govtech review

CRITICAL INFRASTRUCTURE
CYBERSECURITY – IS AUSTRALIA READY?

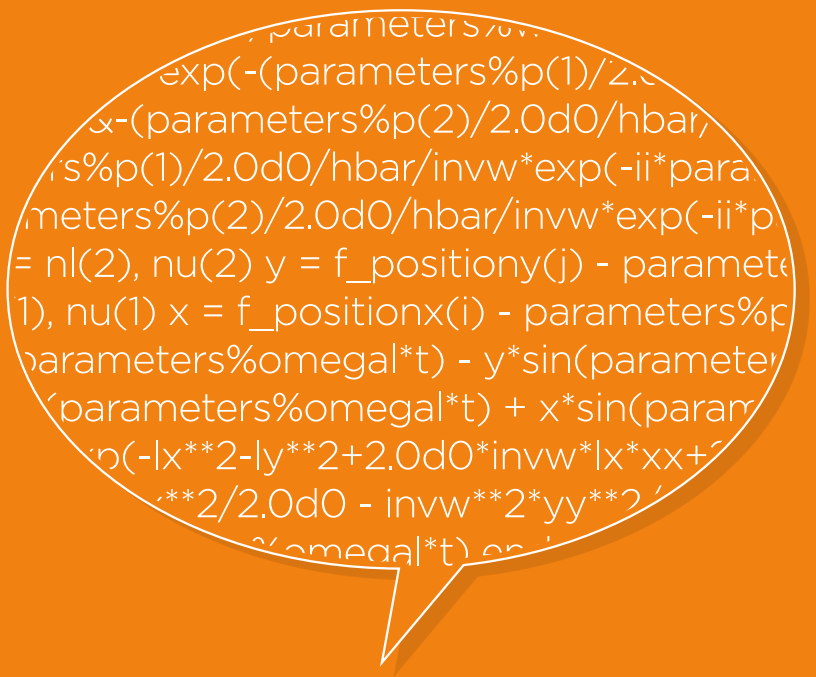
OPERATIONALISED ANALYTICS
FOR FASTER, MORE ACCURATE DECISIONS

GETTING READY
FOR 5G

OPEN SECURITY STANDARDS
AND USER EXPERIENCE

BETTER
CONNECTED HEALTHCARE

Q2 2021
PP100021607



OUR EXPERTS SPEAK HPC SO YOU DON'T HAVE TO.

Some high-performance computing (HPC) providers promise you the world, but leave you high and dry while you attempt to learn a foreign language. At DUG, our reliable, green, cost-effective HPC solutions come with a team of experts. Experts that are fluent in HPC and always on hand to help you optimise your software, onboard your code, and make your project successful. Now that's worth shouting about!

dug

www.dug.com

Q2 2021

INSIDE

FEATURES

cover image: © Stock.Adobe.com/au/Gorodenkoff

Insider

A shared threat

The surge in ransomware attacks across multiple sectors recently prompted the government to launch an awareness campaign. Assistant Minister for Defence Andrew Hastie MP said the government is "tackling cybercriminals head-on" to protect Australian organisations and individuals from cyber compromise.

The Australian Signals Directorate has used, and will continue to use, its broad range of offensive cyber capabilities to disrupt and bring cybercriminal syndicates targeting Australia to their knees, Hastie said. "Offensive cyber is just one of the tools in Australia's toolkit."

The Australian Security Intelligence Organisation (ASIO) received a major funding boost of $1.3 billion to protect Australia and Australians from security threats. Building on Australia's Cyber Security Strategy 2020, the government announced $42.4million to improve critical infrastructure security. Is this enough to protect our critical infrastructure?

In his opinion piece, Secure Code Warrior's Pieter Danhieux says the new government strategy does call out the importance of hardening our critical infrastructure against cyber threat actors, but we need bold statements and bold actions like in the States. The appointment of key members of the Cabinet to cybersecurity and cyber defence would be a huge win for our online safety, as well as support the local cybersecurity industry, and a clear signal that it is a serious consideration as we move forward as a future-focused nation, he argues.

On a different note, Gartner has identified operationalised analytics as a top trend that government CIOs should include in their strategic planning over the next 12–18 months, if they haven't already. For governments to scale and reap the benefits of digital transformation, CIOs must integrate AI and data and analytics capabilities with service delivery and operational processes. All of this while ensuring governance covers data ethics, usage and quality. This makes data and analytics a core business function, which must be connected, continuous and appropriate in the context of its use always.

Another issue that's not going away any time soon is the COVID-19 vaccine rollout. In her piece, Sharryn Napier from New Relic opines that technical challenges and continued outages should be a red flag to government agencies — if the technology is broken, it needs to be replaced. It's also vital that the Australian public is informed through automated alerts, and that the lines of communication are continually open.

Lastly, as you'd have gathered, I have taken over from Jonathan Nally as the Editor of *GovTech Review* and *Technology Decisions*. WF Media and I would like to thank him for all his hard work and commitment. I recognise that I have big shoes to fill, but I'm really looking forward to working with you all and covering this exciting industry.

Mansi Gandhi, Editor
editor@govtechreview.com.au

40 CELEBRATING YEARS
wfmedia
connecting industry

A.B.N. 22 152 305 336
www.wfmedia.com.au
Head Office:
Locked Bag 2226
North Ryde BC NSW 1670
Ph +61 2 9487 2700

EDITOR
Mansi Gandhi
gtr@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Colleen Sam, Veronica King

CIRCULATION
Dianna Alberry
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

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

Technology solutions for connected cities.

