govtech review

IN PARTNERSHIP WITH PUBLIC SECTOR NETWORK

LEADERS IN TECH

OUR EXPERTS' PREDICTIONS FOR 2019

Q4 2018
PP100021607

Q4 2018

INSIDE

FEATURES

OTHER FEATURES

LEADERS IN TECHNOLOGY

Insider

A challenging year ahead

The pace of change in the information technology world just never seems to let up, and 2019 promises to be no different. We'll face new variations on old challenges, and new challenges not yet thought of.

So to try to make sense of what we can expect, what we always do at this time of the year is bring together some of the industry's foremost experts for our Leaders in Technology profiles and ask them to share their insights into the current state of play of ICT and what we can anticipate from the 12 months ahead. And their viewpoints make for very interesting reading. There are some common factors — such as the ongoing need to always do better with cybersecurity — through to strong opinions on topics such as the importance of continuous education of the workforce. We thank all of these tech leaders for sharing their knowledge with us, and we hope you will learn something from what they have to say.

Our lead feature in this issue covers Airservices Australia's remarkable journey into the cloud. The national air traffic services provider has shifted its entire business IT operations into a secure, sovereign cloud system, and is already reaping the benefits that such a move can bring — increased staff efficiency, improved devOps abilities, better disaster resilience capabilities and more. This kind of wholesale migration into the cloud is one that many more government departments and agencies will be making in the years ahead, so it's great to have Airservices' success story to learn from and build upon.

In 2019, cybersecurity will be more important than ever. Cybercriminals never sleep and are always inventing cunning new ways to circumvent security systems either through technology (eg, AI, machine learning) or plain old-fashioned psychology (eg, spearphishing). Data security has never been more important, as citizens, businesses and governments entrust more of their lives to digital records. And it's reasonable for all of us to expect that those records will be kept safe and secure from prying eyes. But will they be? How can it be guaranteed? And if indeed such guarantees cannot be 100% rock solid — as seems to be the case — what does this say about us trusting organisations to do the right thing in terms of our digital lives? Are we expecting too much? Or should we be willing to trade off some level of security and digital safety for the sake of convenience? It's a perennial problem, and it's one that won't be going away in 2019.

Jonathan Nally, Editor
editor@govtechreview.com.au

wfmedia
connecting industry

A.B.N. 22 152 305 336
www.wfmedia.com.au
Head Office: Cnr Fox Valley Road & Kiogle Street
(Locked Bag 1289), Wahroonga 2076 Australia
Ph +61 2 9487 2700 Fax +61 2 9489 1265

EDITOR
Jonathan Nally
jnally@wfmedia.com.au

EDITORIAL ASSISTANT
Amy Steed

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Wendy Blume, Colleen Sam

CIRCULATION
Dianna Alberry, Sue Lavery
circulation@wfmedia.com.au

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

ADVERTISING SALES
Liz Wilson Ph 0403 528 558
lwilson@wfmedia.com.au

Caroline Oliveti Ph 0478 008 609
coliveti@wfmedia.com.au

If you have any queries regarding our privacy policy please email privacy@wfmedia.com.au

All material published in this magazine is published in good faith and every care is taken to accurately relay information provided to us. Readers are advised by the publishers to ensure that all necessary safety devices and precautions are installed and safe working procedures adopted before the use of any equipment found or purchased through the information we provide. Further, all performance criteria was provided by the representative company concerned and any dispute should be referred to them. Information indicating that products are made in Australia or New Zealand is supplied by the source company. Westwick-Farrow Pty Ltd does not quantify the amount of local content or the accuracy of the statement made by the source.

Printed and bound by Dynamite Printing
PP 100021607 • ISSN 1838-4307

AIRSERVICES SOARS INTO THE CLOUD

SHIFTING INTO A SECURE, SOVEREIGN CLOUD ENVIRONMENT IS ALREADY BRINGING BENEFITS FOR AIRSERVICES AUSTRALIA.

Jonathan Nally

© stock.adobe.com/au/phaisarnwong2517

About two years ago, the nation's air traffic services provider, Airservices Australia, began working on a program to refresh its core non-operational business systems — its systems of record, ERP, documentation systems and so on, but not the systems that run air traffic control. At the time, the organisation's main IT facilities were hosted at its head office in Canberra. Almost seven years old, they comprised an older HP virtual platform (which had 800-odd virtual machines), several hundred physical devices and about a petabyte of storage, all running in two large equipment rooms.

"We had to vacate those rooms and … that resulted in our request to the market for an IaaS, which included core compute and storage and all of the desktop support and services that go with that," said Chris Seller, Airservices' CIO.

Following a 12-month process, a contract was awarded to ASG Group, whose solution was "very unique and very attractive", said Seller, because it involved hosting all of the organisation's business systems in Vault. "Everything that runs the business of Airservices was to migrate out of our on-premise [facilities] across into Vault's cloud," he said.

"That involved a very high level of detail of planning," he added. "Like every agency, we had lots of old systems, so we were very wary and very cautious about how that was going to work and how well it was going to work."

But as of October 2018, every one of Airservices systems is now running on Vault's cloud, from the SAP ERP system right through to email systems, Microsoft-based systems such as SharePoint and document managing systems.

"Something like 21,000 man-hours of effort finally got us there," Seller said. "So it was a fairly big effort over the last six months, from the time we did the deal with ASG to the time that we got the last machine across."

MAKING THE MOVE

According to Seller, making a full, whole-of-agency migration to the cloud was not originally on the agenda. "I'd lived through some cloud work; I'd worked for some time at Qantas and at Westpac, and they've moved some of their systems on a project basis to the cloud, and that stuff is fairly torturous and difficult to do," he said. "If you'd asked whether we could move every system that runs the business of Airservices into the cloud, I would have said you were absolutely barking mad."

However, Seller said that he and his team quickly learned that it might be possible. "The more we learned about it, the more we realised it was going to work," he said. "Originally what we were planning to do was move whatever we could into Vault, and the really old legacy stuff, like our SAP environment, we probably would have to maintain on dedicated infrastructure in the Canberra data centre. As it turns out, some of those legacy systems went across a lot more smoothly than anybody, including Vault, could have anticipated."

Vault's founder and CEO, Rupert Taylor-Price, agrees that changeover went smoothly. "Most organisations would have put years into that kind of transition," he said, adding that Airservices' commitment to doing it at that pace was just phenomenal. "Many government agencies are thinking about this stuff, and Chris has just materially gone and delivered it in about the same amount of time that most people think about the concepts of it."

SECURITY

Seller said it took a couple of years to convince Airservices that the move to IaaS was sensible. "There's not a huge financial benefit in the move; it's a modest $1m to $2m per year saving over the base case of us potentially doing it all ourselves," he said. "But we would never have achieved the level of capability that we're now realising inside the Vault environment — the whole software-defined infrastructure and the ability to provision environments in hours instead of weeks, the automation, and the security that comes with it, were things that we would never have been able to do ourselves."

Tight security is a vital requirement for Airservices, which Seller said the combination of ASG and Vault delivers. "It gives us a level of data security that would be difficult for us to build on our own," he said. "Some of the investment that Vault's made in how they manage their infrastructure through the OpenStack technologies and their automation technologies… it would be really hard for me to get the skills to actually replicate that in-house.

Image copyright Airservices Australia

“And you’ve got to question why you would do that when you can go and buy it for basically a bit less than doing it yourself,” he added.

Vault’s systems operate as a sovereign cloud, keeping the data onshore, and they’re ASD-approved too. According to Seller, not all of the systems they’ve moved to the cloud require that level of security today, but they might in the future, as Airservices is midway through combining its air traffic services system with the system run by the Department of Defence. “So down the track, there will be data in this environment that Defence will require to be at a level of security beyond where we are today,” Seller said. “Starting on a protected level of security was a very good outcome for me, and it came at the price point we were happy to pay.”

Vault’s Taylor-Price said that getting his company’s product ASD approved was an “overwhelming process”.

“It’s incredibly in-depth; it was a six-year process for us,” he said. “For probably three of those six years we were in probably near daily communication with them, whether that would be looking at our architecture or our supply chain, or our staffing or processes or procedures. I think there are nearly 100 companies that have attempted to get through this process now. And obviously very few successfully come out the other side.”

Taylor-Price added that the general comfort level that this can bring for CIOs across government, not just for Airservices, is “massive”.

“I think Airservices is an interesting case because it is probably a slightly higher risk environment than average if you look across government departments,” Taylor-Price said. “It’s not as bad as some of the defence and intelligence agencies and health, but it’s up there.”

“I can’t control the threats, but I can control the position I put the organisation in to have as safe and as secure an environment as possible,” Seller said. “We are, like all organisations, a potential target, but the use of Vault and the way Vault has built security into the fundamentals of their system gives us a protection well beyond where we were in the past, and probably much better than I could have built myself — I wasn’t going to spend six years building a security layer in my on-premises capability.”

BENEFITS

“In the field, the average user in Airservices is definitely seeing a performance improvement and we’re certainly getting benefits on the quick turnaround on provisioning and requests for new capability is vastly different than it was before. We’ve generally got very happy users,” Seller said.

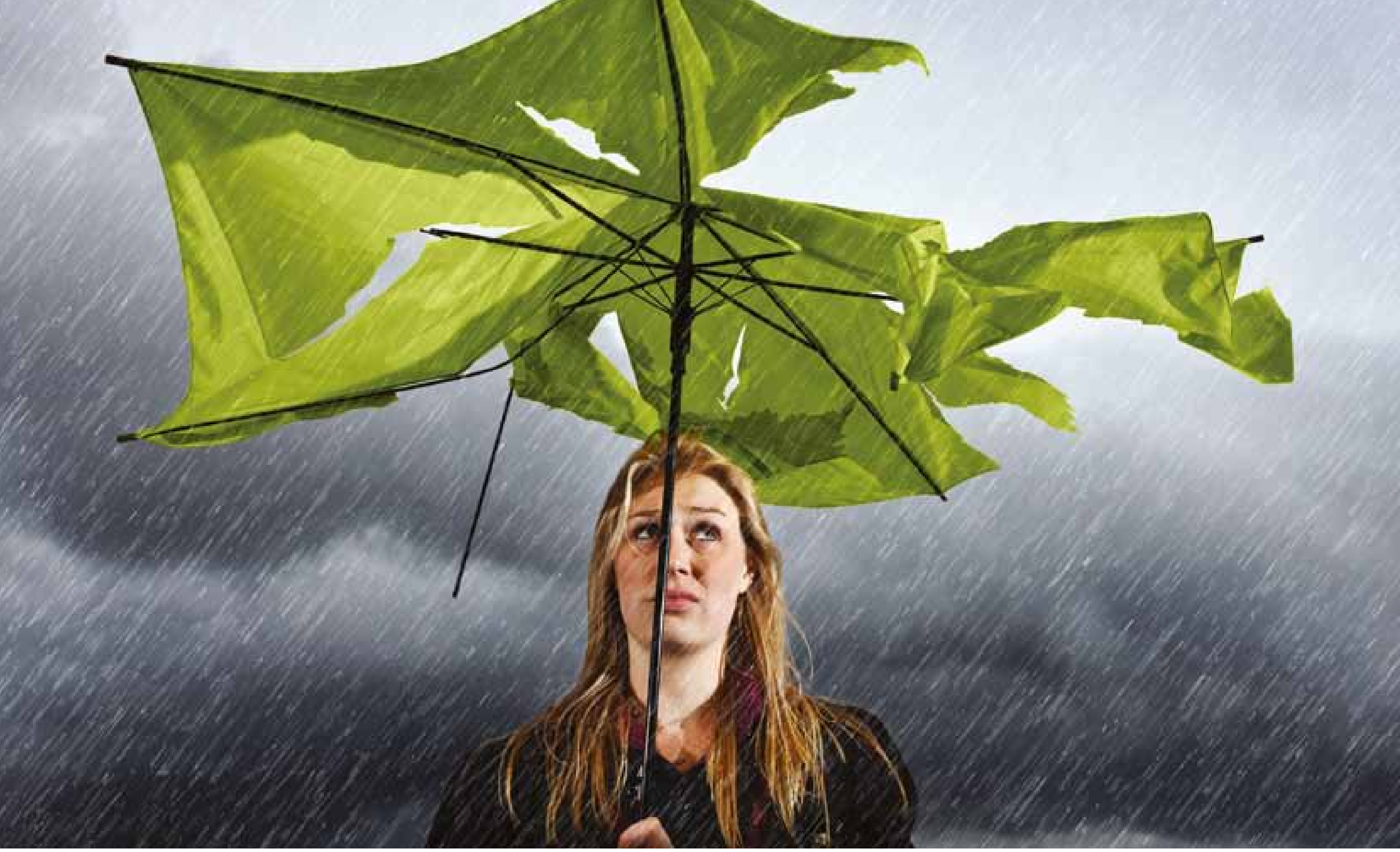
“Anecdotally, we’re hearing that there has been around about a twofold improvement in the opening of an Excel file, the processing of a workflow in our SAP system, the search through our document system.”

But Seller adds that they now need to ‘right size’ the environment. “At the moment we’ve moved like for like, a lift and shift into the cloud,” he said. “We’re now about to embark on a process to look at all the systems — are they consuming the Vault environment in the most economical way? Once we’ve done that piece of work, we expect there will be a consolidation of a number of servers and a reduction in the number of cores used by various systems.”

