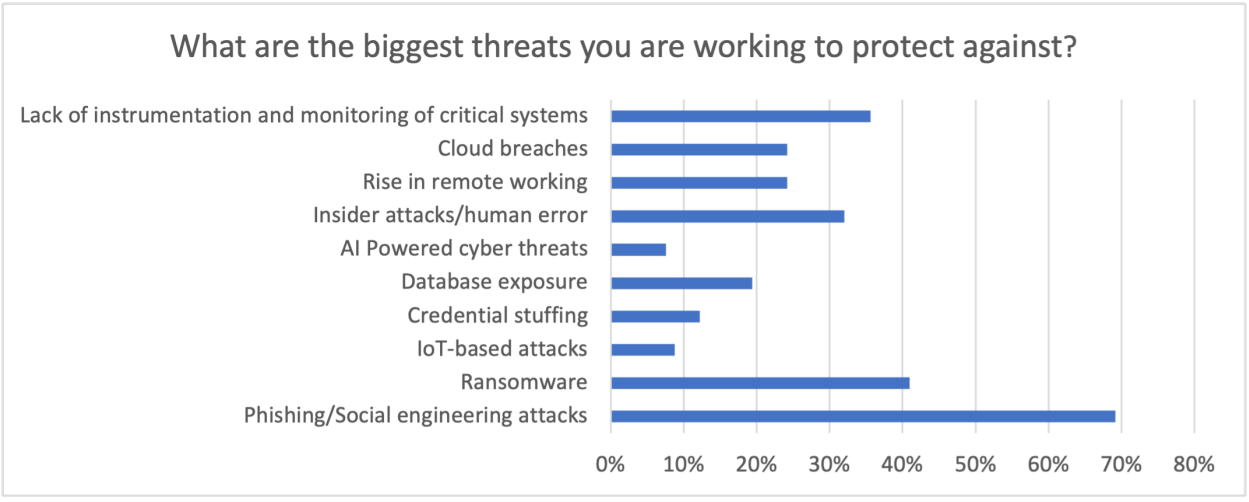

Figure 1: National average of biggest threats

From protection to resilience

Jaynesh Narain says that though the priorities and talking points often change, “it’s pretty scary because many of these [threats] are the same things we have been talking about for ten years.” Not only are the threats often similar, the protections and solutions also haven’t changed much in the last decade. For instance, in the last year alone, things like “administrator passwords, patching, security monitoring and third-party risks” have become more prominent than before, “and we haven’t really fixed the problems.” In part, this is because data is now managed in new and innovative ways and as a result, “there’s increasingly more surveillance across the globe not just in Australia, and we are seeing more and more that the internet has no bounds.” Due to all these factors, the field of cyber security has transitioned from “being protective to being resilient.” One of the biggest changes in the last 18 months has been a mind-set shift. “We’ve gone from knowing we can’t protect everything to making sure that we become more and more prepared to respond to any potential incident.”

Whilst there are many definitions of resilience, especially when it comes to IT and the internet, **David Tuffley**, a Senior Lecturer in the School of Information & Communication Technology at Griffith University in Queensland, says that “when I think of cyber resilience, I look to the future. It means going beyond the technical considerations to the development of an immune system for each digitally-dependent line of business.” This is a useful definition because cyber resilience, like the immune system, “gets stronger the more work it has to do.” And just like proactive health protection, “the object of course, is to identify threats early and to neutralise them, and to continue to do business as usual with minimal disruption.”

Will Luker, the Chief Information Security Officer at the Department of Premier and Cabinet in SA, defines cyber resilience even more simply, as the ability or necessity to “respond, sustain, recover, identify and protect,” all at the same time. This is a continuous cycle since there are incidents or potential incidents occurring all the time.