Secure efficient management of cities and transport networks.

Asset/Process Monitoring.

- IP video systems
- Thermal imaging cameras
- Incident detection

Intelligent Transport.

- Traffic radar
- Temporary signaling

Secure Industrial Networking.

- Networking infrastructure
- Cybersecurity solutions
- Edge-to-cloud connectivity solutions

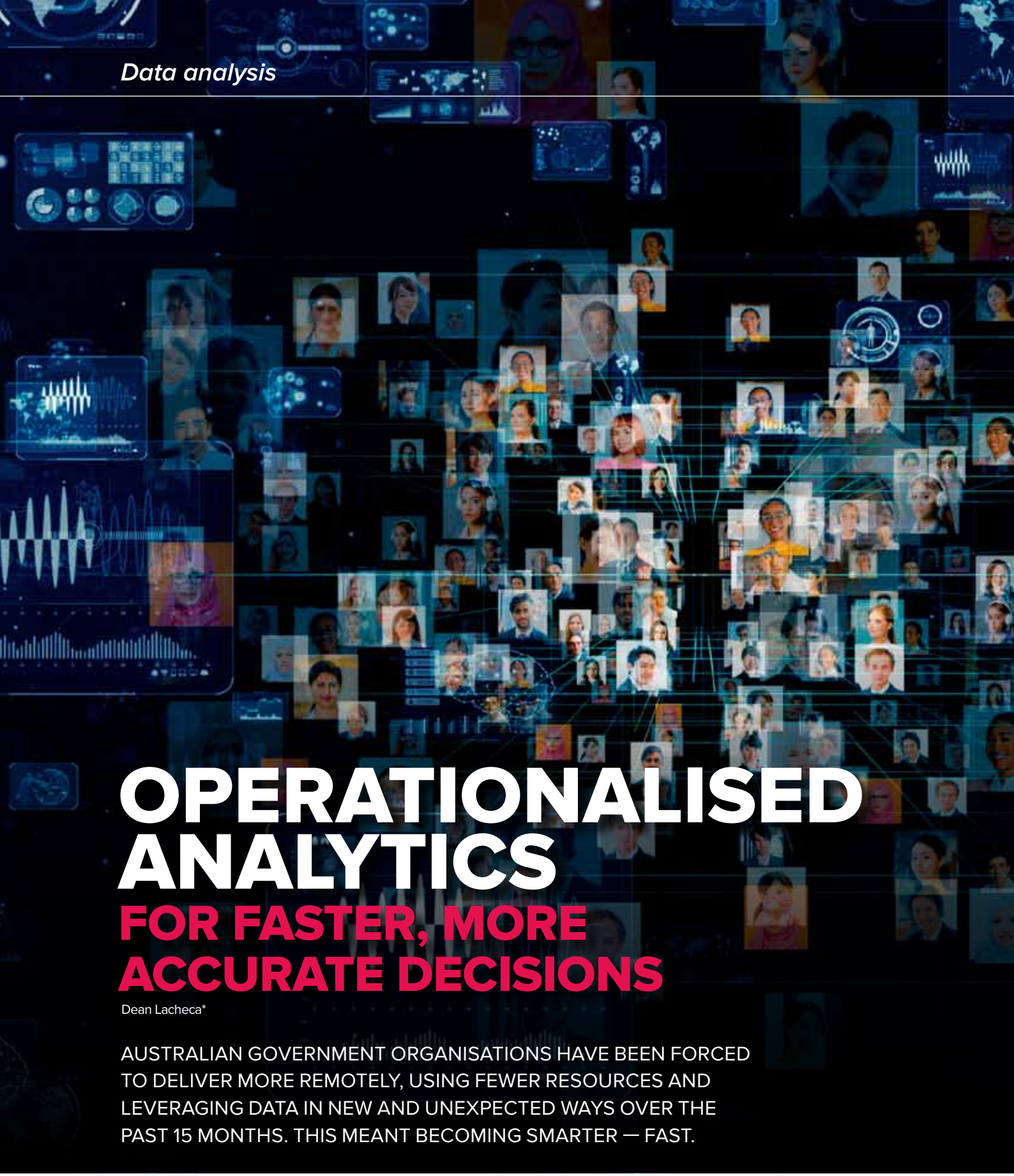
MOBOTIX · Portable Traffic Light · MOXA · RAJANT · CYBERTEC · smartmicro SMART MICROWAVE SENSORS

madison Technologies

Connect with confidence.

Madison Technologies is an Australian owned and operated business that innovates, distributes and supports a range of high-quality products from globally recognised brands. Our team is dedicated to helping partners find practical and reliable solutions for communications and networking challenges, with technical support engineers and stock held locally across our national supply chain.

Sales Enquiries 1800 72 79 79 **www.**madison.tech/smart-cities well connected



OPERATIONALISED ANALYTICS

FOR FASTER, MORE ACCURATE DECISIONS

Dean Lacheca*

AUSTRALIAN GOVERNMENT ORGANISATIONS HAVE BEEN FORCED TO DELIVER MORE REMOTELY, USING FEWER RESOURCES AND LEVERAGING DATA IN NEW AND UNEXPECTED WAYS OVER THE PAST 15 MONTHS. THIS MEANT BECOMING SMARTER — FAST.