Another benefit is disaster recovery. Before the migration, only about 20% of Airservices’ essential business systems were covered by a disaster recovery plan. “When we do our right-sizing of workloads, we can now look at increasing the number of systems — hopefully to all of them — that are covered by our disaster recovery. And being in that elastic cloud environment gives us the capability of doing that.”

Vault has also been doing a lot of work with partners such as MapR and Cloudera to build an ecosystem of options. “We have about 150 of them that now have plug-and-play solutions” that provide a broader market of specialist services, Taylor-Price said.

“That’s an ecosystem I want to tap into,” Seller said. “As other organisations and services that provide service management, monitoring and event management, like Dynatrace, ServiceNow and others, come onto Vault then I’ve got a ready-made, secure capability that I can use in the same data centre environment. That gives me huge opportunities I wouldn’t have realised if I hadn’t gone down this path.”



NICK SOUTHCOMBE

CEO, FRONTIER SOFTWARE

LEADERS
IN TECHNOLOGY
2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

Over the past few years, there has been much hype about and significant adoption of AI applications on smartphones, websites, chatbots etc. This trend will continue with both governments and businesses utilising AI and machine learning to support chatbots, automate functions and tasks to hasten services and drive headcount reduction. As organisations learn how and where to deploy these technologies and skilled resources become available, adoption will increase.

Blockchain will start to emerge as a killer technology for identity management during 2019. However, it will take another three to five years to mature and be adopted by business software applications.

WHICH ICT INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS TELLING YOU THEY ARE MOST WORRIED OR ENTHUSIASTIC ABOUT IN THE YEAR AHEAD?

Customers and prospects are focusing on matters relating to security, such as cyber threats and privacy. Fuelling the growing awareness is the introduction of new privacy legislation, notably the GDPR in Europe and the NDB in Australia. In addition, there have been some well-publicised data breaches, pushing security to the forefront of business thinking. We are fielding more requests to conduct security audits and system penetration exercises. There is also an increased demand from the market to adopt extra layers of security, for both data in transit and data at rest, utilising the newest technologies.

Security-related issues and technologies will get first bite of IT budgets during 2019. This is good news for ICT companies in the security product and services space, but less so for providers of business application software and services.

WHAT WILL BE THE BIGGEST GROWTH OPPORTUNITIES FOR YOUR COMPANY AND YOUR CUSTOMERS IN 2019, AND WHY?

After addressing security and privacy, mobility, mobility and more mobility. On any device. Organisations want to free their workforce from their workstations and to offer access to applications when and where they want, 24 hours per day, 7 days per week. The demand for user-friendly mobile applications is almost insatiable.

WHAT'S ON YOUR TECH WISH LIST FROM INDUSTRY, REGULATORS AND INNOVATORS IN 2019?

Firstly, everyone wants faster internet speed within Australia and from Australia to the rest of the world. During 2018, Australia's global ranking for the average speed of fixed internet connections dropped from 50 to 55. Besides limiting efficiencies within Australia, our poor connections to the rest of the world are hampering Australia's ability to be a global service provider. Not only does the nbn need to deliver on its promise, regulators have to create an enabling framework that encourages and rewards innovators to chase down this gap.

Secondly, the nirvana of development tools is one that can enable us to easily produce software — apps or browser-based — for all types of desktops, tablets and smartphones, and their associated operating systems, from a single set of code.

Nick Southcombe is CEO at Frontier Software. Previously he held general management positions in both regional and international markets. Leveraging over three decades of experience, Nick has overseen the development of the Frontier Software brand and its position in the marketplace.

©stock.adobe.com/au/Worawut

Hitachi signs deal with NSW Government

The NSW Government will work with Hitachi, after the two organisations recently signed a memorandum of understanding (MoU).

The agreement illustrates Hitachi's commitment to collaborate with the state on the development of its Western Parkland City and Western Sydney Aerotropolis.

As a leading global technology player with significant experience in elements of smart city and emerging technologies, Hitachi will lend its expertise to help western Sydney achieve its vision of creating a new city that is at the forefront of technology globally. It will provide the NSW Government — in conjunction with the federal government and eight municipalities in the western Sydney region — with state-of-the-art precinct design and social infrastructure services.

Areas of potential cooperation identified in the MoU include collaborations in healthcare precincts, the provision of operations facilities in areas of heavy engineering and the development of a technology-led centre of excellence in the Western Sydney Aerotropolis, either independently or in collaboration with other research and academic organisations.

The MoU announcement coincides with the return of the world-renowned Hitachi Social Innovation Forum in Sydney on 21 November 2018. The forum will take a deep dive into developments around big data analytics, digitalisation, smart cities and automation. Keiji Kojima, Executive Vice President and Executive Officer of Hitachi, will deliver an Executive Address, and Gladys Berejiklian, Premier of New South Wales, will give a Ministerial Address.

The MoU was executed by Berejiklian and Toshiaki Higashihara, President and CEO of Hitachi, on Thursday, 15 November 2018.

DTA making progress with ICT procurement reform

©stock.adobe.com/au/Amgun

The Digital Transformation Agency (DTA) has made strong progress implementing the 10 recommendations of the ICT Procurement Reform Taskforce report over the past 12 months since its publication.

The implementation of these recommendations has prompted the agency to stop talking about ICT procurement and instead refer to the process as digital sourcing, the agency's Chief Strategy Officer, Dr Anthony Vlasic, said in a blog post detailing the agency's progress to date.

Attention is shifting away from procuring ICT equipment to a focus on ICT as an enabler of digital transformation, and this means governments must evolve beyond a procurement process to playing a role in defining the problems being solved through sourcing ICT products and services.

Meanwhile the DTA has recently released the new Digital Sourcing Framework for government agencies, which was one of the taskforce's key recommendations.

The framework has been designed to provide principles, policies and guidance that outline how to buy digital products and services.

Other initiatives aimed at satisfying the 10 recommendations of the report include completing three whole-of-government supplier agreements, launching the hardware and software versions of the Digital Marketplace procurement portal, and simplifying the standard government–supplier contract template for digital products and services.

"With the first year now complete, we have moved our attention to making government more 'open for business'. That is, increasing opportunities to a broader set of suppliers," Vlasic said.

"After only a year, we have a line of sight to how we can deliver real transformational change. The real test — and how we will know that these tools and strategies have all come together — is if we succeed in changing the conversation from ICT procurement to digital sourcing."

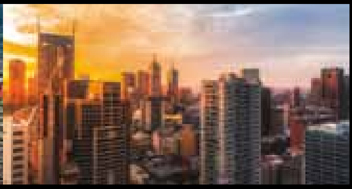
Enabling Wireless Everywhere

Wireless Tech commits to provide the latest innovative wireless products, networking technologies and tailored services in pursuit of supporting System Integrators and Enterprise Customers

PUBLIC SAFETY

INDUSTRIAL/MINING

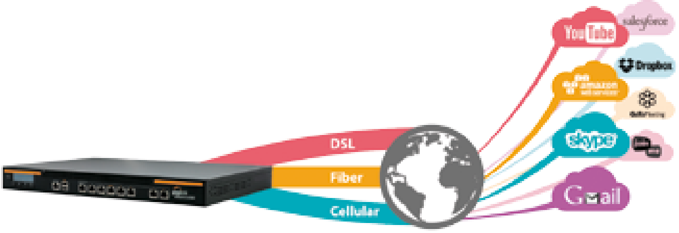
TRANSPORTATION


SERVICE PROVIDERS

- **Licensed and unlicensed wireless point-to-point links (backhaul links)**
- **Licensed and unlicensed wireless point-to-multipoint**
- **Wireless mesh technology**
- **Wireless hotspot and outdoor Wi-Fi**
- **Multi-WAN load balance routers, multi-cellular mobile routers, SpeedFusion bandwidth bonding routers**
- **Application level products: IP cameras, video decoders & encoders, IP SAN & NAS storage, enterprise SD switches, antennas, POEs, lightning surge protectors, customised network and RF cable assemblies, touch monitors etc.**

The Peplink SD World (Software-Defined World)

Software-Defined Wide Area Networking (SD-WAN) is a revolutionary way to approach the simplification of branch office networking and assure optimal application performance by using centrally controlled and managed WAN virtualization.



The Peplink SD-WAN Advantage

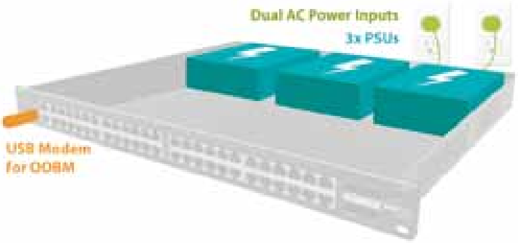
Over the years, Peplink has developed a potent combination of products and technologies that can help to build SD-WAN networks with unbreakable connection resilience, unmatched deployment flexibility, and intuitive ease of use.

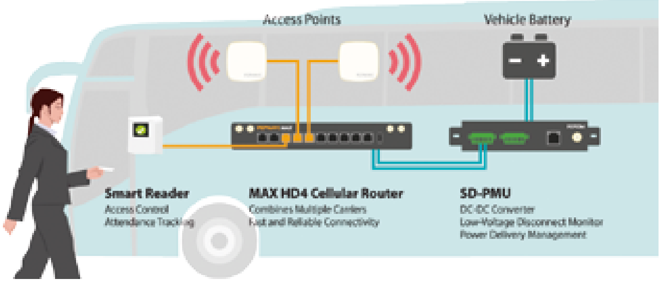
The Peplink SD-Switch Advantage

Centralized Reporting: View the status of every SD Switch, what ports are connected to which devices, and what firmware it is running, all on a single interface.

Tools to Quickly Find the Culprit: Use InControl2 (cloud-based management tool) to see all devices in your network. Search by MAC address and pinpoint the culprit's exact port.

Modern Cloud-Based Management: Centrally define VLAN and firmware update policy. Push configurations to device groups and remotely schedule PoE port operation.





The Peplink SD-PMU Advantage

Voltage Regulation and Boost: The SD-PMU can take power from sources with low or fluctuating voltage and turn them into a reliable streams of 52V. Then, it sends battery voltage information over the IoT Cloud for remote monitoring.

Low Voltage Disconnect: If the battery cannot deliver sufficient voltage, then the SD-PMU will automatically shut off access to the battery after a predefined delay.

WirelessTech

Unit 1, 63-79 Parramatta Road, Silverwater, NSW 2128, Australia
sales@wirelesstech.com.au | www.wirelesstech.com.au | (02) 8741 5080

peplink ABB Cambium Networks Siklu Magic in the air RAD ACTi Connecting Vision L-com Global Connectivity

LEADERS IN TECHNOLOGY 2019

BOB GAULT

CHIEF REVENUE AND SERVICES OFFICER, EXTREME NETWORKS

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

IoT is maturing and will become a lot more prevalent, fundamentally changing the way organisations operate. For example, in supermarkets, we are starting to see paper price tags being replaced with digital LCD screens, updated instantly via Wi-Fi. That's also a challenge, when you have thousands of stock items that now need to be managed and connected on the wireless network. To cope, manufacturers are looking to AI and machine learning to automate network configuration and management — this will ultimately become an operational necessity.

HOW ARE AI, IoT AND CYBER THREATS CHANGING YOUR INDUSTRY SECTOR, AND WHAT IS YOUR BUSINESS DOING TO MOVE WITH THE CHANGES?

We are seeing a widening of the attack surface with the rise of IoT and AI. It is our job to think through these scenarios and devise solutions. Extreme Networks is increasing the use of analytics and machine learning in its products to predict and prevent network failures and security breaches from occurring. We've even developed solutions like Defender for IoT, which delivers security for end points which have limited or even no embedded security capabilities, such as ageing wired devices.

WHICH ICT INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS TELLING YOU THEY ARE MOST WORRIED OR ENTHUSIASTIC ABOUT IN THE YEAR AHEAD?

Our customers are excited by the promise of 802.11ax, also known as Wi-Fi 6. Wi-Fi access points equipped with this technology will help organisations support more devices and more users, each with greater performance. Customers are also looking to better harness the potential of AI and machine learning, and in leveraging automation, visibility and analytics across IT domains to reduce manual provisioning and simplify network operations.

Security and risk management remain a concern. GDPR in Europe, mandatory data breach regulations here in Australia, and new Australian government initiatives like GovPass, open banking and the Consumer Data Right, are driving demand for greater visibility and control over all components of enterprise infrastructure.

WHAT WILL BE THE BIGGEST GROWTH OPPORTUNITIES FOR YOUR COMPANY AND YOUR CUSTOMERS IN 2019, AND WHY?

Extreme Networks solutions are grouped into three main buckets: Smart OmniEdge, Automated Campus and Agile Data Center. Our Smart OmniEdge solutions are designed for the enterprise edge. We expect this to be a major growth area in 2019 due to increasing use of IoT and sensors and subsequent demand for high-quality, low-latency service. Growth for our Automated Campus technology will come from the need to connect more devices, demand for cybersecurity and general digital transformation efforts.

In the data centre, operations teams are feeling pressure to keep pace with business demands for services at cloud speed, but monolithic technology stacks, limited visibility and manual processes are holding them back. Our Agile Data Center solutions will enable organisations to automate at their own pace with cross-domain IT automation, management, visibility and analytics tools that work in any vendor environment.