> **Cyber resilience is therefore the ability to adapt to disruptions caused by cyber security incidents while sustaining critical organisational operations”**
>
> **Will Luker**, *Chief Information Security Officer,* Department of Premier and Cabinet SA

In a state like SA, which is relatively small in terms of cyber infrastructure compared to the larger east coast states, this still means there are many thousands of potential daily incidents, many priority issues and only a small number of agencies to deal with them. “There are always many simultaneous issues,” and sometimes the attackers succeed and the issues make it into the public arena. From “hackers targeting public records,” to “Mt Gambier prison data being leaked,” and “the payroll data of more than 90,000 SA public servants being breached.” These are just some of the incidents that made the news, but they are just the tip of the iceberg. Most incidents either don’t get reported or get thwarted because of diligent and appropriate cyber resilience.

In SA, that resilience comes in the form “frameworks, policies and standards” for a “whole-of-government cyber security approach.” If the resilience technologies work well, then “any attempts to connect to government devices” by external players will be detected, analysed and if something malicious is identified then it will be either automatically blocked or an alert will be sent to the appropriate services. There are many government services so it doesn’t always work quite so seamlessly, but that is the intention.

In the WA Police Force, Karen Owens, the Chief Information Security Officer, also says that they are in the midst of a “cyber security and resilience uplift program.” Though they are just one agency within one jurisdiction, it is important to ensure they get their security and protections in place and up-to-date because the WA Police Force is “the world’s largest single police jurisdiction covering about 2.5 million square kilometres.” They have “over 10,000 employees” and around 2,500 of them are office and administrative staff, with the rest being officers and field employees. The point is that they have a lot of data and a huge area to cover so they need to have appropriate cyber resilience.

Their uplift program began at the start of 2022 with “Part 1: Elevation.” This is about “elevated information security awareness training, an uplift in existing initiatives and a review of existing policies and procedures.” But the most tangible part of the program will begin in 2023 with “Part 2: Resilience.” This is all about “strengthening operational ties with the Office of Digital Government, uplifting our reporting metrics to align with future security demands, and streamlining asset management and infrastructure.” More importantly, it is also about “building on the agency’s incident response plan.” This will lead to “Part 3: Responsiveness in 2024,” which will look to the physical and environmental security environments as well, and will also include HR security and business continuity planning. Finally, in 2025 will be “Part 4: Prospectus,” which is about “reviewing and recalibrating the roadmap to align to the agency’s goals and needs.” Though all the parts are important and will lead to a true uplift, it is the resilience part which will make the most difference as it will ensure that the agency has all the tools it needs to meet any impending threats.

Acknowledging the vulnerabilities

Yet even with the best resilience programs in place, there will always be vulnerabilities. In fact, David Tuffley says that as a result of the "digitisation of the pandemic, which went into top gear, there has been a rapid growth in certain vulnerabilities." In many ways, "COVID-19 has changed the cyber landscape and the threats are more advanced today than they were in 2019." However, even before the pandemic, "cyber security was always the fastest moving sector of the IT industry." At the same time, there were other parts of the IT industry that were always slow moving, like the push towards remote working. **Rod Apostal**, the Chief Information Officer at the Victorian Ombudsman, says that in many ways, "COVID-19 was the best thing that ever happened for our industry in tech. It accelerated the pace towards working-from-home almost overnight by 10 to 15 years, which is wonderful." But particularly in an agency like theirs, it also opened up very specific vulnerabilities. The Victorian Ombudsman deals with complaints and investigations, and thus holds a lot of "sensitive, invasive and personal data."

If people don't trust that we'll hold their data securely and that it won't be leaked, then they won't come to us and tomorrow morning we'll all out of a job. It's that simple."

Rod Apostal, *Chief Information Officer,* Victorian Ombudsman

As a result, the office has a "zero trust policy, even for our employees. We film our staff working, we record all conversations and if you are seen walking out of the office with any kind of paper, you'll be terminated on the spot." The practice to keep data safe is taken very seriously because it shows everyone the importance of the data, but when COVID-19 came, the question was "how do we continue along that zero trust path when staff are working at home?" Multi-factor authentication and geo-locking wasn't going to be enough. The majority of the staff are lawyers or investigators and they are the ones who deal with the sensitive materials. So even "when we sent them home, they

couldn't take paper with them. Plus, we had to make sure that all the people around them couldn't see their screens." In the office, there is a huge room of paper records, but to ensure that there was no breach and that none of those records were taken home, the agency "digitised every single scrap of paper going back to the formation of our office in 1973." Then it was an effort to give staff access, but that was the relatively easy part. "Thankfully there have been no security concerns." And the digitisation should've happened much earlier, but the pandemic precipitated it and ensured that the agency matured, at least digitally. In fact now, "we don't have any paper anywhere at all across the organisation. We have become fully digitised."