Government leaders, particularly CIOs, have been at the forefront of enabling rapid, emergent responses through technology-enabled measures and improved data analytics. The good news is that, while not perfect, some amazing feats were achieved during this time.

For many government organisations, analytics has expanded beyond traditional reporting and policy support functions to include a focus on delivering actionable and timely insights. By exploiting technological advances, they can deliver faster, more accurate decisions at the front line, where significantly greater value is being achieved through embedding analytics in operations.

Service delivery becomes more personalised, responsive and timely across the whole value chain — from sensing to decision-making to action.

The focus of governments on digitally augmenting their workforces has led operationalised analytics to be one of the top trends that Gartner recommends government CIOs should include in their strategic planning over the next 12–18 months if they haven't already.

PREDICTIVE DECISION SUPPORT

Operationalised analytics is the strategic and systematic adoption of data-driven technologies, such as artificial intelligence (AI) and advanced analytics, at each stage of government service delivery or decision-making processes. It represents a shift from the dashboard reporting of lagging indicators to predictive decision support.

Decision-makers — from front line to executives — can make better context-based operational decisions in real time. Proactive business processes are generated that leverage AI and advanced analytics to improve the quality of the citizen experience.

Gartner predicts that by 2024, 60% of government AI and data analytics investments aim to directly impact real-time operational decisions and outcomes.

There are two critical differences between operationalised analytics and traditional analytics. First, operationalised analytics provides information support at the time of decision, embedded within the normal operational workflows. It isn't a separate activity.

Second, timeliness is critical. Information on which a decision is made should be current and contextualised at the time of that decision. For relatively stable information, such as geographic information systems used for address finding in public safety emergency response, the volatility is low and the information only intermittently updated. For volatile, dynamic information, such as personal circumstance or even weather and traffic conditions, current information and contextualised insight are critical.

This contextualised insight moves beyond simply presenting relevant information to predicting likely or possible outcomes based on current circumstances. Operationalised analytics is being used to support decision-making in human and social services, government revenue collection, public safety, law enforcement and intelligence services, and continues to expand.

MEETING NEED FOR BETTER DATA AND ANALYTICS

The need for better data and analytics has been developing for some time. According to Gartner's 2020 CIO survey, 61% of government CIOs said that AI and machine learning (ML) capabilities were either already in place or would be targets of investment within 24 months.

Traditionally, analytics came from a history of reporting to provide management information. Information flowed up from operations and was summarised for management decisions. Management then decided on a response, by reallocating resources or changing policy; this then flowed down into the front line and was operationalised.

This created a long time lag between the collection of information and government response. This was further inhibited by the complexity of metrics and measurement in government — there's no simple alignment with cost, profit and market share as found in commercial organisations.

Measuring success in government is further complicated by the fact that the missions of different government organisations often interact — health with human services, taxation with benefits claims and financial support, road safety with traffic flow optimisation and emissions.

Historically, there were two main blockers: a lack of experience with powerful analytics and an immaturity in the technology that limited the ability to make them usable outside historical analytics/reporting areas. These blockers have been significantly eroded.

At the same time, COVID-19 has forced a realisation of the value of analytics in operations. It demonstrated the ability to share data across the silos of government and the benefits it can deliver. The technologies involved have been available for sufficient time to become usable at a much greater scale by more people. AI/ML techniques are also advanced enough to allow them to be reliably embedded in operations.

Government organisations can now improve the quality, consistency and timeliness of their services and decision-making. The focus of service delivery can shift from reactive to proactive. Knowledge workers can also be freed up by reducing the effort spent doing repetitive administrative tasks or collecting data available by other means.

These developments started accelerating before the pandemic, but addressed more demanding citizenry requiring services from agencies with constrained budgets. This was driving AI-based automation (eg, intelligent process automation) and risk-based case assessment based on advanced analytics.

Government leaders will continue to deal with challenges associated with oversight, control, accountability and the ability to explain the basis of decisions. Operationalised analytics allows people to remain central to the process and benefit substantially from additional tools and insights.

ANALYTICS, A CORE BUSINESS FUNCTION

For governments to scale and reap the benefits of digital transformation, CIOs must integrate AI and data and analytics capabilities with service delivery and operational processes. All of this while ensuring governance covers data ethics, usage and quality. This makes data and analytics a core business function, which must be connected, continuous and appropriate in the context of its use at all times.

Data generated by citizen-facing applications, ecosystem partners, the Internet of Things (IoT) and back-office systems requires a flexible analytics architecture that supports real-time analysis and AI-based decision support.

The classic output from many analytics initiatives — the executive/public performance dashboard — will still exist, but will also evolve in response to these new insights.

Government organisations must execute an analytics everywhere strategy that steadily advances the impact and expands the use of real-time analytics capabilities.

HOW TO TAKE ACTION

Start by developing a compelling future-state vision of the business value and public benefit of operationalised analytics. This can be achieved by building a concise data and analytics strategy aligned with desired business outcomes. Sustain this with adaptive governance practices.

Demonstrate the effectiveness and efficiency opportunities of operationalised analytics by conducting pilot projects that have immediate impacts on productivity or morale, amplifying human talents and reducing errors. Common examples include contact centre services or tasks, field services support or even corporate services tasks, such as HR, payroll or finance.