HOW IMPORTANT IS EDUCATION AND TRAINING FOR ICT PROFESSIONALS DURING TIMES OF RAPID DIGITAL TRANSFORMATION, AND WHAT INITIATIVES NEED IMPROVING ON THIS FRONT?

Education and training have never been more important. Training needs to be delivered in fresh new ways to keep employees interested. At Extreme, we offer an online Dojo training program consisting of competency-based curricula delivered in bite-sized video modules. Coursework covers a variety of topics, and employees receive a belt for each level completed. Feedback has been phenomenal.

Bob Gault is responsible for shaping Extreme Networks' Worldwide Sales, Channel and Services organisations as a core element of its growth and innovation strategy. He has more than 30 years' experience in sales and marketing with service providers and partners, and holds a Bachelor of Science degree in Business from West Chester University.

COLLABORATION IS KEY

Dylan Bushell-Embling

GOVERNMENTS ACROSS AUSTRALIA ARE BEING URGED TO TAKE A MORE COLLABORATIVE APPROACH TO DIGITAL TRANSFORMATION AND SERVICE DELIVERY.

Achieving the digital transformation of government service delivery will be a coordinated effort requiring careful planning, according to digital experts within the NSW Department of Finance, Services and Innovation (DFSI).

On the sidelines of the recent NSW Government Digital Marketplace conference, one of the largest meetings of ICT public and private sector leaders in Australia, the experts shared their perspectives on the challenges and opportunities involved in digital transformation within government.

According to Katarina Ruszczyk, Director of Digital Government at the Department of Finance, Services & Innovation, a common mistake for public sector agencies pursuing the digital transformation of service delivery involves the temptation to bite off more than they can chew.

“In government, because we’re charged with solving the big problems of society, there’s a tendency for government agencies to try to solve the whole problem at the same time,” she said.

“And digital delivery works [best] when you can identify what the whole problem is but then just take a thin slice of that, and just solve that really well, and then take the next slice and solve that really well, rather than trying to boil the ocean at the same time.”

Ruszczyk said the digital transformation model involves identifying a problem in need of solving and then deeply engaging with the customer to understand all facets of this problem, and that this is something that is really new in government.

“It’s something that certain pockets of government are doing really well, but others are on a different stage of their journey. So I think that’s a big challenge for government.”

Another challenge involves the lack of collaboration and communication between government digital transformation teams, according to the department’s Director of Policy and Innovation, Thea Knill.

“We are all working on so many amazing opportunities and projects, and we forget to share that knowledge and information across agencies, and

© stock.adobe.com/au/kasto

sometimes even across teams within the same department," she said.

Knill urged agencies to take advantage of the depth of resources and knowledge at their disposal when designing digital projects. This should include using the programs being offered by lead digital agencies such as the DFSI in New South Wales or the Digital Transformation Agency federally.

"[At] the DFSI, we have a digital accelerator team, an innovation team, and they're resources for across government. And we're there to support other agencies in sharing their knowledge and sharing their lessons learned," she said.

Ruszczyk agreed that learning from each other is essential if the public sector is to successfully transform service delivery.

"There are so many examples of great product delivery teams happening in federal government in other jurisdictions, and even in NSW. So learning from how it's been done in the past and drawing inspiration from that [is important], rather than feeling like you need to reinvent it yourself."

Collaboration should involve working with the private sector as well, according to Knill. Events such as the NSW Government Digital Marketplace forum are useful for helping digital transformation teams understand the latest technologies that are available, and how they can be applied to the problems the public sector is trying to solve.

Kate Foy, Managing Director of the DFSI's NSW Telco Authority, said the unique challenges faced by government departments in transforming service delivery can be divided into three categories — people, culture and the ability to manage change.

Change is something the public sector has famously struggled with, so agencies should be focused on dedicating resources, time and people to managing change well, Foy said.

"As far as people are concerned, I think [the challenge is] making sure we've got the right capabilities, not only in the public sector, but also the partnerships with the private sector. People deliver projects, people deliver outcomes," she said.

"Tools and systems and processes are part of it, but getting the culture right — a culture focused on the customer, focused on delivering the services, focused on understanding the problems and leaning in — is really where we can start to shift the dial."

Addressing these challenges may require the development of entirely new ways of approaching digital service delivery projects. Foy highlighted a model proposed by prominent academic and Western Sydney University Chancellor Peter Shergold, who suggested in 2016 that the public sector should consider taking a cue from Hollywood.

"In the Hollywood model, amazing people — screenwriters and directors and actors and costume designers — come together, make something pretty magnificent and then move away," Foy said.

"I think we can really look at adopting that in government — how can we bring people from all parts of the [relevant] sectors together to be able to scrum in, work hard on something and then walk away with something that's a pretty amazing product?"

DIGITAL TRANSFORMATION IN PRACTICE

The NSW Government's recent digital activities represent a demonstration of these principles being put into action.

In September, for example, the government hired former New Zealand Department of Internal Affairs Service Integration Lead Pia Andrews as its new Executive Director of Digital Government, tasked with supporting greater collaboration, innovation and digital transformation across government.

The government likewise this month invited officials from the New Zealand Government to share their experiences designing digital life journey services, which aim to provide citizens with unique and tailored access to all the government service-related interactions they will require at various points in their lives.

Other major initiatives being planned include adopting common components capable of providing people with a single view of government, and building a design system that can scale the delivery of people-centric digital services across government.

Moustaches save lives
Movember's mission is for men to live happier, healthier, longer lives. With Oracle Cloud, they can innovate in the digital space to better connect with more of their fundraisers.
Dan Cooper, Global Innovations Director, The Movember Foundation

SUREND DAYAL

VP, PUBLIC SECTOR LEADER, AUSTRALIA, ORACLE

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

Blockchain is something that has been talked about throughout 2018, but in 2019 I expect to see it becoming a reality for many people. Blockchain is offering an alternative for trust in an ecosystem. Trust will be augmented or, in some instances, replaced by blockchain. This will enable new partnerships to form and ideas to emerge far more quickly, as blockchain will remove the need to wait for a trusted third-party or governance layer to be set up. In many Government processes and functions, this will increase trust in the system.

HOW ARE AI, IOT AND CYBER THREATS CHANGING YOUR INDUSTRY SECTOR, AND WHAT IS YOUR BUSINESS DOING TO MOVE WITH THE CHANGES?

As the momentum behind digital transformation builds, more and more organisations are moving their workloads to the cloud. At Oracle OpenWorld, we announced the launch of our Generation 2 Cloud. This recognises the need to treat the Cloud space as a theatre of war with multiple threat vectors globally, requiring increased security in the cloud space. In our Generation 2 Cloud, we put customer code, data and resources on a bare metal computer, while cloud control code lives on a separate computer with a different architecture. With this approach, we cannot see customer data, and there is no user access to the cloud control code. By having separate cloud control computers we create an impenetrable barrier that protects the cloud perimeter and customer zones. We also use AI to increase the speed of defences, because humans cannot compete with the AI technologies used by malicious actors.

On the IoT front, we have built IoT into our cloud so that data from the increasing network of connected devices can be managed and harnessed at industrial scale. We see this having major impact on smart cities in particular.

WHAT WILL BE THE BIGGEST GROWTH OPPORTUNITIES FOR YOUR COMPANY AND YOUR CUSTOMERS IN 2019, AND WHY?

In 2019, we will be focused on Oracle Autonomous Database. When we talk about this technology, what we mean is a database that is self-repairing, self-securing and self-managing. It can deliver automated patching, upgrades and tuning — including performing all routine database maintenance tasks while the system is running — without human intervention. Oracle Autonomous Database is self-securing. It automatically encrypts all data, providing security updates with no downtime, along with protection from both external attacks and malicious internal users. Lastly, by autonomous database, we mean a database that is self-repairing. The self-recovering capability automatically detects and applies corrective action to ensure nonstop access to your data.

Product features aside, the really exciting part about this is what it means for organisations. It's easy to use; you can deploy a new database in minutes. Once it's set up, the next things users notice is how fast it is. Adaptive machine-learning algorithms drive automatic caching, adaptive indexing, advanced compression and optimised cloud data loading — with no effort from the end-user. Users find they can expand and shrink compute and storage independently without downtime, which results in a cost saving, as they are paying only for resources consumed.

WHAT'S ON YOUR TECH WISH LIST FROM INDUSTRY, REGULATORS AND INNOVATORS IN 2019?

In 2019, I see government being the technology platform that brings together citizens, regulators and service providers, to be able to provide services that are increasingly digital in nature and deliver citizen-centric outcomes.

Surend Dayal leads Oracle's Public Sector business in Australia, having joined Oracle after it purchased his company RuleBurst. Surend is well-known in the Canberra community. He has significant involvement at the Australian National University, and also as an angel investor in multiple local start-ups who he has mentored through the challenges of taking their businesses global.

pitney bowes

Introducing

A revolutionary new dataset for Australian Government.

GeoVision® is a comprehensive view of Australia's built environment that allows Government agencies to:

- Plan and predict risk.
- Manage disasters and emergencies.
- Identify non-compliant buildings and pools.
- Improve town planning and development.

pitneybowes.com/au/geovision-govt

NIGEL LESTER

ANZ MANAGING DIRECTOR, PITNEY BOWES SOFTWARE

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

Digital technologies that support the ‘smart cities’ agenda backed by data will be a game changer in helping to meet the infrastructure asset management challenges. Solutions like Confirm on Demand will become an essential component to the development of smart cities. Our work with Sustainable Sydney 2030 is helping the city to realise this smart vision by providing real-time updates, helping to comply with legislative mandates and managing the life cycle of $12.7 billion worth of infrastructure assets. As the demand for asset management technology grows, government agencies will be able to evaluate data to demonstrate the improvement in delivery of services.

HOW ARE AI, IOT AND CYBER THREATS CHANGING YOUR INDUSTRY SECTOR, AND WHAT IS YOUR BUSINESS DOING TO MOVE WITH THE CHANGES?

Digital transformation is a key driver to the changing tech landscape and our customers tell us that to better manage AI and IoT they need best-in-class, data-driven, cloud-based and mobility solutions to drive business outcomes. With a renewed focus on IoT, Pitney Bowes Confirm capabilities enable companies to securely gather, process and analyse data collected through IoT devices to improve physical infrastructure efficiencies. We are in a fortunate position of supporting our customers with the provision of data streams and robust management systems, helping companies transform their data into actionable insights.

WHICH ICT INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS TELLING YOU THEY ARE MOST WORRIED OR ENTHUSIASTIC ABOUT IN THE YEAR AHEAD?

With digitisation, customers get worried about the influx of data and how it is siloed across organisations. Understanding who a customer is, is more challenging than ever, as data is created both physically and digitally. But clients are excited that there are solutions for these challenges with Single Customer View (SCV). Fortunately, advanced data management solutions, such as SCV, can assist with delivering a single view of the customer, achieved by improving the completeness, validity, consistency, timeliness and accuracy of customer data through standardisation, verification and, most importantly, the production of a ‘golden record’ of data.

WHAT’S ON YOUR TECH WISH LIST FROM INDUSTRY, REGULATORS AND INNOVATORS IN 2019?

The projected number of connected devices is staggering: in 2020 we can expect this number to increase to over 20 billion. Businesses and our industry need to consider the role of location intelligence to harness the power of ‘where’ and helping to recognise the spatial component of data. Mapping of sensor data can reveal geospatial relationships that expose macro-scale patterns such as ‘heat islands’ in cities where energy consumption may be expected to be high. The coming wave of sensor-based data from the Industrial Internet provides some really exciting opportunities for innovation across industries.

Nigel Lester is Managing Director for Pitney Bowes ANZ, responsible for growing sales in-country, as well as business management and the delivery of software and services across Pitney Bowes’ data, location intelligence, customer engagement and customer information management solutions.

REINVENTING STATE AND LOCAL GOVERNMENT DIGITAL SERVICES

GOVERNMENT MUST CONTINUE TO REINVENT ITSELF IF IT IS TO REMAIN RELEVANT AT A TIME OF CHANGING COMMUNITY NEEDS. DIGITAL GOVERNMENT IS A NECESSARY AND FUNDAMENTAL STEP IN THE EVOLUTION OF GOVERNMENT SERVICES, AND THIS CREATES NEW OPPORTUNITIES TO DRIVE SAVINGS BY TAKING A FRESH LOOK AT THE WAY THESE SERVICES ARE DELIVERED.

Traditionally, government has been structured according to three separate pillars: engineering (OT and IoT), business systems (IT) and economic development (technology start-ups). Increasingly, governments are finding the need to break down the barriers between these internal structures, particularly when considering a common data strategy and technology skills development.

The innovation agenda is a key focus for many state/local governments, even though the delivery of practical outcomes can be illusive for many governments. However, a number of common success factors are emerging.

A more balanced approach is required in driving digital transformation. Some leaders are inspiring change through the introduction of contemporary technologies, while others are realigning to focus more clearly on the citizen.

Digital technology is no longer something that can be considered separately from the overall business of government, or simply as a backroom activity. Technology is now part of the underlying fabric of every part of government service delivery: from business systems modernisation, to industry policy, to the provision of IoT devices such as smart street lighting. However, coordination between these technology pillars is still typically managed through loose alignments, rather than through a concerted effort to bring the strategies together.

