DELL Technologies

vmware®

Accelerating the Cyber Resilience Mandate

A Government CXO’s Imperative for 2021

With Australian organisations facing cyber threats on multiple fronts, it is more important than ever that government agencies and the private sector work together to safeguard their interests. This is especially important when it comes to protecting the vital infrastructure that supports the Australian economy. How to build cyber resilience through collaboration was a key theme of a recent roundtable hosted by Dell Technologies and VMware and convened by 6 Degrees Media, titled ***Accelerating the Cyber Resilience Mandate – a Government CXO's Imperative for 2021***. Guest speakers included **Darren Kane**, Chief Security Officer at **nbn** and **Lucas Salter**, General Manager for Data Protection Solutions for Asia Pacific & Japan, **Dell Technologies**. They were joined by a select audience of chief information, security and cyber leaders from the Australian public sector. Together, they discussed the latest trends in cyber defence and strategies for risk mitigation, and the role that greater collaboration could play in minimising threats.

Guest speakers (left to right): Adam Spencer, Moderator; Darren Kane, Chief Security Officer, nbn; Lucas Salter, General Manager for Data Protection Solutions for Asia Pacific & Japan, Dell Technologies.

As Chief Security Officer at **nbn**, Darren Kane oversees the continuous monitoring and protection of facilities, personnel, and information systems associated with the largest infrastructure project ever undertaken in Australia.

The value of the **nbn** was amply proven in 2020 when mandated lockdowns forced millions of Australian workers and students to remain at home.

"It wasn't road nor rail that actually saved the Australian economy last year during our lockdown, it was connectivity," Kane said. "So, the importance of connectivity and the role we play in ensuring connectivity was never more critical."

As an industry voice and appointee to the Australian Federal Government's Cyber Security Industry Advisory Committee, Kane is also helping other organisations rise to the cyber challenge by guiding implementation of the nation's cybersecurity strategy, and by providing ongoing advice to address emerging cybersecurity challenges.

Kane shared with roundtable guests the recent cyber-attacks against privately-owned transportation and communications companies, highlighting the importance of these sectors to the economy and the escalating need to ensure they were adequately protected.

"Industry makes up such a large part of the ownership of critical infrastructure. It is common sense to try and make sure that the government and industry work together on the strategy," Kane said. "Nobody can afford to be left behind in relation to cyber resilience, because you've only got to have one weak link, and we all may go down with them."

Defending Critical Systems in the Era of Continuous Attack

While companies in sectors such as communications and data processing had very robust cyber defences, the same could not always be said of other operators of what is now considered to be critical infrastructure, such as in transport, higher education and research, or water and sewerage.

Kane said the private sector and government needed to work together to help operators make the investments that would bring them up to required standards, and to ensure they could maintain these defensive capabilities.

"Unfortunately, this is evolving from a risk perspective every six to 12 months," Kane said. "It's not a one-off payment, it is an annual fixed cost to manage security risk in your business."

This sentiment was echoed by Dell Technologies' General Manager for Data Protection Solutions for Asia Pacific & Japan, Lucas Salter, who applauded many of the initiatives being undertaken by governments at all levels to work with industry to raise cyber defence capabilities.

"It's a never-ending battle to combat security attacks or recover systems in the event of an attack," Salter said. "The collaboration between industry and government is making more funds available and is more targeted to solving these problems."

While cyber security was often thought of as being a technology-based issue that should be solved through the application of defensive technology, Kane said it was important to always remember the human element in the equation – both as an avenue of attack, and as a solid line of defence.

"You've got to prioritise and resource the job of creating a security-focused culture," Kane said.

"It's not a side job. We have a whole team dedicated to this at **nbn**. They are professionals who are skilled in making security meaningful and accessible, and we tailor it to people's needs. We use humour and plain English. We don't get caught up in the acronyms and terminologies that makes it difficult to understand. And we really push the fact that security is everybody's responsibility."

Kane said another key strategy at **nbn** had been to elevate discussion of cyber risk up through its senior executives to the organisation's board, and even to government stakeholders.

"Security risk has been elevated to one of our more senior business operational risks," Kane said.