One of the reasons why the industry is generally so fast moving, as Jaynesh Narain points out, is because "there probably isn't an organisation around that confidently say that they know what all their assets are and how each of them are connected and accessed," except maybe an agency as secure as the Ombudsman. In large organisations in particular, assets change daily (ie; new starters may get new computers or new logins) and it is therefore "pretty hard to protect ourselves if we don' actually know what we're protecting in the first place." So the starting point is always an identification of assets and vulnerabilities.

Roadshow participants were asked at what stage of the cyber journey they are currently on, and it is pleasing to see (figure 2 below) that almost a quarter are at the stage of identifying their vulnerabilities, and more than half are at the next stage, which is creating the roadmap or strategy for improved network security.

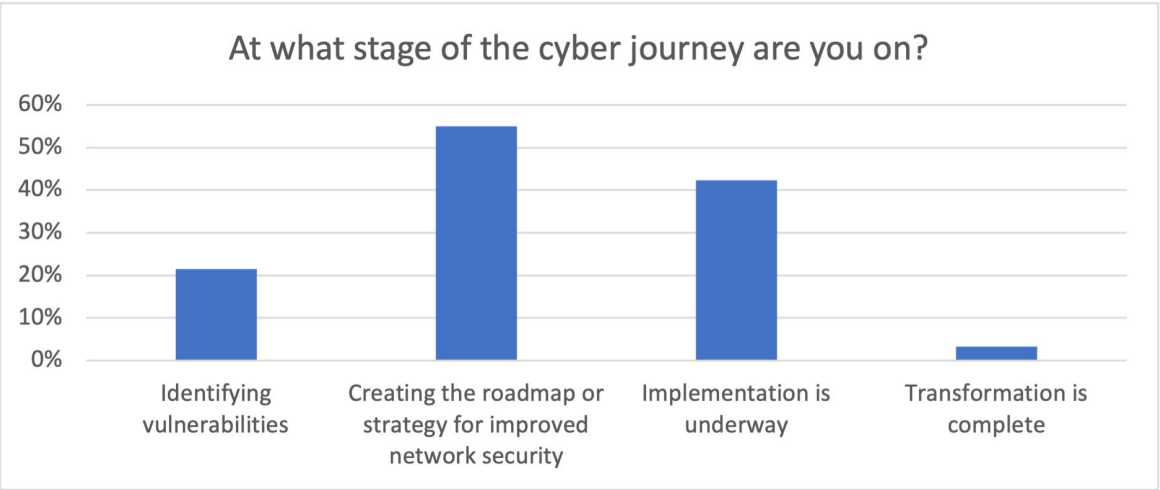

Figure 2: National average of cyber journeys

The importance of a supportive culture

Identifying vulnerabilities however is only one element. As alluded to earlier, resilience is not simply about protecting systems and ensuring that threats are thwarted. It is about a continuous cycle of protections and ensuring that everyone sees the benefit of such protections. In short, it is about creating a culture of resilience. But Jaynesh Narain says that overall, "we're struggling to embed the right kind of culture." For instance, patching is a relatively simple process, which "has been available as a fix for years," but "it's hard to bring everybody on board to educate them about why it's important to patch." The truth is that most people who work in a field associated with IT understand the importance of creating the right kind of culture, but also realise that it has to be across the board. It can't simply be the domain of the IT department. Everyone needs to understand why resilience is so important. It is therefore also pleasing that creating a culture of cyber security was seen as the greatest national priority for the next 12-18 months, according to roadshow participants, as shown in figure 3 (below).