- Most chief information officers interviewed by Ovum continue to be focused primarily on the modernisation of internal business systems and the development of improved digital services.
- Smart IoT devices are typically being managed by city engineers, and guided by a separate business strategy.
- Economic development is also treated separately, and typically reports to the policy areas of city councils.

There is a growing need to develop better coordination between the three pillars. The key reasons typically relate to skills retention and information management. Ovum has found that the more advanced councils are looking at coordinated strategies linking the three pillars, such as integrated data management, advanced analytics and open data, as well as integrated geography-wide strategies around people and skills retention.

IoT — MORE THAN DEVICES

The Internet of Things has quickly become a pervasive part of local government. We now have smart lighting, smart parking, smart traffic management and smart cities. IoT is inevitable for all governments, but these often involve big and expensive assets with long depreciation cycles. Limited budgets and fragmented approaches mean that some local governments have limited themselves to small, targeted smart city initiatives, covering only a single application or neighbourhood.

© stock.adobe.com/au/YiuCheung

DRIVING THE DIGITAL ECONOMY

Economic development continues to be a core function of government, and state/local governments have redoubled their efforts to attract small business in the fast-growing technology sector. However, while the objectives are clear, the path to success remains elusive for many governments. Industry assistance needs to involve more than just financial support.

Government routinely collects a significant amount of data that can be a valuable source of intelligence for emerging industries. It has always aimed to provide the best policy and regulatory environment to encourage innovative small businesses to flourish. However, as small business transforms, government must remain in lockstep with these changes. In the digital era, government must find new ways of listening to the emerging needs of small business.

PRAGMATIC APPROACHES

The time for simple 'fix my street' apps has long passed. Today, the big challenges are about providing a broader and more integrated response that goes to the very heart of reinventing government service delivery. The previous focus on quick wins has created a false impression that transformation can be successfully delivered by just writing another app. Unfortunately, real-world government administration is much more complicated.

Ovum research has found government agencies are evenly divided around two popular methods for driving transformation:

- Some government agencies are driving change through innovative technology, such as mobile/omnichannel services for citizens or leveraging cloud services to transition quickly to new and innovative services.
- Others are driving change through a fundamental realignment in favour of the citizen. These government agencies invest their efforts into measuring citizen feedback and driving the human aspects of change.

INNOVATING WITHOUT DISINTEGRATING

Innovation is a key focus area for many state/local governments, but the achievement of practical outcomes can be elusive. It is not just an issue that can be solved in a hierarchical way. Leadership is everybody's responsibility, but the message is often diluted as it moves up the hierarchy and across the organisation. Most significant concerns are frequently directed up the org chart ("lack of support from my boss's boss") and across the org chart ("lack of engagement from my peers").

A SOLID FOUNDATION

For years, IT managers have been chastised for not being sufficiently business-focused. The lack of business alignment has been the topic of countless editorials, surveys and self-help groups. Perhaps the most enduring image has been the self-imposed 'wall' between the business and IT.

Today's IT challenge is not about managing and maintaining the walls that create separation and boundaries, but about finding efficient and effective ways of tearing them down. Citizens are looking for more agile and flexible solutions from government, and they do not want to be concerned about how government agencies are structured internally. Local government digital services are feeling the impact of this challenge even more acutely, as adverse community feedback can be swift and direct.

Common platforms need to replace bespoke systems. Even when there may be general agreement that a particular system has outlived its usefulness, there will always be some parts of the organisation that will fight hard to keep that system running. Successful government agencies have solved this problem through negotiation and pragmatism, rather than by building barriers.

REINVENTING GOVERNMENT SERVICES

The community now expects to interact with government in a certain way, and this creates new opportunities to drive savings while improving service delivery. The requirement that one should be balanced against the other no longer exists. In this context, digital government is about good government. It is an opportunity for government to innovate, serve and engage with the community in a better way. It is a turbulent time for democratic government, as governments globally scramble to be more responsive to changing community needs while retaining confidence in the processes of government.

This research was commissioned by Infor and conducted by Ovum. A more extensive White Paper on this topic is available at www.infor.com

SECURE YOUR ENTERPRISE

Protect your business
and mitigate security risks

BlackBerry®

DAVID NICOL

MANAGING DIRECTOR, BLACKBERRY — AUSTRALIA AND NEW ZEALAND

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

Mobility and hyper-connected 'things' such as drones, robots, wearables and vehicles are already changing how products and services are delivered in the private and public sector. Many organisations are testing new technologies for a variety of uses, but are hesitant to fully deploy — hampered by complexity and security risks.

Ultimately, we believe a game changer in 2019 is software that offers ultra-security, letting departments fully embrace digital transformation by allowing all those connected endpoints to truly trust one another, communicate securely and maintain privacy. The key is simplicity and ease of management — meaning a single platform that can secure and manage all existing endpoints now, but will scale to embrace the new things as they enter the workplace.

Another game changer is the use of more intelligent crisis communication technologies to account for people and maintain business continuity in the case of an incident. This means the use of multi-modal, two-way communication to ensure trusted messages are sent in real time.

HOW ARE AI, IoT AND CYBER THREATS CHANGING YOUR SECTOR, AND HOW ARE YOU MOVING WITH THE CHANGES?

As a company that has transformed through significant disruption, BlackBerry is not just moving with the changes but is several steps ahead. Let me share a couple of examples. First, we recently announced BlackBerry Spark is coming in 2019, a next-generation platform that will allow enterprises to leverage AI and manage smart 'things' regardless of operating system. It will also enable people to use and trust any hyper-connected end-point by making military-grade security easy and intuitive to use.

BlackBerry has also entered into a definitive agreement to acquire Cylance by February 2019. Cylance's technology has proven effective at predicting and preventing known and unknown threats to fixed endpoints, including stopping zero day threats such as Petya, notPetya and WannaCry.

WHICH ICT INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS TELLING YOU THEY ARE MOST WORRIED OR ENTHUSIASTIC ABOUT IN THE YEAR AHEAD?

Our customers are concerned not only about how data is securely shared between connected endpoints, but recognise that it is also a people issue. Behavioural change is becoming just as important as having the right software — and organisations are often faced with a skills gap when it comes to cybersecurity. Are staff educated to identify a threat? Are the processes in place to respond when a threat becomes real? Who can help?

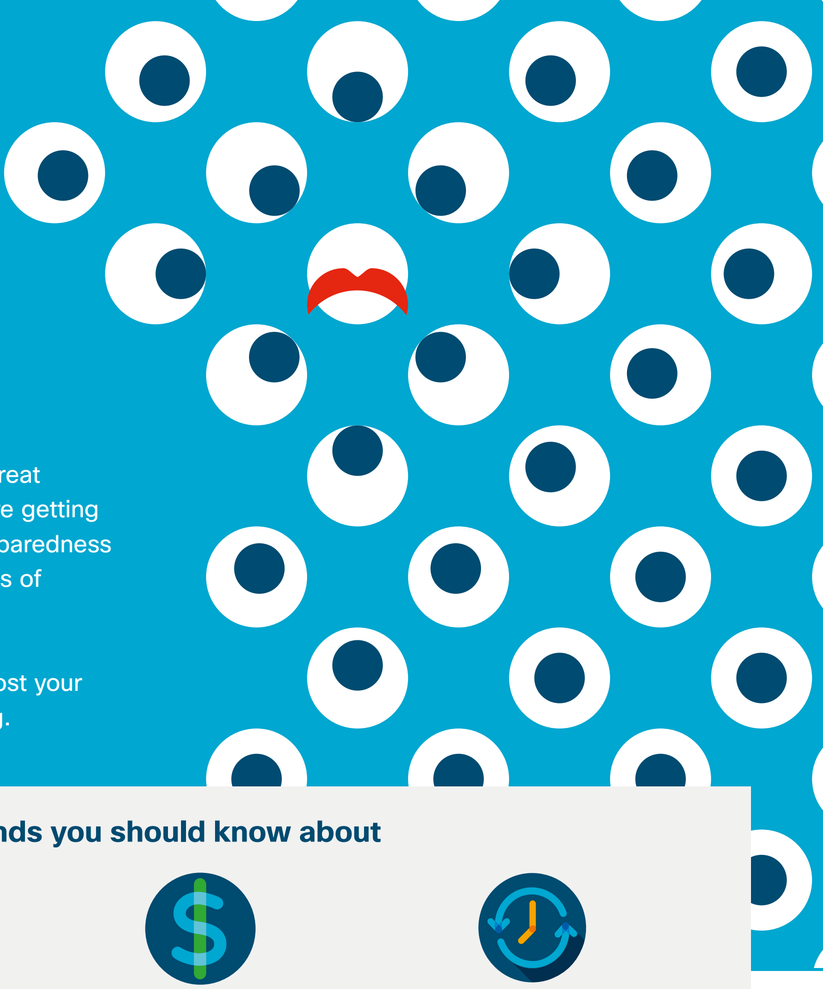
Departments need to get focused with available resources, or get the right help externally. As well as investing in the right tools, it is most important to build out capabilities, particularly in development operations teams, to ensure new apps and automated processes are secure by design from the beginning. Our cyber-experts work with many customers faced with this challenge to help evaluate, identify focus areas, then take action.

WHAT'S ON YOUR TECH WISH LIST FROM INDUSTRY, REGULATORS AND INNOVATORS IN 2019?

When a cyber attack happens, we usually think of the digital impact. But the reality is that large-scale cyber attacks are also affecting lives. Look at how WannaCry led to UK hospitals re-scheduling urgent operations in 2017. This is changing how any organisation with a duty of care is planning for risk in an increasingly complex world. We see a lot of opportunity for the government and private sector to work together to introduce regulation that will enable more effective and cost-friendly networked critical communication networks. The end goal? A more crisis-ready and cyber-resilient Australia.

David Nicol is the Managing Director for BlackBerry in Australia and New Zealand. With over two decades in leadership roles in the IT sector, David heads a team of software and cybersecurity experts who help companies and governments mitigate security risks, protect endpoints and communicate securely and privately.

Open your eyes to cybersecurity



Asia Pacific is the world's fastest growing region. But with great opportunities come serious cybersecurity threats. Attacks are getting more sophisticated. There is a prevalent lack of security preparedness leading to greater scrutiny from stakeholders and higher risks of financial and reputational losses.

In today's cybersecurity landscape, a single oversight can cost your business overnight. It's time to put security above everything.

Eye-opening APJC trends you should know about

53%
receive more than 10,000 alerts each day

51%
of cyberattacks resulted in a loss of more than $1 million

$433,000
losses incurred by a large enterprise that instantly detected a breach

$1,204,000
losses incurred if detection is delayed by more than a week

Six ways to reduce risk

There's a lot of cybersecurity challenges to overcome, but following the best practices below can reduce exposure to emerging risks, slow attackers' progress and provide more visibility into the threat landscape.

☑ Implement first-line-of-defense tools that can scale, like cloud security platforms

☑ Employ network segmentation to help reduce outbreak exposures

☑ Perform deeper and more advanced analytics

☑ Review and practice security response procedures

☑ Back up data often and test restoration procedures

☑ Access timely, accurate threat intelligence data and processes

Make security your priority

www.cisco.com/go/openeyestosecurity

STEVE MOROS

DIRECTOR OF CYBERSECURITY, CISCO

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

We will see threat intelligence and integrated security approaches reach maturity. These will be real game changers in 2019 as they play a key role in resolving many of the core challenges organisations are faced with. One of the key things to come out of the Cisco 2018 Asia Pacific Security Capabilities Benchmark Study, is the complexity of the environment. Australia has one of the most complicated landscapes in APAC — a huge number of organisations have more than 10 security vendors — but we're going to see a lot more consolidation. In addition, our customers are telling us they are most about innovations and disruptions in cybersecurity, multicloud, automation and 5G in the year ahead.

WHAT WILL BE THE BIGGEST GROWTH OPPORTUNITIES FOR YOUR COMPANY AND YOUR CUSTOMERS IN 2019, AND WHY?

As we go more digital, more becomes vulnerable from cyber attack. Customers' attack surfaces have grown exponentially, putting them at increased levels of risk. The network is a critical component for building cyber resilience. We also increased investment in digital infrastructure that is 'software defined' and can be automated and assured. Everyone is wanting to leverage this technology.

There'll also be investment in private-public cloud security, management and orchestration — running workloads where it makes most sense economically, from a reliability and risk perspective. And delivering reliable, available, secure applications that provide the best user/employee experience — this is how we are interacting with business and government more and more; it's an application and mobile economy.

WHAT'S ON YOUR TECH WISH LIST FROM INDUSTRY, REGULATORS AND INNOVATORS IN 2019?

In terms of cybersecurity, the defenders are trying to fight a war against unlimited attackers. So we need to build an ability for more threat and intelligence sharing across the industry to combat the alarming growth in cybercrime. Industry, corporations, governments, academia and technology vendors need to work together. For example, if a big financial institution is attacked, they should share that information because information about what they were hit with can be passed around and put into that threat intelligence layer. So then what happens is that we start protecting Australia and the economy, minimising the bad guys' ability to find a surface area for attack.

HOW IMPORTANT IS EDUCATION AND TRAINING FOR ICT PROFESSIONALS DURING TIMES OF RAPID DIGITAL TRANSFORMATION, AND WHAT INITIATIVES NEED IMPROVING ON THIS FRONT?