Finally, build a roadmap for capability development by assessing AI and analytics capabilities within your organisation and across your government. Plan to close gaps by contracting with suitable service providers or academic institutions and leveraging cloud-based AI and analytics services.

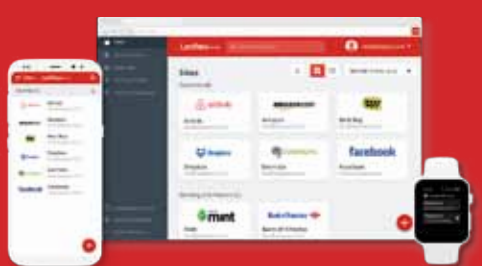
Dean Lacheca is a senior director analyst at Gartner, supporting public sector CIOs and technology leaders on their transition to digital government. Lacheca covers topics including digital strategy, digital workplace, open data, government case management and citizen engagement. His research also includes the adoption and potential impact of emerging technology trends, such as artificial intelligence, on government.

LastPass •••|
by LogMeIn

Protect and empower the digital identities of your modern workforce.

From single sign-on and password management to adaptive multifactor authentication, LastPass is the comprehensive access platform for securing every entry point to your business.

www.lastpass.com



03.09.2020/PDF/LMI1309

© Stock.Adobe.com/au/Chalabala

Aussie X-ray tech to transform US airport security

Australian company Micro-X will establish its US headquarters at SeaTac, Washington State, as it expands its capabilities to better support its growing business. The proximity to the airport for Micro-X's future airline passenger self-screening development, the high level of software talent in the greater Seattle region and the room in South King County for the company's expansion plans all contributed to SeaTac being chosen as the location for Micro-X's headquarters.

Using its patented carbon nanotube X-ray cold emitter technology, Micro-X has invented Rover, a mobile X-ray machine that is lightweight and ruggedised for high-intensity use in field hospitals and remote locations. The technology could also transform airport security across Australia, enabling faster X-ray baggage screening, thereby reimagining airport checkpoints.

Brian Gonzales, CEO of Micro-X's US operations, predicts that the SeaTac facility will be a centre of excellence for imaging product development, revolutionising medical, defence and security X-ray imaging.

"Our mobile X-ray machines are available now for use in public and military hospitals. They're lighter, cheaper, more robust and more precise than our competitors. In Australia we're developing a CT brain scanner, so small and so light that it will integrate into any ambulance, allowing brain scans at the point of care," said Gonzales.

Gonzales added that the team at SeaTac will work on proprietary imaging software and algorithms as part of this project. The company will also work with the US Government to develop a self-service booth that provides a 3D image of carry-on luggage together with a body scanner and passport reader.

The invention that enables these ideas is inside Micro-X's X-ray tube, which replaces conventional X-ray tubes that use a hot filament, like an old-fashioned light bulb, to generate the electron stream needed to make X-rays. Micro-X's technology applies voltage to an emitter made from carbon nanotubes (CNT) to generate the stream of electrons instead. It is smaller, more energy efficient and longer lasting, like LED lights.

Funding for Qld firm supplying software to NASA

Gold Coast-based Opmantek, which is supplying software to NASA for use in its Artemis mission, is one of the 44 companies that have received a funding boost from the Queensland Government.

The funding is part of the second round of Trade and Investment Queensland's (TIQ) grant program, which supports Queensland exporters to finalise new export deals in their target markets. Premier and Minister for Trade Annastacia Palaszczuk said the companies will share in total funding of nearly $930,000.

CEO Danny Maher said Opmantek's is the only monitoring software the US space agency is using for its Artemis program, which it hopes will see the next humans land on the moon in 2024, including the first woman. The funding will help the company make modifications to the software for NASA's purposes and train their engineers.

Opmantek, a five-time Queensland Exporter of the Year and two-time Australian Exporter of the Year, was founded in 2011 and is already exporting its open-source software to 130,000 companies in 178 countries.

"We think of ourselves as modern-day explorers — we hope we're breaking down barriers in some markets and making it easier for Australian companies to do business in those markets, just as those before us have broken down barriers and helped us.

"I'm sure most tech companies in the world would love to be involved with a space mission, and this grant helped us take that step and make it commercially possible," Maher said.

©stock.adobe.com/au/Prostock-studio

acer

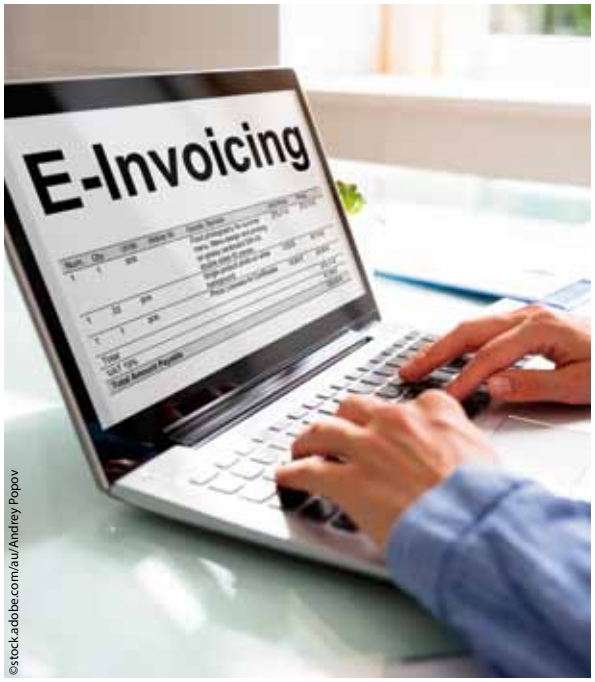
Intel® Core™ Processors

TravelMate Spin P4

NEW 2-in-1 Premium Business Laptop for Professionals

A smart and sleek business-grade device that offers 360-degree rotation versatility to meet any working environment.