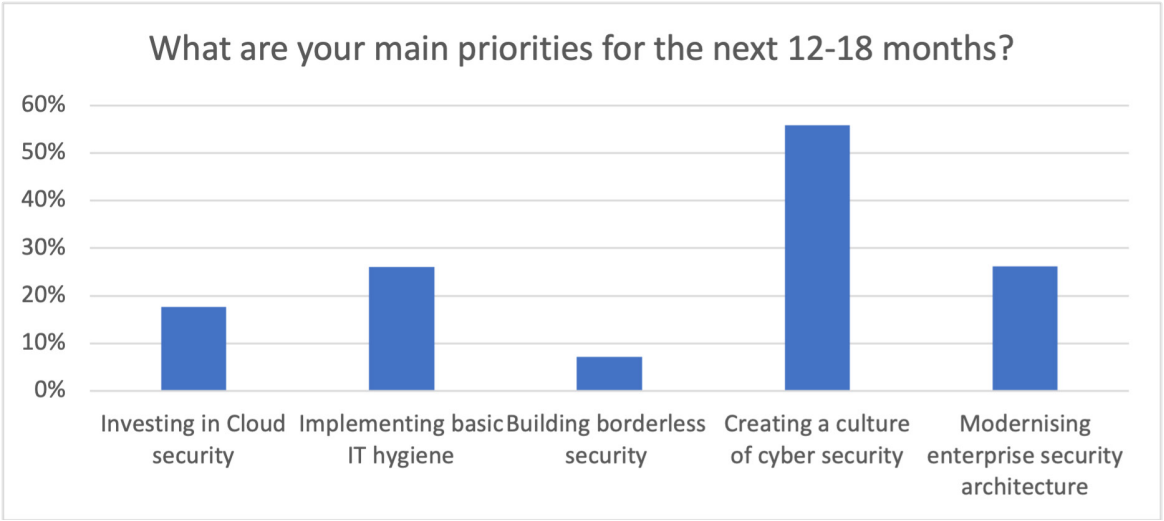

Figure 3: National average of main priorities

However, one of the biggest impediments to the creation of a cyber culture is the virtual world that so many of us now inhabit. Jaynesh Narain says that "everyone is doing their own thing in their own time, with productivity outcomes rather than cyber security outcomes foremost on their mind." The key to creating the right kind of culture is to educate everyone about it. In a separate question, the survey also found (see figure 4 below) that whilst skills, infrastructure and funding were barriers in reaching improved cyber security, the biggest barrier was staff awareness manifested in culture.

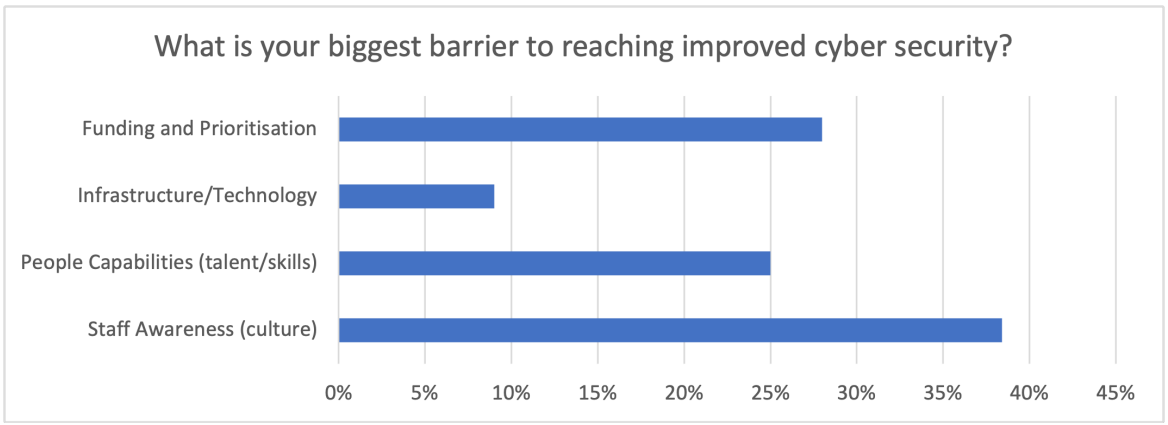

Figure 4: National average of barriers to improvement

To combat this, **John Stevens**, the Manager of Information Security Architecture and Operations at the Victorian Department of Justice and Community Safety (DJCS), says that all departments need to invest in "training around information value adding."