ICT is one of those industries that has that additional challenge of moving at such at rapid pace. This makes it difficult for professionals to stay current and across current trends. There is some great work happening in the training sector now around the emergence of micro credentialing. E-learning has been around for a long time, but it is about how best to use this mode in the most effective and impactful way. Offering modularised content for the adult learner to grab and learn 'on the go' is what mainstream education providers are starting to invest in. Technology lends itself to support this, as learners can learn not just from their laptop but from their phones and tablets, and through podcasts or videos.

Steve Moros is Director of Cybersecurity at Cisco. He is a Cisco veteran of 18 years with experience in working across the ANZ business with key customers and partners. He is passionate about building cyber awareness on a broad scale and is focused on helping organisations build cyber resilience capabilities and strategies for protecting their data, assets and customers.

CHARLIE HAMER

CO-FOUNDER, PUBLIC SECTOR NETWORK

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

I think cloud is getting there in government, and cybersecurity certainly has been a priority, along with a push towards AI and automation. Real-time data analytics is also moving along, and there are some great use cases now in government about this.

HOW ARE AI, IOT AND CYBER THREATS CHANGING YOUR INDUSTRY SECTOR, AND WHAT IS YOUR BUSINESS DOING TO MOVE WITH THE CHANGES?

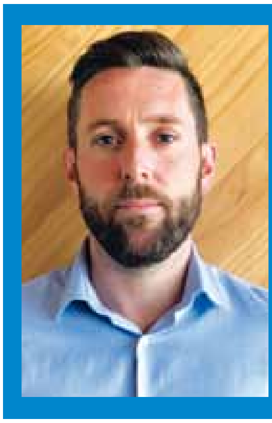
If you look at AI, IoT and cyber, you immediately think of the smart cities movement, and by that I mean everything from transport and healthcare to education, and other key government departments. As we know, IoT will permeate every part of our lives in future, and with that comes challenges. One personal challenge for me recently was when I was looking at baby monitors and cameras for my son's room, and reading some of the horror stories about them being hacked and personal information being stolen from the parents — crazy, and something you would often not think about. PSN is fully aware of these challenges for the public sector in particular and has tailored events and training around a number of these topics, from our Data Management & Analytics Series with Deloitte, Smart Cities Series with KPMG and our Cyber Series with PwC.

WHICH ICT INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS TELLING YOU THEY ARE MOST WORRIED OR ENTHUSIASTIC ABOUT IN THE YEAR AHEAD?

AI, robotic process automation and machine learning seem to be the most concerning, but are also the most interesting new areas of focus for the public sector. As always, there is concern that these technologies will remove jobs; however, as we know, this is not the case. Automating the more menial jobs and tasks frees up workers to focus on the higher value tasks and offers a better service to citizens and key stakeholders. I heard a great story recently of departmental field workers who, in the past, would have taken 20 minutes to conduct a fire risk survey. But with the technologies mentioned, as well as mobile and some digital apps, the department was able to pull together multiple data sources (including open data from the Bureau of Meteorology) and have a result back in under one minute. This is the type of innovation that is only scratching the surface of what is possible with advanced technologies.

HOW IMPORTANT IS EDUCATION AND TRAINING FOR ICT PROFESSIONALS DURING TIMES OF RAPID DIGITAL TRANSFORMATION, AND WHAT INITIATIVES NEED IMPROVING ON THIS FRONT?

Education is paramount. If you stand still, you are left behind — it is as simple as that. Given the rapid pace of technological change and the growing need to adapt and be agile based on the needs of the customer, continuing education — whether that be in-person, online, networking functions or working groups — is critical to ensure that the public sector can keep pace with change. There is no need to be fearful of new technologies — by embracing change and accepting that these things will happen with or without you, enables you to continue to learn. Key skills in data analysis and problem solving are important, but so also are often-overlooked softer skills. Improving emotional intelligence should be a key piece of our continuing education moving forward.



Charlie Hamer is Co-founder of Public Sector Network, a research and events company. He works with government bodies, consultants and technology vendors to develop public sector research, events and training in a number of areas. He is passionate about innovation and technological change.

BUILDING A SECURE NETWORK INFRASTRUCTURE

Vince Parry, Director–Government ANZ, Alcatel-Lucent Enterprise

GOVERNMENTS CANNOT RELY ON LEGACY NETWORK TECHNOLOGIES TO KEEP PACE WITH MODERN MOBILITY, IoT AND SECURITY DEMANDS.

© stock.adobe.com/au/Sergey Nivens

As Australian governments, large and small, strive to integrate the latest innovations in mobility, data analytics, cloud computing and IoT into their processes and IT systems, it quickly becomes clear that their underlying network infrastructure will be fundamental to achieve successful outcomes.

Legacy network architectures aren't equipped to support today's user needs — or the new technologies that governments must implement to support a digital transformation. Such networks are unable to support new use cases and scenarios that integrate new technologies to benefit the business, and can no longer offer secure and efficient operations. For instance, they likely were not designed to provide the capacity needed to meet today's instant-on, multi-device load on the network generated by the latest wave of multimedia applications.

In this landscape, Australian governments must rethink the very foundation of their networks to reduce costs, improve performance and security, and support new devices, technologies and business use cases.

The federal government's Digital Transformation Agency (DTA) understands this, which is why network equipment and services are two of the key categories in its Hardware Marketplace. The DTA is also encouraging a cloud-first philosophy, which, by its very nature, is heavily dependent on the provision of reliable, high-speed networking.

DRIVERS OF NETWORK TRANSFORMATION

The following set of three key trends will drive network infrastructure transformation for government departments and agencies.

Mobility and BYOD. The proliferation of mobile devices connecting to the network is the single most important factor driving the need for evolving the network. According to Deloitte, smartphone ownership rose from 84% of all Australians to 88% in 2017, with at peak of 90–95% expected in the next few years. However, as use of mobile devices increases, networks can easily be overwhelmed with bandwidth demands. For government departments, the problem remains of onboarding and securing the multiple different devices users bring to the network under BYOD policies.

IoT and exploitation of data. Governments of all sizes are taking the IoT very seriously, seeing in it the opportunity to collect valuable information and control infrastructure. An example is Launceston's LORA network, which will gather data on transport, inventory control, traffic, health and sensing, all in real time. And in NSW, the Newcastle and Lake Macquarie councils are installing shire-wide LoRaWAN networks that they see as being 'game changers' for the provision of services.

These IoT networks generate unprecedented volumes of data, presenting challenges for network management and security. To gain the benefits of IoT, Australian governments will require a cost-effective network infrastructure that simplifies IoT device on-boarding, ensures system security and is easy to manage and operate.

Government networks must be resilient, high-performing and scalable to handle ever increasing volumes of traffic. These data flows can now produce their own performance and inspection data, enabling new insights into network operational efficiency and agility. Such services create a kind of self-monitoring network consciousness and intelligence that enables automation of IT functions, increasing network security, resiliency and management simplicity.

Rise of cloud and services. As Australians are now using their mobile phones everywhere for everything, another challenge for government network administrators is to take advantage of this trend by looking for additional ways to engage with citizens and enhance the user experience, while maintaining network integrity, reliability and security. Location-based services (LBS) offer the potential for new services such as targeted communications — for instance, alert messages sent during emergencies and natural disasters. LBS can also provide information that can be analysed to reveal citizen behaviours so that departments and agencies can optimise the services they provide.

> *Security is a fundamental component in government network architecture, especially with BYOD, IoT and new applications from the cloud.*

STRATEGIC APPROACH

Alcatel-Lucent Enterprise (ALE) believes the solution to these challenges lies in adopting the correct network services strategy, underpinned by three pillars:

- Securing mobile and IoT networks by properly onboarding, managing and securing all elements of the network, backed up by sophisticated analytics and management systems.
- Aligning business objectives and investment strategies with flexible provision models, including CAPEX, OPEX and cloud-managed hybrid infrastructures.
- Adopting a verticalised connected experience through value-added solutions and dedicated integration and capabilities designed for specific ecosystems in healthcare, transportation and general government needs.

The need for security hardly needs any description. Cyber attacks are increasing in volume, in complexity and in recovery cost, and the expense isn't limited to direct financial loss — it also includes damage to public confidence. A high-quality user experience can only be assured if the network is always running and the information is protected. Security is a fundamental component in government network architecture, especially with BYOD, IoT and new applications from the cloud. More than ever before, security needs to be built in from the ground up and applied universally across all methods of access for the network.

Layered security should start with network integrity, device security, user profiles, application analytics and then moving to the levels of IoT containment, the operating system and code validation.

ALE recommends an optimised, high-performance network design based on a single network infrastructure with a secure, automated, efficient, virtual private network (VPN) for every department. We also recommend a multi-layered approach to securing the network from the edge, to the core, and shortest path bridging (SPB) to optimise network performance and minimise network downtime when adding, removing or replacing network devices.

An additional consideration is distributed intelligence control technology, which removes the possibility of a single-point-of-failure from the network and enables easy scalability. And a unified access framework provides for policy integration and consistent user experience, giving users a single set of credentials that grants them access to wireless or wired services with maximum security.

Smart analytics can enable improved decision-making and network planning by providing visibility and detailed information about the network, users, devices and applications being used on the network. It also provides predictive analysis reports that give visibility into potential future bottlenecks.

By adopting the approaches described above, Australian governments can ensure their network infrastructure is fit for purpose in the provision of essential public services, while maintaining the flexibility to meet the opportunities and challenges presented by an increasingly connected world.

CYIENT

REAL-TIME DATA IS CRITICAL FOR COMMUNICATION SERVICE PROVIDERS

WHAT'S IMPACTING THE USER EXPERIENCE?

- Large volumes of customer data
- Lack of insight-driven solutions
- Limited data optimization
- Fragmented data continuity

WHY THE NEED TO GET ITOA?

- By 2020, approx. 1.7 megabytes of new data will be created every second
- At the moment less than 0.5% of all data is analyzed and used
- Poor data quality can cost businesses 20% to 35% of their operating revenue
- 5% increased productivity and 6% increase in profits for businesses who adopt data-driven strategies

ITOA can transform the telecom industry
by providing actionable insights in real time to improve end-to-end customer experiences.

IT'S TIME TO CHANGE HOW CSPs INTERACT WITH IT OPERATIONS

To learn more scan the QR code
or visit us at **http://go.cyient.com/itoa-video**

cyient.com

SANJAY KRISHNAA

SENIOR VICE PRESIDENT, COMMUNICATIONS BUSINESS & PRESIDENT, APAC, CYIENT

LEADERS
IN TECHNOLOGY
2019

HOW ARE AI & IOT CHANGING YOUR INDUSTRY SECTOR, AND WHAT ARE YOU DOING TO MOVE WITH THE CHANGES?

Artificial intelligence (AI) and IoT are generating intense heat, and developments in these fields show no sign of abating. However, service providers are looking at AI and IoT to combine to eventually hand over control of the network to machines. The adoption of 5G in the near future will further complicate matters, as it will require network analytics capabilities to support complex network slicing and optimisation. We have recently launched the IoT-enabled Tower Operation Centre, which helps better manage and monitor passive cell tower infrastructure using advance analytics and IoT. Our solution enables efficient tower monitoring resulting in attraction of new tenants and increasing tenancy ratio and profitability. It also addresses issues such as escalating energy costs, lack of visibility on asset health, increasing tower downtime, managing unsecured remote sites, and fuel pilferage.

WHICH INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS MOST WORRIED OR ENTHUSIASTIC ABOUT FOR THE YEAR AHEAD?

Well, the biggest worry for CSPs is revenue growth. This is the struggle that every carrier globally is experiencing. As the margins are shrinking with the consumers, the focus for them will be on the enterprise business — they will have to be innovative here. The current structure and mindset don't support this business model and need to be addressed.

There is also a sense of both excitement and concern from customers we have spoken with as to how the new era of AI will empower innovation within their organisations. The deployment of AI along with RPA will work across customer engagement, business process transformation and securing of mission-critical virtual assets. AI has the potential to be one of the most momentous and transformational technologies of the next decade.

Service providers such as Cyient can help enterprises build data models and architectures that will help capture new data and improve existing knowledge models. The underlying theme that will drive the change is 'digital transformation'. Cyient brings industry and domain experience and expertise that will help enterprises extract and utilise their data more effectively — this is where we will see the biggest area of differentiation between service providers. We are currently helping some of the carriers achieve these objectives.

WHAT WILL BE THE BIGGEST GROWTH OPPORTUNITIES FOR YOUR COMPANY AND YOUR CUSTOMERS IN 2019?

In our conversations with service providers globally, there is a sense of urgency in building capabilities around all aspects of delivery of network-related services and solutions. Clients are looking at how can they take a digital leap forward, bringing digital transformation, enhancing customer experience with a focus on network automation and closed-loop networking, bringing in new partner ecosystems, and employing artificial intelligence and M2M services. Cloud is another big thing.

Growth for us would align with what our customers are looking for. For the last 25 years we have seen how the telecommunications sector has transformed, and we believe we are in a good position to support our customers when it comes to the rollout of next-gen networks such as small cell, 5G, or bringing about digital transformation through robotics process automation, IoT or AI. The deployment of small cells will be another major growth driver for our business for the next 4–5 years. We are leaders in small cell design and deployment and will continue to invest in this technology.

Sanjay Krishnaa is Cyient's Senior Vice President, Communications Business, and President, Asia Pacific region, responsible for growing the company's communications business globally and creating a robust and differentiated portfolio of offerings. He sits on the advisory board of the Deakin School of Engineering and is a member of Engineers Australia.