"It's no longer a tech issue. I'm a direct report of the C-suite and regularly speak to the Chairman and the CEO and to government agencies about how we're managing the risk here. This gives me seniority in the company, but also gives me some control and authority over how we manage and what controls we put in place."

> **"You've got to prioritise and resource the job of creating a security-focused culture. It's not a side job. We have a whole team dedicated to this at nbn. We use humour and plain English. We don't get caught up in the acronyms and terminologies … we really push the fact that security is everybody's responsibility."**
>
> – Darren Kane, **nbn**

> **We're seeing an opportunity for security teams to actually be the enabler of digital transformation.**
>
> – Lucas Salter, Dell Technologies

Building Inclusive Cyber Strategies

Fostering the human aspects of cyber defence was also discussed as being critical to unlocking the necessary funding for technology and training initiatives. Attendees reported that these conversations had been made easier by the impact of COVID-19 and the heightened appreciation for risk that many organisations now held.

As one attendee said: "I'm firmly of a view that we need to take a collectivist approach towards this issue. We need to work towards developing a capability of security around the data. It's not just leveraging budgets, but it's about shaping culture, and ultimately we need to shift organisations and individuals to be cyber natives."

While there was general agreement that the crises faced by others could be used to motivate leaders to invest to avoid similar fates, Kane said he had now switched his messaging internally to focus on the benefits and opportunities that came from having good security risk posture, hygiene, and culture.

"The building of trust as a provider of services is an important way for business owners to get the value from managing security risk properly," Kane said. "Take the **nbn** for example. Our whole vision and mission here at the security group is to provide a trusted and reliable secure broadband network to all of Australia and be the best network in the world.

"Now, if we're able to do that, we'll actually build connectivity, and we'll encourage small businesses to join us."

Salter said similar arguments could also prove persuasive in organisations that were undertaking transformation programs, as investments in cyber security could serve to de-risk some aspects of transformation.

"We're seeing an opportunity for security teams to actually be the enabler of digital transformation" Salter said.

"I use an analogy of being the seat belts and suspension and brakes on the race car, as organisations accelerate their digital transformation. I think that communication and that executive engagement is really important."

While the shift to home-based working during the COVID-19 crisis was highlighted by attendees as one of the most critical security concerns of 2020, Kane said it had also served to galvanise appreciation of the need for strong cyber defences.

"It has actually turned the community's mind to how important security risk management is," Kane said.

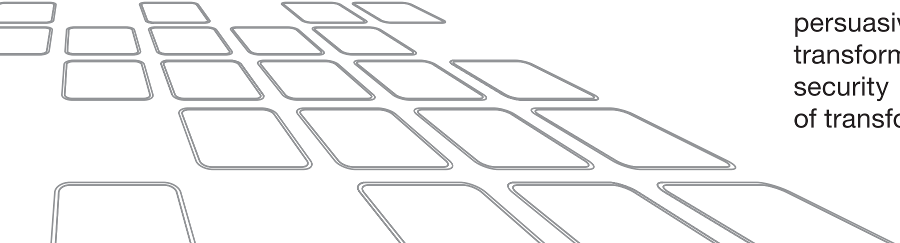
"One of the most important points is definitely that it is all about having the people understand that security risk is their own responsibility. COVID and the lockdown and work-from-home has enhanced their want for knowledge, and we should be prepared to support that."

Near and Long-Term Horizons

While the threat landscape is evolving quickly, many of the challenges that attendees faced in 2021 were the same of those faced last year, including the need to protect workers from cyber threats in their home environment.

As one attendee said: "We're seeing compromises to people's home computers, leading to compromises of their credentials for our systems, and we're seeing more and more of our credentials appearing on the dark web."

Salter said that cyber criminals had also changed the nature of their attacks, and those that engaged in



ransomware had flipped their strategy from locking up data and demanding a ransom to instead threatening to release stolen data publicly.

"Ex-filtrating data is really the biggest concern," Salter said.

"A lot of organisations are being impacted by not only their systems being rendered useless or being disrupted, but also by trying to understand what data has left their organisation and the sensitivity of that. So, they've got a couple of different big problems to solve in a very short period of time."