Every department seems to think they're somewhat special and only they can train their people. If we get more and more people educated in cyber security, that is a good thing because they are members of the public as well. They will educate their friends and their families and that on its own is one step towards the prevention of attacks and constant threats."

John Stevens, *Manager, Information Security Architecture and Operations,* Department of Justice and Community Safety (Vic)

Mandy Turner, the Manager of the Cyber Security Operations Centre and Adjunct Lecturer in the School of Social Science (Criminology) at the University of Queensland, takes it further and says that "mandatory awareness and training is great, but unless you actually do a culture uplift, people will just do it because it's mandatory and then they'll be done with it."

Having a cyber culture means everyone is responsible and everyone has their bit to play in responding to cyber threats. Without that, it doesn't matter how many gateways, firewalls, patches or anything we do, it won't protect us, because we have to understand ourselves and know what we're defending and why."

Mandy Turner, *Manager, Cyber Security Operations Centre | Adjunct Lecturer, School of Social Science (Criminology),* University of Queensland

In terms of creating the right kind of culture, Anafrid Bennet, the Head of Security and Operations at Victoria's Greater Western Water, says that "we don't need a technology expert to talk cyber to our business people." If the point is to create a culture where everyone knows the purpose of having a good and secure process, then "what we really need is to have people who think like a hacker." In fact, some of the best people in the cyber security team at Greater Western Water come from fields that are far removed from IT. For instance, a hospitality graduate who lost their job as a result of COVID-19 "proved to be one of the best people in our team because he thinks multiple steps ahead and reads the room better than most." People

like that were able to “bring our culture to the next level.”

John Stevens says that happened in their department too. For various reasons, DJCS recently went through a process of “downsizing, but those that remain still have the same amount of work to do, if not more” since colloquially the department is referred to as the “Department of Just About Everything.” Through the downsizing process, many people left through voluntary retirement packages but some of those roles still needed to be filled, so “our focus now is on getting talented people at a low level, bringing them in and training them up.” Some of those people are straight out of university but others come from different fields and that is proving to be greatly beneficial. “It might take time but it’s worth the effort even if they leave because we can bring them in, they will grow, they will add to the community knowledge of cyber security and they will benefit our organisation in the process.”

Knowing the enemy

But it is not only about culture and education. That is the starting point and the baseline, though the end goal is greater resilience so that that the statistics from NSW and around the rest of the country can be reversed. To do that, Mandy Turner says that it is “important to know and understand the enemy.” However, just like there are many definitions of resilience, so too there are many ways to define cybercrime with “no global definition.” However, according to the Australian Federal Police, there is a national definition, which put simply is “crimes against tech, or crimes using tech as part of the offense.” This is intentionally broad because it covers everything that could fall under the umbrella of technology, from “online fraud and hacking, to child exploitation, espionage and sabotage and so much more.” The point is that “it is huge, and the more tech evolves, the more cybercrime evolves with it. Our enemy can be just a curious student, or it can be a large criminal organisation backed by a state, and we have to remember that any emerging technology that is used by us is certainly being used by them.” This diversity is often what most people and agencies are not prepared for.

It is true that some incidents even in the public service are carried out by amateurs, whether they be students or occasional hackers. But the truth is that most cybercrime these days is much more professional. Jaynesh Narain says that “ransomware operations are increasingly run as organised businesses,” whilst Mandy Turner says that for the most part, “these people are organised, they know what they’re doing, they’ve got lots of money and they do a lot of research and development.” In fact, many of the large operators function as so-called legitimate businesses and “they do their homework.” Most of the time they don’t approach random targets; they have usually scouted out their targets for quite some time and know when and where to strike. “They know their targets and they know us, so we have to know our enemy and ourselves.”