What value can blockchain really offer for government?

©stock.adobe.com/au/<h9>kugelwolf

Background

Blockchain is the shiny new toy in disruptive and transformative innovation. The technology has attracted a huge amount of attention and served as a lightning rod for extensive scrutiny from its proponents and opponents alike.

Adoption of the technology is flourishing, with approximately 117 blockchain-related government initiatives running across 27 countries around the world in 2017, representing significant year-on-year growth, which is forecasted to increase in the coming years.

A McKinsey industry analysis report published in June 2018 revealed more than 90 discrete use cases for blockchain across major industries. In the past, the majority of these would have been classified as discovery, proof of concept and pilot exercises, however as the projects mature from their experimental stages, an increasing proportion have transitioned to full operational deployment.

Transition to explicit trust

A blockchain is an immutable, time-linear series of data blocks forming one or more distributed ledgers across a network of nodes. Each block comprises a collection of transactions and a distinct pointer to its predecessor block. Strong cryptographic techniques are employed to maintain integrity between each block and its former and latter neighbours. This allows blockchains to be shared and corroborated by anyone in the network with the appropriate permissions.

One of the key values of blockchain is its innovative way of creating a seamless experience of explicit trust between multiple parties. Implicit trust refers to the hope that other entities in a transaction will perform their obligations truthfully according to a prior agreement. On the other hand, explicit trust offers a guarantee that these obligations will be objectively adhered to. All parties no longer need to assume reliability — everyone knows that everyone else will make good on the agreement upon the fulfilment of set conditions.

People, businesses and government organisations have been heavily relying on implicit trust to interact with each other for a long time. While this may be sufficient in certain circumstances, the industry as a whole is increasingly gravitating towards the implementation of explicit trust.

A potent example is the 'smart money' project led by CSIRO's Data61 published in October 2018. Blockchain coupled with new payments technologies were employed to provide more choice, control and flexibility for conditional payments between participants and service providers in the National Disability Insurance Scheme (NDIS).

By attaching conditions, the 'smart money' knows what it can be spent on, who it can be spent by and when it can be spent. Blockchain enables explicit trust of money use to work in unity, providing greater empowerment of participants, reduced administration overhead for businesses as well as higher visibility for government.

One piece in the stack

Blockchain technology is often incorrectly compared to full stack solutions better suited to accomplishing a certain goal, in order to emphasise and overstate its limitations.

An analogy for this would be claiming that a car can transport people better than tyres can. Blockchain is just one element in the overall technology stack of a system. It is not designed to be a sweeping, complete replacement for all of the other bread-and-butter architectural components. In fact, it is a trailblazer of a new kind.

Due to its differences to other traditional architecture constructs, many are struggling to find a mould that fits blockchain. It is not just another type of database as some business logic exists in the form of smart contracts. Similarly, it is also not just another type of application as it provides sophisticated data handling and storage mechanisms. So what is it really?

Blockchain is a new, unique element that straddles across the software, distributed network and database layers. It only comprises a subset of components and needs to be augmented with additional modules to form a complete solution. The ratio of blockchain contribution among each layer varies from one business application to another, which in turn, determines the extent of its value in a particular use case. With this concept in mind, business and technical leaders will be better positioned to analyse and understand where and how blockchain can help.

Standardisation

The Australian Digital Transformation Agency's (DTA's) preliminary findings on blockchain in the public sector, released in October 2018, highlight the challenge posed by the industry's fragmented approach to deployment, and calls for greater standardisation to accelerate the pace of adoption.

In September 2016, the International Organisation for Standardisation (ISO) approved a proposal to establish a new technical committee for blockchain topics such as terminology, privacy, security, interoperability and auditing. Australia's leadership in this area was demonstrated by the appointment of Standards Australia to manage the Secretariat of ISO/TC 207, Blockchain and Distributed Ledger Technologies.

A Blockchain Standards Workshop was hosted in February 2017 with more than 50 representatives from government, industry, academia and end users, featuring renowned international and local speakers. The event resulted in the establishment of a Roadmap for Blockchain Standards which identifies a collection of high priority standardisation domains. The work of the committee on this front continues to progress today.

Active government participation in innovation

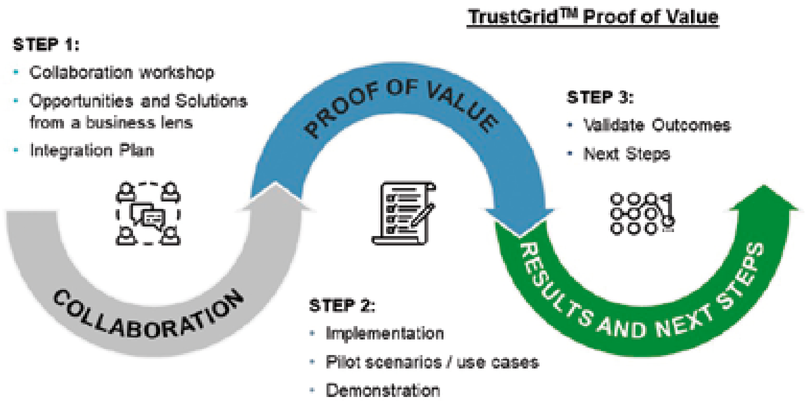
While blockchain is an emerging technology, it is indeed a promising one. The discovery of valuable applications and new business models today are only possible due to the strong drive to ideate, participate and innovate.

Government plays a central role in unlocking the potential of future public services as well as enabling the Australian industry to deliver next generation solutions to do things better and smarter. It is the willingness to engage in a conversation and manifest concepts into actions that will allow organisations to thrive in our complex and ever changing environment.

TrustGrid™ by Secure Logic

TrustGrid is a pioneering blockchain based solution by Secure Logic that delivers a digital trust ecosystem in Government, uniquely tailored to suit a wide array of use cases relevant to the public sector. The TrustGrid solution offers a high degree of privacy, security and integrity to facilitate the technology interfaces between government entities and vetted private organisations such as hospitals and financial institutions.

Secure Logic is a Cyber Security Technology Leader with a focus on delivering innovative Cyber Security and Digital Identity solutions. Speak to Secure Logic to find out how TrustGrid can work for you in three simple steps:



SECURELOGIC

Secure Logic
www.securelogicgroup.com

ARE WE THERE YET?

Greg Wells, NSW Government Chief Information and Digital Officer

DIGITAL GOVERNMENT IS ABOUT DESIGNING FOR CITIZENS' NEEDS, KNOWING THEIR STORY AND CONNECTING AGENCIES TO DELIVER BETTER SERVICES.

One of the more thought-provoking common questions we receive working in 'digital government' is quite simply, "Are we there yet?" If Denmark, Estonia and Seoul are accepted as being 'there', how does NSW get 'there' too?

We think we've made a great start. In fact, we think NSW is a leader, but many would probably agree we are not completely 'there' yet. So we are openly sharing the next steps in our journey, with a threefold purpose.

Firstly, the more input and ideas we get the better. While we are simultaneously developing and delivering a digital.nsw delivery roadmap and investment strategy, we do not have all the answers.

We are seeking a wide range of input (including from citizens) to help to shape our approach, on the basis that suggestions about what has worked elsewhere may help us to achieve our goals faster. Some of our best solutions have come from ideas generated outside government.

Agencies will continue this heritage with innovation challenges such as those being run by the NSW Department of Transport, and we hope to ramp this up through a number of new channels too, such as the Pitch to Pilot event in November.

Secondly, we want to model the way digital organisations should operate. Our objective is to transform the way government operates, from policy, regulation and investment through to service delivery and procurement. Working in the open is a foundation of this transformation.

Finally, we hope that the documentation of our journey — including what does and does not work, and what we learn along the way, will be of use to others on a similar journey.

WHERE IS 'THERE'?

We agree with Tom Loosemore, founder of the Government Digital Service in the United Kingdom, who has said: "We're not here to change government websites; we're here to change government."

For us, changing government quite simply means we support people — parents, carers, students, patients — with better government services.

© stock.adobe.com/au/Kwest

People want services that are smart, simple and seamless.

So, when will NSW be there?

'There' is when government knows and understands citizens' stories — which they should only have to tell us once (particularly for our most vulnerable).

'There' is when we support important events in citizens' lives in a way that is appropriate for their contexts and situations — where possible, without paper and without visiting a government 'office' at a time that is convenient for government.

'There' is explaining what people need to do in simple terms (not in government, or agency jargon).

And 'there' is when services are designed around citizens' needs and can be accessed in a manner of their choice.

'There' is also about government respecting citizens' time, making them feel safe, being proactive about issues that impact them and finding opportunities to help.

Feedback from people across NSW who have renewed a licence, used an online courtroom or needed a clinician to access their medical images from anywhere in the state tell us that we are 'there' with many of our services, which is great.

So the question now is: how do we do more, accelerate and scale this up?

WHAT DO WE HAVE PLANNED?

Accelerating customer experience initiatives is our number one focus. Everything we do should be viewed through this lens first. Right now we are focused on:

- working across clusters to design and deliver government services based on customer journeys and important life events. Our plan is to start with 'Making it easier for new parents to start or grow a family' and 'Making it easier to manage the loss of a loved one', as also prioritised by the Australian Digital Council;
- building more capacity in the Digital NSW Accelerator (DNA) Lab to work closely with Service NSW and agencies to rapidly design, test and prototype how we support these customer journeys;
- the adoption of common components across government that provide people with a 'single view of government'. We have built a Customer Experience (CX) Pipeline to enable this work. Service NSW has already delivered a range of these products, in particular the MyService Account/ID;
- building a digital.nsw design system to scale the delivery of consistent, people-centric digital services across government. The digital design system will have everything from style guidance and code for common tasks through to methods, roles and ways for the community to contribute and maintain it. The first iteration is planned for later in 2018.

However, delivering digitally enabled services means progressing work on many fronts. For example:

- a digital.nsw roadmap, funding model and architecture must be linked and our assurance model must work in this context;
- accelerating customer experience initiatives requires common architecture components and our digital design system. It is also closely linked to the way we use, share and analyse data;
- building trust with people means that cybersecurity and critical infrastructure must underpin everything we do.

Our teams are working hard not only in these areas, but also on priorities such as buy.nsw, the Critical Communications Enhancement Program (and connectivity more generally) as well as our data ecosystem, cybersecurity and technology platform priorities.

Digital government is about technology, but it's mostly about people: designing for their needs, knowing their story and connecting agencies to deliver better services. When we do this, at scale, NSW will definitely be 'there'.

Public Safety Radio Networks
Fibre and Data Solutions
IoT/M2M Solutions
Solar Energy Solutions
In-Building Coverage Solutions
Battery Storage Solutions
Your Wireless Technology Partner
RFI
TECHNOLOGY SOLUTIONS

SCOTT MAGEE

CEO, RFI TECHNOLOGY SOLUTIONS

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

The advent of 4.9G/5G mobile technology brings with it capabilities that we have never had before. Some great innovations now have their platform for delivery so we see real change coming. The other area in which are seeing huge transformation is the energy space. Advances in energy storage technology over the last five years, and what's coming in the next five, will really shake things up. The power demands of modern networks are a huge challenge for operators and everyone wants more data and more coverage, which of course requires more power.

HOW ARE AI, IOT AND CYBER THREATS CHANGING YOUR INDUSTRY SECTOR, AND WHAT IS YOUR BUSINESS DOING TO MOVE WITH THE CHANGES?

For AI the bigger issues come with commonality of platforms, data security, privacy and the like. There are similar issues with IoT. We have witnessed this in our business with machine-to-machine communications applications that our customers have been working on for many years. The difference today is the advent of high-capacity and high-coverage mobile networks that deliver these solutions on a mass scale. Equally, new technologies such as LoRaWAN and Sigfox are exciting alternatives and ones we are watching with interest; and then again the carrier and NB-IoT developments look compelling too. On cyber threats, we are always keeping an eye on these within our own business, but now with mobile technology taking this to every device... well, the threat just became bigger.

WHICH ICT INNOVATIONS OR DISRUPTIONS ARE YOUR CUSTOMERS TELLING YOU THEY ARE MOST WORRIED OR ENTHUSIASTIC ABOUT IN THE YEAR AHEAD?

Across the wireless sector our customers are seeing IoT and LTE and 5G as being great disruptors. Equally, how government radio networks now become part of the overall ICT mix is an intriguing challenge. Emergency services need security but also access to the high-speed data that LTE and 5G can provide. That's the future for mobile radio.

WHAT WILL BE THE BIGGEST GROWTH OPPORTUNITIES FOR YOUR COMPANY AND YOUR CUSTOMERS IN 2019, AND WHY?

Government radio networks across the globe have many challenges but there are some great technology opportunities. How they balance voice and data between narrowband and broadband wireless networks is what we are working on with government agencies. IoT is huge, too. Taking wireless signals above ground and extending them underground into stadiums, shopping centres, carparks and road tunnels is a growing need. People expect to be connected all the time wherever they are.

WHAT'S ON YOUR TECH WISH LIST FROM INDUSTRY, REGULATORS AND INNOVATORS IN 2019?