Another attendee raised concerns about data integrity and providence, and the risks associated that came with data integration and connectivity.

"As we all pursue a single source of data truth to eliminate duplication, what happens is we become reliant on the internal control systems of other organisations and individuals. That's the one area that I can see an enormous risk, but I'm not seeing an awful lot of conversation around it."

While the ability to detect and protect against threats was vital, Kane said it was important that cyber professionals also enhanced their capability to recover quickly.

While the ability to detect and protect against threats was vital, Kane said it was important that cyber professionals also enhanced their capability to recover quickly.

"Unfortunately, in the industry we've got, it's going to be incredibly hard to ensure you're never compromised," Kane said.

"We're in an industry where you will be hit. But what I can do is recommend we make more of an effort to look at the back end around response and recovery."

Skills, Attitude and Building Capability

Another topic of discussion was Australia's recognised shortage of cyber security professionals. While some organisations were turning to automated solutions, Kane cautioned that these investments should not come at the expense of training programs.

"Automation, machine-based learning and technology tools will soon make some of the more base-level introductions into this space redundant," Kane said.

"We've got to make a pathway for those people that would be introduced to a cyber role or career, because some of these more junior roles, such as eyes-on-glass, will disappear."

Kane said when looking for new skilled employees he sought people with a good understanding of technology, but also with inquisitive minds.

"We want people that want to listen to their elders, but then start to develop their own knowledge and experience and skills," Kane said.

"The role we have is evolving every six to 12 months. Today if I employ for skills, they're redundant in 12 months. We need someone who is self-motivated to continue to professionally develop and enhance their own skills."

The need to look widely for skills was echoed by other attendees.

As one said: "If you don't have diversity of thought and cultural background and gender, you'll end up with them repeating your own answers back at you. So, we need to make sure we're all looking wide, rather than narrow."

While the skills challenge was significant, Kane said that infrastructure organisations such as his and others could not shirk the responsibility of developing a skilled capability within their workforce.

"We owe it to the industry, as owners of this space in these large government departments, multi-national and national organisations, to develop a capability," Kane said.

> **We're seeing the start of it now, with government and regulatory organisations leading the way in providing more descriptive – and in some cases more prescriptive – opportunities and advice to organisations.**
>
> – Lucas Salter, Dell Technologies

"We need to bring more interns and graduates in, and we have to stop expecting the world of them and put some time and effort into their development."

According to Dell Technologies' Vice President and Managing Director for Australia and New Zealand, Angela Fox, solving the skills challenge also meant reaching out to under-represented groups and ensuring they played a greater role in the workforce.

"We talk a lot as leaders in the industry about STEM and how you attract more women," Fox said.

"It's about demystifying the mystery and creating intrigue, so that people actually understand it's not unattainable.

"None of us started our journey having all the skills. But we got there."

Greater diversity of backgrounds and thinking would also assist those organisations who were striving to merge their cyber and physical security teams and create a more holistic risk function. One attendee described how their organisation had successfully merged these two groups by breaking down traditional siloes.

"We've integrated a lot of those treatments so that we're getting a much better outcome. It's a lot more fun, and you can attract people into this area. I think I would say that the converged model is the way to go – we're actually fighting off graduates who want to come in and join the team."

Looking Ahead – Collaboration is Key

To be successful as a nation in combating cyber threats, the trend towards greater cross-skilling and collaboration also needed to extend beyond the limits of individual organisations.

Salter suggested that cooperation between government and industry would need to grow stronger over the next few years to create a stronger cyber resilience.

"We're seeing the start of it now, with government and regulatory organisations leading the way in providing more descriptive – and in some cases more prescriptive – opportunities and advice to organisations," Salter said.

Kane said that as government agencies gave more prominence to cyber issues, this would also make it easier for cyber professionals to gain the attention of senior leaders and boards of directors.

However, every organisation's ability to respond to cyber threats would always come back to the total capability of its people.

"The three most important things in security risk are people, people, people," he said.