Anafrid Bennet says that the other thing that is important to realise and be prepared for is that when there is uncertainty or chaos, “this is when hackers thrive.” For most people,

the start of the pandemic in particular was a turbulent time, but cyber criminals saw it as an opportunity and the number of incidents went up significantly, partly because "human psychology principles suggest that stress can easily lead to poor or impulsive decisions online, and that is where hackers thrive."

Numerous studies have shown that threat actors look to exploit human psychology as a key to achieving their goals."

Anafrid Bennet, *Head of Security and Operations,* Greater Western Water (Vic)

Many cyber criminals also flourish on self-promotion and the more notorious they can become, the better. However, they also have frailties and during "stressful events, they too can make mistakes." Anyone working in cyber security needs to be aware of this and needs to be extra vigilant when there is chaos, particularly national or global chaos like all of us have recently experienced.

Rod Apostal says that in their office, at all times "our investigators are essentially a roomful of hackers. Their job is to go out there and gather information in whatever way they can, through social media or other channels." Whist they do this, the IT guys often have fun at their expense, by "protecting and fighting against our own defences, sometimes just for giggles, but it's a really good thing to be tested and to see that you might not be as smart as you think are." Until the pandemic, there were no real consequences of such actions and it was just a test, but "suddenly in COVID it all got real" and though staff didn't mean to do the wrong thing, because of circumstances, they didn't know what to do and for a little while there was a lot of panic and scrambling, but then the office came up with an idea. "We gamified the process, giving our IT security guys the opportunity to come up with the same processes and poke holes in the same way the real hackers would. We have a points system for the best attempts, with a bit of public shaming too." But the process has resulted in extremely robust protections and a continued impenetrability even in a remote environment.

The key to success is collaboration

With so many looming threats, the real key to successfully overcoming them, is to collaborate like the hackers do. Mandy Turner says that the "future of cybercrime is more cartel-like behaviour because the ransomware groups are combining forces. On Darknet forums, they proudly talk about the fact that they're in cartels with each other, that they're affiliated with each other." This means that "we have to collaborate because we are stronger together. We need to share information and we need to remove the competition between agencies."

John Stevens said that the pandemic proved that departments can work together for the greater good, but even before COVID-19 struck, "a lot of the department cyber security people were getting together and discussing problems and issues, but there isn't a formal forum, which I think is a huge problem." There are many informal gatherings and fora, often convened by vendors, but many of these are generic or cover broad issues, "which might be great for small organisations, but is not so good for large organisations like ours which deal with extremes of information and classifications." Nonetheless, there is a lot of collaboration within the department and with their federal or other colleagues as required, but that doesn't always feel like enough, especially because there is a "push to centralise IT services within government," but not necessarily when it comes to cyber security matters. "Responsibility still remains on each of us." Victoria however is in a distinctive position with a state election coming up in November, after which "there will machinery of government changes no matter who wins, so things will change" and maybe more collaboration with departments will be built into the new formation.

In NSW, Charlotte Wood says that for the purpose of collaboration, and to combat the stats and threats that they are currently seeing, they are setting up a Cyber Insights Panel in conjunction with the NSW Government Chief Information & Digital Officer, to be "a risk-based discussion that aims to influence, advise, guide, and positively challenge leaders across all NSW government agencies in uplifting the performance of cyber security." The purpose of the panel is to specifically "facilitate collaboration, cooperation, and positive partnerships across NSW government," with "senior officials responsible for cyber risk requested to attend." The panel will also include "independent advisors to provide impartial industry expertise, and to share examples of best practice from across the sector." Cyber Security NSW was set up to provide and support a "government-wide cyber security uplift" and thus collaboration is key.

Cyber security needs to be seen and managed as a whole-of-business risk consideration, with early identification and validation of whole-of-government cyber risk, including trends and emerging risk areas."