Advice to regulators and industry: Be sensible, don't dabble unnecessarily. Collaborate. We all hear about smart cities, and governments at federal, state and local levels are talking it up. But we need to be sensible; not going after the one great idea only to find it was time and money wasted. It's a real balancing act right now given the number of technology options we have at our disposal. We can clearly see the need for an IoT governance framework around devices and data and how they are used and controlled. Does there need to be a certified or trusted operating system or platform? Who would or should regulate that? How do we handle the legal and ethical challenges of IoT data collection and usage? These are big questions to be answered.

Scott Magee is CEO of RFI, a technology solutions company specialising in wireless coverage and solar power. He is responsible for the operational direction of the organisation, as well as executing RFI's 2020 strategic vision of becoming a major global technology solutions company.

VIRTUAL DESKTOPS FOR DOCTORS

© stock.adobe.com/au/18percentgrey

THE NT GOVERNMENT'S HOSPITAL-BASED VIRTUAL DESKTOP INFRASTRUCTURE PROJECT HAS TAKEN OUT A PRESTIGIOUS NATIONAL IT AWARD.

A virtual desktop program that enables Royal Darwin Hospital (RDH) staff to spend more time with patients and less time on paperwork has been recognised with a prestigious national IT award.

The Northern Territory's Virtual Desktop Infrastructure–Supporting Hospital Service Delivery project — implemented by the Department of Corporate and Information Services (DCIS) and the Department of Health — was one of four finalists from 25 national nominations in the Australian Computer Society's 2018 Digital Disruptor Awards.

The VDI project was technically intricate, with 10 different products configured to provide tap-on/tap-off, rapid six-second logon, hot desking, auditable access and other technology benefits for staff, and improved security of patient information.

The project was 'stress tested' in the busiest part of the RDH, and its success has seen the technology also introduced to the Palmerston Regional Hospital.

"Territorians deserve access to the best health services and this significant achievement highlights the innovative work of our health and IT sectors that leads to better health outcomes for Territorians," said the NT Minister for Health, Natasha Fyles.

"RDH Emergency Department sees about 70,000 patients a year and quick access to patient records is vital. Clinicians can access a device up to 200 times during a shift, which can add up to the equivalent of eight FTEs in a year!

"The VDI project introduced cybersecurity improvements and fast-tracked computer access for busy medical staff, freeing up time for bedside care for better health outcomes at Royal Darwin Hospital."

The NT Minister for Corporate and Information Services, Lauren Moss, said the project "is an excellent example of the Territory leading the nation in virtual desktop infrastructure (VDI)... providing a comprehensive secure solution to meet the specific needs of clinicians and ensuring high levels of patient care.

"The national award highlights and recognises the calibre of the local ICT sector and importance of investing in jobs of the future.

NT Government staff leading the project include DCIS officers Adam Smith (Director ICT Enterprise Architecture) and Greg Connors (A/Senior Director, ICT Architecture and Cyber Security), along with the Department of Health's Godfrey O'Connor (IT Project Manager). RDH's Associate Professor Didier Palmer led the clinical team collaborating on the project.

Two local professionals from NEC Australia — Wilma Weaver and Lily Kawai — were also national finalists. This was the first time three Territory ICT nominations had made finalist status in the national ACS awards.

The VDI project was also a finalist in the Chief Minister's Awards for Excellence in the Public Sector in the category 'Making the NT a Better Place to Live through Innovation'.

PUBLIC SECTOR NETWORK

PUBLIC SECTOR INNOVATION SHOW

Achieving innovation, transformation and sustainability

26th March 2019

National Convention Centre, Canberra

ANTONY STINZIANI
Chief Information Officer, Information Services Division
Department of Parliamentary Services

MARK SAWADE
Chief Information Officer
Department of Education and Training

ELIZABETH KELLY PSM
Deputy Secretary, Innovation
Department of Industry, Innovation and Science

JOSE CLASTORNIK
Executive Director of AGESIC, the National Agency for e-Government and Information Society (CIO)
Government of Uruguay (UR)

RACHEL BACON
First Assistant Secretary - Policy Analysis and Implementation Division
Department of the Environment and Energy

SARAH PEARSON
Chief Innovation Officer & Chief Scientist
Department of Foreign Affairs and Trade

Quote **GTR50** for **50% off*** your ticket - GovTech Review subscribers
*Government ONLY

Register now

Call: (02) 9008 7676

Email: info@publicsectornetwork.com.au

Visit: publicsectornetwork.co

© stock.adobe.com/au/Jacob Lund

MAKING SOCIAL MEDIA YOUR FRIEND

Cimon Constantine, Area Director, Meltwater Australia and New Zealand

SOCIAL MEDIA'S TWO-WAY TRADE OF INFORMATION PRESENTS THE PERFECT WAY FOR GOVERNMENTS TO CONNECT WITH THE PUBLIC.

Social media has democratised the public sphere, opening up new ways for governments to disseminate information and engage with constituents. It is now a vital platform for government outreach. And constituents now have the power to share their opinions as easily as any minister. But with opportunities come new challenges. It's no longer good enough to be simply using social media. It needs to be seen as a crucial element to engage with constituents and help make decisions.

UNDERSTAND WHAT REALLY MATTERS

Social media has become a soundboard for ideas and opinions, so it's important to be across what is being said on these platforms. Understanding what constituents want starts with listening to these online conversations, and not just as a one-off exercise. These conversations move fast, so social media listening tools that monitor what's being said online will ensure you have the right information to understand the situation and make an informed decision, fast.

Earlier this year, Queensland school girl Dolley Everett tragically took her own life after being subjected to relentless bullying. Her friends took to social media, starting a campaign that went viral and resulted in the government investing $3.5 million on cyberbullying awareness, education, detection and prevention campaigns. It also inspired new laws to combat cyberbullying and online trolls.

By listening to the opinions and concerns of constituents on social media, both the federal and state governments were able to quickly respond and propose a plan of action.

CRISIS PREVENTION AND MANAGEMENT

In the digital age, news spreads in seconds. Instead of dealing with the fallout after the fact, conversations need to be identified early and in real time before they spread far and wide. This is crucial to preventing and mitigating potential crises.

Keyword and influencer monitoring is a good place to start, but beyond this, governments should set up anomaly detection so any abnormal rises in chatter are flagged before they have a chance to escalate into a full-blown communications crisis. A sudden spike in social mentions of a politician could point to a potential issue which, left unaddressed, could spread into a full-blown crisis.

Consider Malcolm Turnbull's recent rebuttal Tweet to Scott Morrison's radio appearance on Alan Jones's radio show following his visit to Indonesia on behalf of the Prime Minister. Turnbull's rebuttal Tweets showed a different side of the story, amassing 6200 likes, 1242 re-tweets and 1335 comments. But if Morrison left the conversation without correcting the record, the end result could have been a lot worse for his image with the Australian public. Government representatives at any level must be on the front foot to identify and respond to conversations accordingly and mitigate potential crises.

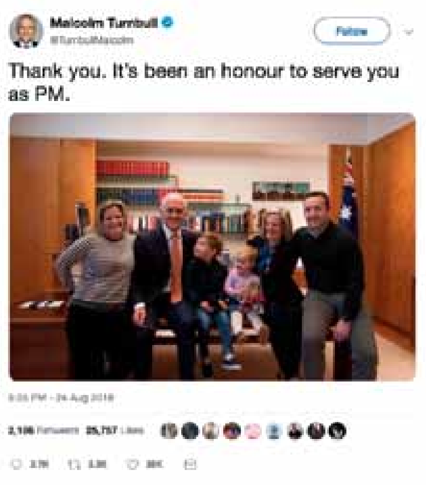
BETTER GOVERNANCE AND ENGAGEMENT

Social media has broken down established barriers between communities and governments to increase two-way discourse. But it's important to remember to keep communication on social media authentic and informative. For example, Malcolm Turnbull is known for sharing personal and political moments on his Twitter account, which has helped connect him with citizens. When Turnbull left parliament earlier this year he Tweeted a photo of his family, thanking Australia for his time as Prime Minister. The Tweet received engagement close to 30,000.

Engaging with audiences on a human level and outside of election periods helps build trust with constituents to ensure receptiveness when it comes time to vote.

YOUR SECRET WEAPON

Many media intelligence tools are capable of monitoring online news, blogs and social media, but the challenge is turning these conversations from noise to actionable insights. All levels of government should be analysing online conversations to better understand how policies and decisions are being received by the community. If not, they could be missing a huge opportunity to better engage with constituents.



Malcolm Turnbull
@TurnbullMalcolm

Thank you. It's been an honour to serve you as PM.

5:35 PM - 24 Aug 2018

Featured products

Cloud-enabled UPS

The APC Smart-UPS is a cloud-enabled UPS for servers, storage and network power protection. Smart-UPS provides availability and manageability to a network, allowing users to focus on business growth instead of business downtime. The product protects critical data and equipment from power problems by supplying clean and reliable network-grade power.

Connected Smart-UPS units have a networking feature that makes them adaptable and easier to deploy: APC SmartConnect is a feature which allows users to view the status of their UPS through a secure web portal. Through this innovative remote monitoring interface, users receive automatic notifications, firmware updates and advanced support. APC SmartConnect's easy-to-use network connectivity is designed to provide added value.

Schneider Electric IT Australia

www.schneider-electric.com/ups

Cloud infrastructure

The iQ3 Cloud Compute cloud infrastructure encapsulates Private Cloud (iQ3 and GovDC), Public Cloud (Azure and AWS), Hybrid Cloud, Testing and Data Recovery.

It is a private cloud with a client portal that enables users to create and run up to 20 VMs for 30 days free.

The solution includes access to 24/7 critical incident support, monitoring and alerting, and is fully managed by the iQ3 team of Australian-based staff.

Users will experience the flexibility to scale up and down, depending on their requirements; the ability to generate cost efficiencies to meet business demands; the opportunity to reduce operational overheads associated with managing infrastructure; and the agility to support innovation and transformation.

iQ3
VOCUS
EQUINIX
amazon

iQ3

www.iq3.com.au

STEVE NEWELL

BUSINESS DEVELOPMENT MANAGER, GME

LEADERS IN TECHNOLOGY 2019

WHICH TECHNOLOGIES OR INNOVATIONS DO YOU THINK WILL BE GAME CHANGERS OR REACH MATURITY IN 2019?

There are many different technologies competing for government attention in the business- and mission-critical communications space at the moment. But not all of them are truly mission-critical. We feel that even though consumer-grade mobile devices have a role to play, traditional technologies are still the best bet for providing reliable, robust and dependable communications for public sector workforces. That's one of the primary reasons we've entered the P25 communications market. P25 is the standard used nationwide and across the world by emergency services. It's a digital technology that gives you the same sort of mission-critical capability and benefits that the police, fire and ambulance services enjoy.

Another consideration is maintaining staff safety, which should be of prime concern for all organisations, including government. There are many technologies available to ensure worker safety, but one that is often overlooked is the personal locater beacon (PLB), which is a tried and true technology that works anywhere on the face of the Earth — you don't need to be within range of government radio or commercial carrier networks. This is an important factor to consider, given the mandatory lone-worker regulation requirements.

HOW ARE AI, IOT AND CYBER THREATS CHANGING YOUR INDUSTRY SECTOR, AND WHAT IS YOUR BUSINESS DOING TO MOVE WITH THE CHANGES?

We're going to be heavily focused on the telemetry and data space over the next couple of years. The market for these technologies is exploding, and we see it changing the way governments of all sizes operate — by gathering more and better data (both encrypted and non-encrypted) to analyse and make better decisions for citizens. The IoT and data sensors will be game changers for making things happen for local councils, shopping precincts, sports facilities, infrastructure operators (eg, tunnels, roads, pipelines) — anywhere where data needs to be collected and systems monitored.

Our customers are also very interested in the potential inherent in the 4G LTE communications standard. GME has a high recognition of the up-and-coming capabilities of LTE for mission-critical applications.

HOW IMPORTANT IS EDUCATION AND TRAINING FOR ICT PROFESSIONALS DURING TIMES OF RAPID DIGITAL TRANSFORMATION, AND WHAT INITIATIVES NEED IMPROVING ON THIS FRONT?

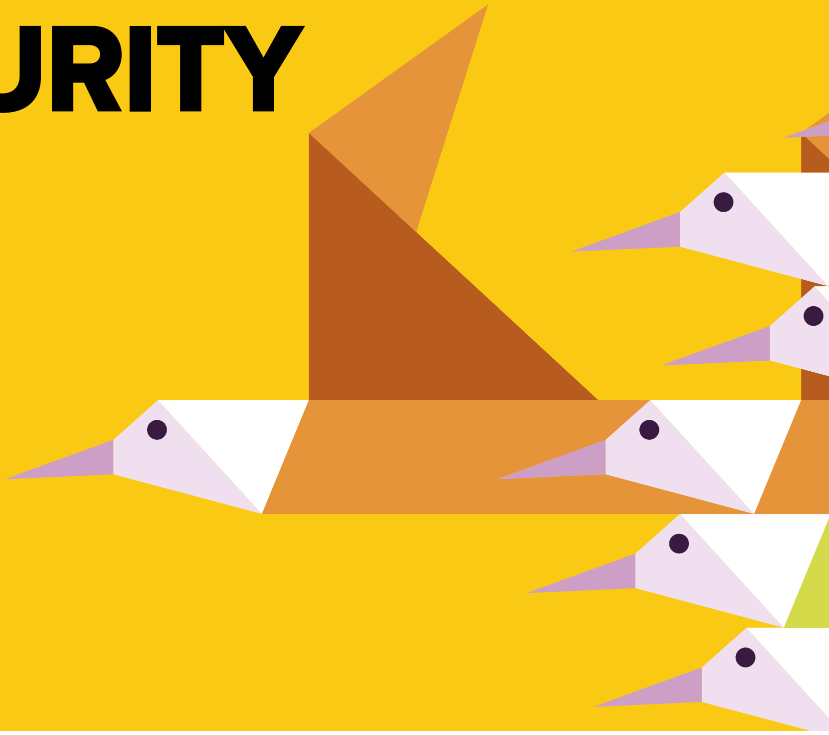
There's a big need for more skilled cybersecurity staff in the ICT world, particularly with IT and communications crossing over so heavily these days. GME has been a fairly big hirer of people in recent times, and we're very cognisant of the crossover between communications and IT. That influences our roadmap of products as well, by bringing in that talent. With recognition of where the market is going, it's a natural reaction of us to bring those sorts of people aboard.