"Really focus on making sure they're aware of their accountabilities as individuals, where they sit as owners of their own data, and what their responsibilities are – both at home and in the workplace.

"If I could do anything more, it is to continue to drive that vehicle."

Top Three Digital Transformation Programs Accelerated

APJC

		Australia/ New Zealand	China	India	Japan	Singapore
1	Strengthening our cybersecurity defenses: 50% (2% more than the global average)	Strengthening our cybersecurity defenses: 50%	Strengthening our cybersecurity defenses: 52%	Strengthening our cybersecurity defenses: 52%	Rolling out broader remote working capabilities: 46%	Strengthening our cybersecurity defenses: 49%
2	Reinventing how we deliver digital experiences to customers and employees: 44% (6% more than the global average)	Rolling out broader remote working capabilities: 45%	Reinventing how we deliver digital experiences: 51%	Transforming our services and consumption models: 48%	Strengthening our cybersecurity defenses: 42%	Rolling out broader remote working capabilities: 42%
3	Rolling out broader remote working capabilities: 43% (1% less than the global average)	Using data in completely new ways: 43%	Transforming our Edge deployments: 49%	Using data in completely new ways/ extending our business domain: 48%	Reinventing how we deliver digital experiences: 32%	Transforming our services and consumption models: 40%

"Which digital transformation programs have you successfully accelerated this year?"
Base: respondents from organisations which have successfully accelerated at least some digital transformation programs (3427) APJC (1171)

Dell Technologies' *Digital Transformation Index 2020*

Top Three Barriers To Digital Transformation

APJC

		Australia/ New Zealand	China	India	Japan	Singapore
1	Data privacy and security concerns: 37% (6% more than the global average)	Lack of budget and resources: 41%	Lack of the right in-house skill sets and expertise: 33%	Data privacy and security concerns: 47%	Lack of budget and resources: 33%	Data privacy and security concerns/ Lack of budget and resources: 42%
2	Lack of budget and resources: 32% (2% more than the global average)	Data privacy and security concerns: 36%	Data privacy and security concerns: 33%	Unable to extract valuable insights from data and/ or information overload: 38%	Lack the right in-house skill sets and expertise: 28%	-
3	Unable to extract valuable insights from data and/or information overload: 31% (2% more than the global average)	Lack of economic growth: 28%	Lack of the right technologies to work at the speed of business: 29%	Lack of economic growth: 36%	Data privacy and security concerns: 27%	Unable to extract valuable insights from data and/ or information overload: 38%

“What are the main barriers to digitally transforming your organisation?“
Base: all 2020 respondents (4300) APJC (1400)

Dell Technologies’ *Digital Transformation Index 2020*

Top Three Tech Investments

APJC

		Australia/ New Zealand	China	India	Japan	Singapore
1	Cybersecurity solutions: 42% (1% less than the global average)	Data management tools: 43%	Cybersecurity solutions: 53%	Artificial intelligence algorithms: 50%	Artificial intelligence algorithms: 27%	Data management tools: 48%
2	Data management tools: 41% (2% more than the global average)	Cybersecurity solutions: 37%	Artificial intelligence algorithms: 50%	5G infrastructure: 45%	Commercial/ industrial robotics: 24%	Cybersecurity solutions: 47%
3	Artificial intelligence algorithms: 40% (8% more than the global average)	Privacy software: 35%	Data management tools: 48%	Software: containers and serverless: 44%	5G ready hardware: 21%	5G infrastructure/ Privacy software/ Artificial intelligence algorithms: 37%

"What new innovations or solutions is your organisation investing in over the next 1-3 years to enable digital business?"
Base: all 2020 respondents (4300) APJC (1400)

Dell Technologies' *Digital Transformation Index 2020*

DELLTechnologies

6 DEGREES MEDIA
WHERE LEADERS CONNECT

About Dell Technologies

Dell Technologies helps organisations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

About 6 Degrees Media

6 Degrees Media was established by Angela Horvat, former Editor and Publisher of award-winning publications including *Computerworld, Information Age, My Business, The Who's Who of Financial Services* and Founder of FST Media; and Emma Charter, one of Australia's most connected and respected media and events strategists.