Charlotte Wood, *Director of Policy, Awareness and Research,* Cyber Security NSW

In SA, Will Luker says that as part of their collaborative efforts, they have set up "communities of practice" on a whole range of IT and cyber security related issues, and are making a concerted effort to "share intelligence and incident responses across SA government." On top of that, they are also collaborating with other states and further afield on "intergovernmental relations" to build up their overall resilience. Meanwhile in the WA Police Force, Karen Owens says that to create better resilience, they are working together as an agency to "create a culture of compliance, are constantly reviewing the agency's business continuity and disaster recovery management," and they are ensuring that information security awareness training is delivered for everyone.

To really build up collaborative efforts, we are also leveraging industry expertise including using tools designed to improve efficiency."

Karen Owens, *Chief Information Security Officer,* WA Police Force

All these factors, combined with greater departmental engagement will enhance their resilience, which after all is the ultimate goal. On that note, Anafrid Bennet says that "partnerships are key. We need to partner with industry, vendors and different industry organisations to learn and share, and to learn from failures to build up our resilience."

Coming together in greater resilience

As we've seen, the way to combat the cyber threats is to create and embed greater cyber resilience. At the Victorian Ombudsman, Rod Apostal says that since they have become digital, their goal is "to emulate electronically what we do in the physical world." In their case that means building in many extra levels of security into their network, from "secure classifications on all of our emails and documents" to secure networks, servers and clouds. The pandemic was a major turning point for them "with the first few months really scary, but we came out of it better and with improved services and processes." They used to share a lot more information with other agencies by physically delivering documents or sending them by very secure mail. Now they simply talk about them and share less, but collaborate more using other means, and in the process they have built up their resilience in new and unique ways.

Anafrid Bennet says that no matter what security products are in place or what organisations do, "the hackers will always be out there trying to exploit people, networks and systems." That is what they do and therefore anyone working in cyber security or even anyone working anywhere, shouldn't be disheartened "because our journey to cyber resilience is a continuous process. It is not a destination." David Tuffley agrees, and as a result says that every individual in an organisation, irrespective of their title or role, "should act more like a leader in order to develop cyber resilience." Whilst many people are managers, there is a significant difference between a manager and a leader.

A manager issues orders, gets people to do things, whilst a leader is somebody who makes the person want to do what it is they want them to do, in this case for the purpose of cyber resilience."

David Tuffley, *Senior Lecturer, School of Information & Communication Technology,* Griffith University (Qld)

It is also however important to be an ethical leader. That means “looking for a win-win situation where every stakeholder wins, rather than a win-lose scenario, where in order for someone to win, someone else has to lose.” To create real cyber resilience, “you need good, ethical leadership displayed by everyone.”

Mandy Turner says that these days, cyber resilience is really about looking at things in different ways and anticipating things before they happen. “A moat won’t save your castle if the enemy is arriving by dragons. To be more effective at cyber security, we need to understand who we’re defending and what we’re defending against. The criminals in this case are dragons. They’re coming at us constantly and they’re breathing fire and we need to be ready.” At the end of the day, to really be more resilient, “we have to know our enemy, we have to know ourselves, we have to be more adaptable and we have to learn from our enemy to protect ourselves.”

Featured Speakers

JAYNESH NARAIN

Director, Cyber Security and Digital Trust
PwC

CHARLOTTE WOOD

Director of Policy, Awareness and Research
Cyber Security NSW

ANAFRID BENNET

Head of Security and Operations
Greater Western Water (Vic)

ROD APOSTAL

Chief Information Officer
Victorian Ombudsman

JOHN STEVENS

Manager, Information Security Architecture and Operations
Department of Justice and Community Safety (Vic)

MANDY TURNER

Manager, Cyber Security Operations Centre | Adjunct Lecturer, School of Social Science (Criminology)
University of Queensland

DAVID TUFFLEY

Senior Lecturer, School of Information & Communication Technology
Griffith University (Qld)

WILL LUKER

Chief Information Security Officer
Department of Premier and Cabinet SA

KAREN OWENS

Chief Information Security Officer
WA Police Force

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