- Weight Starts at 1.5kg, 18mm Thick
- MIL-STD 810G Compliant
- Durable Hinge
- Multi-touch Panel
- Acer Active Stylus
- Up to 1TB NVMe PCIe Gen3 x 4 Lane SSD
- eSIM-enabled 4G LTE and NFC (optional)
- Up to 14-Hours Battery Life



Mandatory e-invoicing for NSW agencies from 2022

E-invoicing will be mandatory for all NSW government agencies from 1 January 2022. The mandate will apply to the delivery of goods and services up to the value of $1 million.

The mandate will help reduce payment times, paperwork and manual errors, and save buyers and suppliers a significant amount of money, said NSW Minister for Digital and Minister for Customer Service Victor Dominello.

"There is an estimated shared saving of around $20 each time e-invoicing replaces a paper invoice and around $17 each time it replaces a PDF invoice," Dominello said.

"Based on the 4.2 million invoices across NSW Government in 2019, a shared saving between the suppliers and NSW Government is estimated to be $71 million."

Funding was allocated through the Digital Restart Fund to set up an e-invoicing service.

Research suggests that e-invoicing rates in Australia range from 15% for small businesses to 23% for large businesses, compared to 28% across Europe and 40% in Denmark and Finland.

NSW Minister for Finance and Small Business Damien Tudehope said, "This mandate will enhance the government's existing Faster Payment Terms Policy, by ensuring that the accounts payable teams in government agencies receive invoices within minutes, enabling payment to eligible small businesses within five business days."

Suppliers will have the option to use e-invoicing or continue to invoice government agencies through existing means.

5G IA appoints new governing board, broadens membership

The new board for 5G Infrastructure Association (5G IA) has elected its new governing board for two years. The 16 organisations represented in the governing board of the 5G IA are elected among the 5G IA's 'Full Industry Members'.

The represented organisations include Ericsson, Huawei, Netaş, Nokia, Orange, RHEA Group, Samsung, Telenor, Thales, TIM, Alliance for Internet of Things Innovation (AIOIT), Public Safety Communications Europe (PSCE), the Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), TNO, Eurescom and Nextworks.

The newly elected governing board appointed Dr Colin Willcock, Head of Radio Network Standardization at Nokia, as Chairman of the governing board. Dr Huge Tullberg, Principal Researcher at Ericsson, was appointed as Vice-Chairman of the governing board.

The 5G IA represents the European industry for the development, deployment and evolution of 5G. At the same time, the 5G IA is preparing for advancements in mobile communications with the new 'Smart Networks and Services' (SNS) Partnership in the framework of the Horizon Europe Programme.

Within the SNS, the 5G IA will serve as private side representative, jointly managing the Partnership with the EU. The SNS Partnership aims to support European technological sovereignty on Smart Networks and Services. It will contribute to enable the digital and green transitions and will allow European players to develop the technology capacities for 6G systems as the basis for future digital services towards 2030.

The 5G IA continues to expand its membership and is open to ICT associations, to make it fit and ready for the SNS Partnership and its extended scope.

HD4 MBX

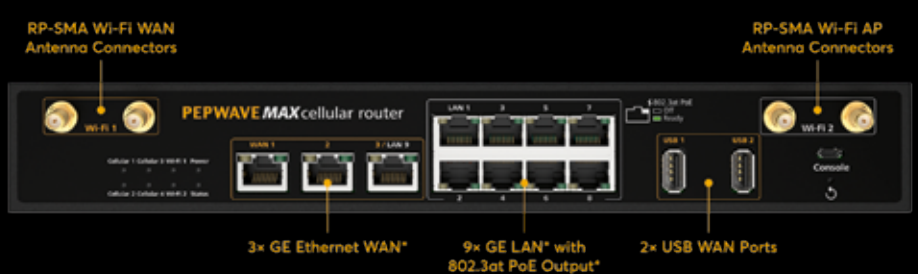
Ideal for On-The-Go Deployments

Quad Cellular Gigabit LTE Mobile Powerhouse

The HD4 MBX is capable of combining the bandwidth of up to 4 cellular links into an unbreakable, high-speed SD-WAN connection. The HD4 MBX supports up to 8 SIM cards,with room for another 8 with the optional SIM Injector. With up to 16 cellular providers to connect to, spotty coverage will simply not be a problem.

Ready for any environment

peplink



WirelessTech

+61 2 8741 5080
sales@wirelesstech.com.au
www.wirelesstech.com.au

GETTING READY FOR 5G

Dick Bussiere, Technical Director, APAC at Tenable

The Australian Government recently auctioned off Australia's fastest 5G spectrum as demand for faster and denser internet connectivity continues to grow from consumers and businesses alike. If last year was any indication, we need to enable quick, seamless connections to live, work and play in this highly digitised world.