We sometimes feel that governments and educational institutions are going more in the direction of university and the higher technology software side. But in the communications side, it's always been driven through TAFE-level training and apprenticeships. For this sector, it definitely feels as if governments have been pushing too hard at the university-level education and not enough at the vocational level. Communications people are hard to find these days.

Steve Newell is Business Development Manager (Professional Radio) for GME. He has 40 years' experience in the business- and mission-critical communications industry, specialising in two-way radio, intrinsically safe devices, telemetry and data applications. He is responsible for government and local council solution sales.

TAKING THE LEAD IN CYBERSECURITY

Thomas King, Head of Cyber Security Products, Telstra



© stock.adobe.com/au/Mangsaab

C-LEVEL EXECUTIVES ARE IN A PRIME POSITION TO PROMOTE A UNIFIED APPROACH TO CYBERSECURITY AND DRIVE AWARENESS AND ADOPTION THROUGHOUT THEIR ORGANISATIONS.

C-level executives are no strangers to risk. They make important decisions regarding financial and regulatory risk every day, and increasingly they have to do the same with cybersecurity risk.

Cyber risks are frequent and the damage caused to organisations in the event of a breach are highly detrimental. The Cisco 2018 Annual Cybersecurity Report suggests 53% of attacks now result in damages of $500,000 or more, while 8% of attacks resulted in damages in excess of $5 million.

Given the increasing likelihood of being affected by a breach, as well as the legal requirement for organisations to publicly disclose any loss of data, security is now an organisation-wide concern.

The good news is that executives are continuing to take a more active role in cybersecurity by understanding the importance of security initiatives, increasing their involvement in these initiatives and shouldering more responsibility for security incidents when they occur.

A TEAM EFFORT

The Telstra Security Report 2018 discovered the IT department is still seen as the main business unit that leads cybersecurity initiatives, with 40% of respondents believing the IT team are primarily responsible in the event of a breach.

However, the same research found a high number of respondents placing attribution of responsibility on the shoulders of the C-level of organisations — 20% of respondents surveyed held the CIO accountable for a breach, while 19% pointed to the CEO.

This trend is likely because employees expect leaders to take responsibility for issues that impact the bottom line in the way an unexpected breach can. But in an environment where a stolen device or single misguided response to a suspicious email from any employee could spell disaster, organisations need to take a unified approach to cybersecurity.

As the report outlines, more Australian organisations are putting in place an incident response plan (76% in 2018 versus 66% in 2016). They are also testing and reviewing their plans more frequently. This has resulted in improved response times in the event of a security breach.

The frequency of security reporting in Australia is also on the rise — 37% of organisations surveyed in the report are recording their security activities on a quarterly basis, with 29% submitting reports monthly. These figures are shining examples of comprehensive initiatives in practice and underscore the positive role executives can play in the development of security solutions.

These programs deliver tangible results and enable businesses to be proactive in their fight against cybercrime. Yet they require a commitment at the C-level because the deployment and execution of incident response plans demands investment, leadership from the top and effective staff training.

A HELPING HAND

Having the appropriate solutions and policies in place is important, but there is a critical human element that needs to accompany the overall process. Basic training designed to drive awareness and equip employees with the ability to spot suspicious behaviour can be the difference between a secure organisation and a hefty fine and damaged reputation.

A lot of attacks could be preventable if employees are trained in cybersecurity best practice. The Office of the Australian Information Commissioner (OAIC) publishes quarterly statistical information notifications received under the Notifiable Data Breaches (NDB) scheme. Its recent July 2018 report identified human error as the major source (36%) of reported breaches.

A large quantity of malicious attack comes back to this idea of human error. Staff can be prone to making mistakes, accidently clicking on phishing emails or disclosing passwords. Figures like those published in the OAIC report point to the fundamental role awareness plays in an organisation's cybersecurity defences.

This is because employees are the critical first line of defence against attack. Employees should be informed on how to identify potential breaches like email phishing campaigns, and organisations should have specially devised playbooks to deploy in the event of a crisis.

Executives need to create organisational buy-in by championing tailored contingency plans and long-term security education programs.

C-level executives are in a prime position to help alleviate some of the pressures of the IT department, by empowering their work-force to become a formidable first line of defence.

Regular training for staff and consultation with skilled security partners can help a company dramatically reduce any chance of a major breach. Formal and consistent end-user preparation at all levels of the business can ensure employees know how to handle sensitive data appropriately.

As modern workplaces take advantage of cloud technologies and increase their collaboration with third parties, leaders should prioritise a unified approach to cybersecurity to drive awareness and adoption throughout their organisations.

FIVE EYES FOR NATIONAL SECURITY

Dylan Bushell-Embling

© stock.adobe.com/au/SFIO CRACHO

NEW ZEALAND'S GCSB IS USING THE NATION'S MEMBERSHIP IN THE FIVE EYES ALLIANCE TO HELP SAFEGUARD NATIONALLY SIGNIFICANT ORGANISATIONS.

The New Zealand Government is leveraging its position as a member of the Five Eyes intelligence alliance to better safeguard the cybersecurity of its nationally significant organisations. During a speech to the Aspen Institute Cyber Summit Forum in early November, the Director-General of New Zealand's Government Cyber Security Bureau (GCSB), Andrew Hampton, provided an overview of his agency's CORTEX cyber defence initiative.

CORTEX is a suite of cyber defence capabilities developed by the GCSB that can be deployed at different points on a user's network depending on their network configuration and risk profile.

The services range from providing simple alerts when specific activity is discovered on a network to services that actively disrupt malicious activity.

Hampton said the CORTEX suite is designed to take advantage of the unique capabilities afforded to New Zealand as a member of Five Eyes, the intelligence and surveillance partnership between

> *“An independent assessment commissioned by the bureau found that the value generated by CORTEX in terms of harm prevented is significantly greater than the cost of developing and deploying it.”*

Australia, New Zealand, the UK, the US and Canada.

“We took a range of standard products and combined them with the unique cyber threat insights available to us through our Five Eyes relationships. This allows us to deliver cyber threat detection and disruption capabilities typically not available through commercial providers,” he said.

“We also contribute unique insights to our Five Eyes partners about the malicious activity we are seeing on New Zealand networks.”

When the CORTEX initiative was launched in 2013, the GCSB began the task of convincing public and nationally significant private sector organisations to use the bureau’s cyber defence capabilities.

This was no mean feat, Hampton said, as it was around the time that Edward Snowden’s NSA leaks blew the lid on the existence of numerous global surveillance programs run by Five Eyes. This triggered a vigorous debate about the role of national intelligence agencies and the Five Eyes partnership.

“In spite of this, we received strong support and now a broad reach of New Zealand’s most important organisations receive our CORTEX services,” he said.

An independent assessment commissioned by the bureau found that the value generated by CORTEX in terms of harm prevented is significantly greater than the cost of developing and deploying it. This led to the government’s decision in May to expand one component of the CORTEX system — its Malware Free Networks initiative — to even more nationally significant organisations.

“The concept behind CORTEX is more than just direct cyber threat detection and disruption. If we know activity is targeting a customer’s network, we can make that cyber threat information available to a much wider group — not directly protected by CORTEX capabilities — and enable them to mitigate the threat also,” Hampton added.

Work on CORTEX is ongoing, and the GCSB recently asked 250 users to self-assess their cybersecurity maturity and preparedness to respond to cyber threats.

Hampton said the assessment showed a broad range of maturity and preparedness levels. It uncovered a range of issues including uneven engagement about cybersecurity at a governance level, limited readiness to respond to incidents, insufficient investment in people and skills, and substantial supply chain risk.

“The survey has given us and our customers a solid basis from which to determine where to best focus our ongoing cyber defence efforts,” he said.

The CORTEX initiative has drawn acclaim at local awards ceremonies. In November, CORTEX was named Best Security Project or Initiative at the 2018 Information Security Awards NZ. In July, the project also received the Institute of Public Administration (IPANZ) Excellence Award for Building Trust and Confidence in Government.

Meanwhile, Hampton noted that nearly a third of the cyber incidents investigated by the GCSB contained indicators that could be linked to state sponsored attackers.

“A number of times in the past year the GCSB, on behalf of the New Zealand Government, has joined other like-minded nations in calling out North Korea and Russia in particular for undertaking global campaigns of malicious cyber activity that served no legitimate national security purpose,” he said.

“New Zealand sees this type of activity as unacceptable. It is counter to our vision for an open, safe and secure cyberspace, and we will continue to use public attribution as one of the tools available to deter such threats.”

Complicating matters, as the global threat landscape continues to evolve the line between state and non-state actors is getting blurrier, Hampton said.

As well as its cybersecurity mandate, the GCSB is also responsible for securing New Zealand’s telecommunications networks by working with network operators to identify and mitigate risks to national security.

Hampton said that while the bureau has managed to perform this role effectively to date, the advent of 5G and other emerging communications technologies has the potential to increase the security risk by making it more difficult to isolate potentially vulnerable equipment.

This is reminiscent of the justification used by the Australian Government to ban Chinese vendors including Huawei and ZTE from providing equipment for Australia’s 5G rollouts. When the ban was announced in August, the government asserted that 5G networks will be designed in such a way as to blur the distinction between the core and access components of the mobile network. As a result, the government is concerned that traditional security controls protecting the network core could be circumvented by exploiting equipment in the edge of a network.

But despite the looming challenges, Hampton said the GCSB will continue to work to fulfil its mandate of “[doing] anything necessary or desirable to protect information infrastructures of importance to the New Zealand Government”.

THE SECRET INGREDIENT FOR SMARTER CITIES

NEW CITY INITIATIVES ARE DRIVING A MORE INTEGRATED, SUSTAINABLE AND ARCHITECTED APPROACH TO DIGITAL DEVELOPMENT.

Technology is now part of the underlying fabric of every aspect of local government service delivery, including business systems modernisation, small business policy and the provision of IoT devices, such as smart street lighting. However, coordination between these technology pillars is still typically managed through loose alignments rather than through a concerted effort to bring the strategies together.

It is quite reasonable that early digital transformation initiatives have focused on particular classes of services. Priority has necessarily been given to the enabling tools, technologies and business processes that deliver the quickest return on investment. However, this has sometimes meant that the underlying infrastructure has taken second place and has been relegated to the backroom as important but lower priority work.

Kevin Noonan, Chief Analyst, Practice Leader for Public Sector, Ovum

During Ovum interviews with city senior executives, some have noted with frustration that priority can be more easily given to ‘ribbon-cutting’ projects, such as ‘fix my street’ apps, at the expense of improvements to underlying infrastructure where there are fewer public accolades.

Earlier city initiatives saw the development of data stovepipes, and IoT-enabled smart city initiatives, such as smart lighting and traffic control, were typically treated as the responsibility of city engineers. Digital initiatives, such as billing and citizen engagement, were treated as the responsibility of the CIO or chief digital officer; and economic development initiatives, such as small business development grants and government-funded incubators, were treated as the responsibility of city policymakers.

The next generation of city initiatives is, however, providing a more integrated approach, with architected data management and better policy coordination at its core. There are a growing number of examples of well-coordinated initiatives that are driving a more fundamental approach to integration.

In China, Alibaba Cloud is already into the second generation of its City Brain initiative, with the objective of “empowering cities to think through data-driven governance”. This is an architected approach to data management across all aspects of city management, including:

- the Urban Government Model to provide common facilities that address government administration to make the city more responsive to citizens
- the Urban Service Model to provide efficient urban services and conserve public resources
- the Urban Industrial Development Model to provide publicly available urban data as a catalyst for industrial development.

In Australia, the New South Wales government is addressing a different part of the problem through its Sydney Start-up Hub. This initiative commenced operations in 2017. The small business campus is the third-largest in the world and the largest in the Southern Hemisphere. However, one of its key differentiators is much more subtle: the campus co-locates industry start-ups, established IT companies and offices of the key government department responsible for industry development. This enables a better environment where government decision-makers are in close physical contact with the practical realities of running a small start-up and building a business to drive innovation. Co-location enables government to drive better policy development, including open data initiatives.

The first generation of intelligent city initiatives has now created the crucial momentum for change, and the next generation of city initiatives is now driving a more integrated, sustainable and architected approach to digital development that will support city development into the long term.

FREE

to industry and business professionals

The magazine you are reading is just **one of eleven** published by Westwick-Farrow Media. To receive your **free subscription** (magazine and eNewsletter), visit the link below.

www.WFMedia.com.au/subscribe