Asia Pacific is predicted to become the leading region in terms of 5G adoption, accounting for 65% of global 5G use by 2024. The power of 5G undoubtedly changes the playing field for both the private and public sectors, with boundless opportunities for greater interconnectivity between intelligent devices. This connectivity increases the value of the network to society in general, as the criticality of any network is proportional to the number of devices connected to it. Examples include highly interactive traffic control systems, smart power grids, smart cities and, of course, autonomous vehicles of all types. The possibilities are endless.

Unfortunately, as we become more dependent on this intricately


© Stock.Adobe.com/au/ringaipunni

connected infrastructure, the risk of disruption also increases as more intelligent and interoperable devices are online. The unfortunate side effect of greatly expanded connectivity is an expanded attack surface providing a greater temptation to malicious actors.

History has shown us time and time again that as new technologies emerge, cybercriminals won't be far behind, testing the new technologies for their resilience to cyber attacks. With today's highly interconnected organisations, no sector of the economy is without some inherent risk, whether that is the result of a natural disaster or a malicious automated attack. We only have to look at the cyber attack against Colonial Pipeline to understand the extent of the impact on the wider public.

As private and public organisations prepare to fully embrace the opportunities of 5G, it's important they do so in a way that avoids the risks that arise with it. Below are five steps to a secure 5G implementation.

Build people into your policies — In order to embrace the benefits of 5G and minimise the associated risks, we need to ensure that robust policies are in place to protect OT. This involves people and processes first, then technical solutions. It's critical that we're taking people in all areas of an organisation on the journey, ensuring that the risks of deploying 5G devices are considered.

Develop industry-wide collaboration — 5G security policies must include sharing of threat data, security methodologies and interoperability within the wider community. It's only through this communication and collaboration that we can adequately manage risks and take full advantage of the benefits of 5G.

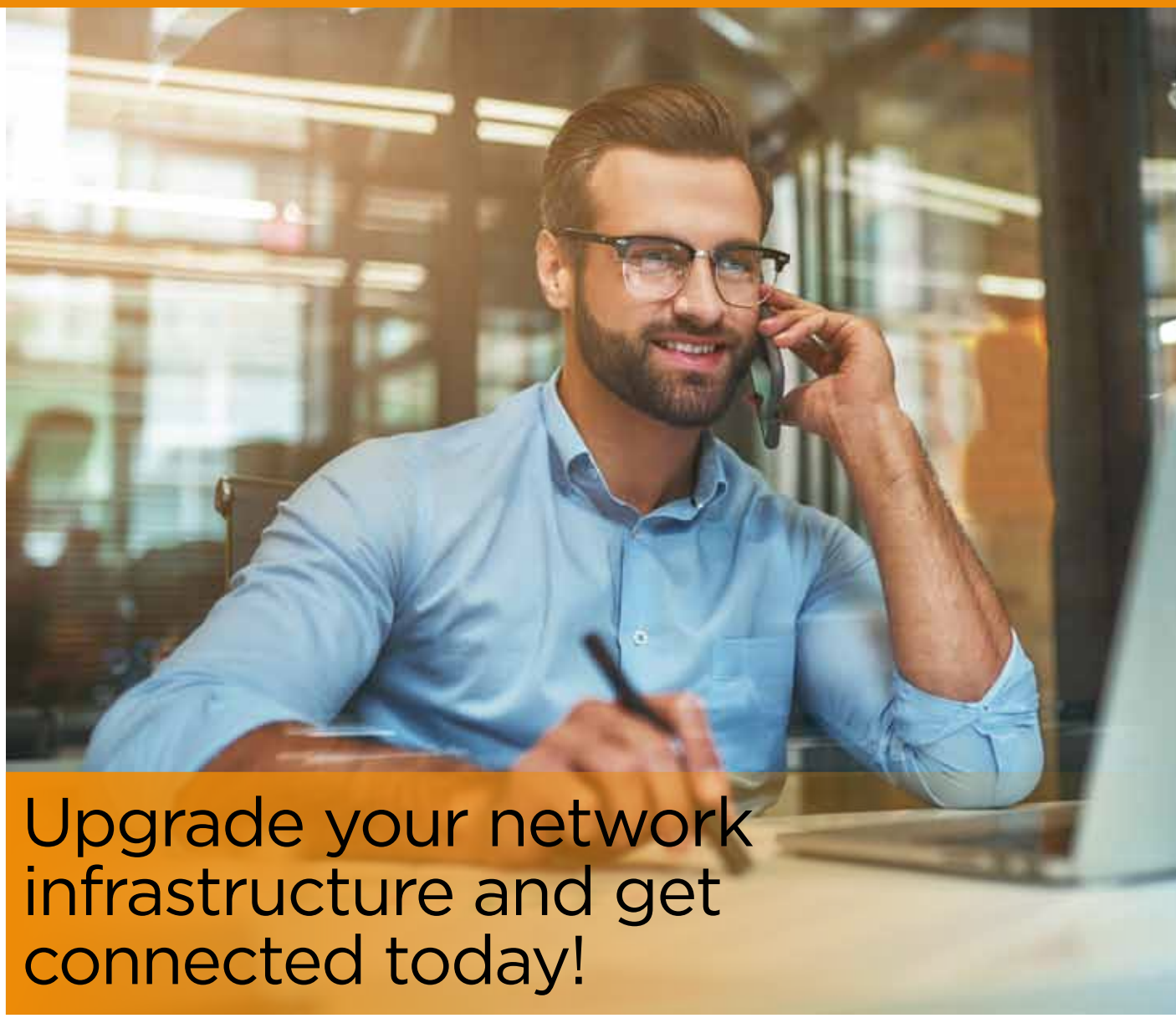
Share the responsibility — Cybersecurity is a shared responsibility, neither governments nor organisations can address it alone. The private sector owns and operates most networks as well as elements of critical infrastructure. Those owners and operators must be viewed as essential partners in ensuring the protection of this critical infrastructure, especially if 5G is being incorporated. In this shared risk model, the network owners/operators do the utmost to ensure that the infrastructure is as secure and available as it can be. At the same time, the users (public sector) of the infrastructure assume responsibility for the security of their applications. The public sector, as a user of the infrastructure, should build and maintain strong partnerships with the private sector and actively participate in the overall security and availability of the shared network resources.

Close the exposure gap — As data continuously flows through potentially vulnerable 5G infrastructure, a gap will exist between the visibility we have and the true scale of vulnerabilities across the entire attack surface. In order to combat this, it's key that owners and users of the 5G infrastructure work together to close the gap and combat new and emerging threats.

Prioritise based on risk — An effective 5G security program should be prioritised based on risk. This prioritisation saves both time and resources by focusing on critical vulnerabilities existing on critical assets. Risk-based vulnerability management allows us to focus on what is important to maintain availability and allows lower priority issues to be dealt with later.

EMBRACE THE CHANGE, BUT MINIMISE THE RISK

Once 5G is widely available, the floodgates will open, and both the white hats and black hats of the world will experience a swift learning curve in navigating the wonders of 5G. The profound speed and reach will connect businesses more than ever before, which will lead to greater efficiency, but also translates to dangerous ripple effects of a successful attack. As we begin to adopt 5G more widely, it's important that we are taking security into account and ensuring that our organisations and people are protected in doing so.



Upgrade your network infrastructure and get connected today!

As Australians return to work and back to the office, secure and reliable connectivity solutions have become more important than ever before. The new normal requires the flexibility to operate remotely.

The Australian Government is rolling out a variety of new connectivity solutions for its citizens and Powertec Wireless Technology stands firmly behind these government initiatives, such as the Regional Connectivity Program and the On-Farm Internet of Things (IoT) Trial. These programs aim to support Australian farmers to become digitally enabled and to improve the productivity, competitiveness, and sustainability of the agriculture sector.

Powertec's Agribusiness Sensors

Powertec monitors and sensors allow you to receive real-time data updates directly to your phone, tablet, or computer — no matter where you are. All this information is displayed on an interactive and easy-to-use online dashboard allowing you to make informed decisions.

All Powertec sensors come as a complete package, ready to be installed and include the sensor, a Powertec CM10, solar power source, antenna, cabling, and mounting accessories.

1. Ultrasonic Level Sensor: Build a clear picture of your entire storage in silos, vats, and tanks. Ultrasonic level monitors use an ultrasonic wave to record the distance to a surface. Also, suitable to measure water levels, tide conditions, snow depth, creek heights and water trough levels.
2. Hydrostatic Level Sensor: Accurate consumption monitoring will simplify

how you manage liquid levels and new stock purchases. Measure fuel tanks, water tanks, dam levels, chemicals, wine vats, borehole level, reservoir level monitoring, snow depth, tide conditions, creek heights and water trough levels.

3. Local Weather Stations: Gain insights into weather conditions on your property, including temperature and humidity. Micro-weather stations are especially beneficial for large farming properties, which often experience different weather conditions across a wide geographical area.
4. Soil Probes: Understanding soil characteristics can provide unparalleled insight into soil changes, allowing you to develop precision cropping and harvesting techniques. Soil probes will enable you to measure the salinity, moisture, and temperature of your soil at various depths.
5. Advanced Tracking solution gives you enhanced visibility of your high value assets giving you full visibility into the location, activities, and condition of your critical equipment so you can better utilize your powered asset.

A better-connected community ensures communications are more efficient. It is time to take extra steps to ensure all Australians can be connected to the Internet.

Powertec has over 140,000 installations in Australia and New Zealand, including large companies, government departments, small to medium-sized businesses, farms, aged-care facilities, hospitals, and individual consumers. Below is a case study by Powertec which details the capabilities of their cellular signal booster, Cel-Fi GO.

Eliminate call dropouts and dead zones with the next generation Cel-Fi GO4!

Does your office receive little to no signal? It is essential for government employees working within multi-storey buildings, especially in below-ground levels, to receive mobile signal. To ensure adequate signal levels are dispersed throughout a building, Powertec Wireless Technology provide a range of cellular boosting solutions.

Product Profile

Cel-Fi GO4 represents the latest in 4G cellular repeater technology. Building on the success of the GO2 model, the GO4 has a higher output power (+20 dBm), providing the largest coverage area of all GO models. Up to 3000 m^2 coverage area.

GO4 operates on more frequency bands, now supporting Optus 700 MHz and 2300 MHz 4G networks and can be easily switched between Optus and Vodafone-TPG should you change service provider.

Cel-Fi GO4 is ideal for large inbuilding cellular coverage applications for Optus and Vodafone. The higher output power means more service antennas can be run from the one repeater expanding the coverage area, and by popular request, the unit now has an RJ45 Ethernet network interface for remote management.

Expanding on GO2's dual-band functionality, GO4 supports carrier aggregation with 40 MHz of relay bandwidth.

This business and residential solution is ideal for use in warehouses, hospitals, corporate office buildings, universities, government offices and much more!

Features

- 700L/850/900/1800/2100/2300/2600 MHz (700 band not supported on Vodafone)
- 3G, 4G, VoLTE, NB-IoT (GO4 has 5G capabilities, but currently not enabled or approved)
- Carrier Switching using WAVE App between Optus or Vodafone — Telstra approval pending
- Up to 3000 m^2 coverage area
- Two band simultaneous relay
- Total System Relay Bandwidth — Up to 40 MHz
- Remote Monitoring, Control and Alert Capabilities via WAVE Portal
- Ethernet Port for connection to internet source for live monitoring

Business Benefits

The Cel-Fi GO4 installation has provided this government building with a strong and reliable cellular mobile signal in all areas of the building.

Cel-Fi GO4 is available now, stay up to date with Powertec's latest products, visit www.powertec.com.au or contact the Powertec team today on 1300 769 378.

powertec
WIRELESS TECHNOLOGY

Powertec Telecommunications Pty Ltd
www.powertec.com.au

PROTECTING **CRITICAL INFRASTRUCTURE**

IS THE AUSTRALIAN GOVERNMENT EQUIPPED TO FIGHT CYBER ATTACKS?

© Stock.Adobe.com/au/Egor

In the past year, a number of Australian organisations, from Lion Beverage Company, Toll Transport and Nine Entertainment, have been impacted by cyber attacks. More concerning, in recent months Australia's government and institutions have been targeted by ongoing sophisticated state-based cyber attacks. Some of the attacks have been on local government departments, hospitals and state-owned utilities — all of which hold sensitive economic and personal data. The increasing number of attacks has, for the first time, seen the Australian Government enter the top five industry sectors to notify data breaches.

In response to the spike in continued large-scale cyber attacks, the Australian Government recently released the Australian Cyber Security Strategy 2020. The strategy highlights new initiatives and a $1.67bn funding boost to be used over the next decade, to achieve their "vision of creating a more secure online world for Australians, their businesses and the essential services upon which we all depend".

Australia is not alone and governments around the world have stepped in to reshape and update their cybersecurity plans and infrastructure, including strategies and regulations that businesses are required to follow when handling our most precious digital resources. However, as we move through digital advancement at a cracking pace, it has become difficult for many to keep up with the number of threats, possible attack vectors and compliance requirements that are part of an ever-changing landscape.

Much of our daily life is powered by software, even if it's not highly visible. This month a cyber attack forced the temporary shutdown of one of the US's largest pipelines, highlighting already heightened concerns over vulnerabilities in the nation's critical infrastructure. The attack comes amid rising concerns over the cybersecurity vulnerabilities in the States' critical infrastructure and after the Biden administration launched an effort to beef up cybersecurity in the nation's power grid, with a call to install technologies that can thwart attacks on electricity supply.

Closer to home, healthcare provider UnitingCare Queensland recently experienced a cyber attack. The attack impacted all

operational systems including internal staff email and patient operation booking, forcing staff to revert to paper-based operations for the foreseeable future. However, it turns out the hackers behind the attack were identified as the same group responsible for past attacks against major targets including Apple and Donald Trump. The new government strategy does call out the importance of hardening our critical infrastructure against cyber threat actors.

However, what's next? We need bold statements and bold actions like in the States. To prevent costly and damaging cyber attacks, such as the recent Service NSW data breach or NSW Labor Party ransom, it's important to assess and validate the suppliers we use and the software these suppliers write for the Australian Government and for businesses across Australia.

It is clear from the Australian Government's push to get serious about cybersecurity that it has been identified as a key risk area on a national level, but is their strategy reaching far enough? Here's where we could be doing more:

CABINET ROLE

Countering cyber attacks, disrupting active cybercriminals and ensuring their prosecution, as well as intelligence sharing with international allies are all important factors, but imagine if the nation-wide standard for protection was focused on prevention. What we need is something similar to Biden's recent multi-billion-dollar cybersecurity support plan, as well as the appointment of key members of the cabinet to cybersecurity and cyber defence. It would be a huge win for our online safety, as well as support the local cybersecurity industry, and a clear signal that it is a serious consideration as we move forward as a future-focused nation.

Therefore, it is troubling that we still don't have a dedicated cabinet role for cybersecurity in Australia and as such, even with funding, it is easy to be 'out of sight, out of mind'. In the wake of nation-state cyber attacks and unprecedented access to our sensitive information if a data breach is successful, this lax approach that maintains a status quo has been ineffective to date.

Like any other malicious attack that has the ability to disrupt our way of life, resilience is absolutely crucial — not just to withstand such an attempt, but to act as a deterrent to it happening at all. At the end of the day, even threat actors can be lazy, and they will move to an easier target to achieve their goal if too many barriers are put in the way of their success.

The job is too big to be tacked on to a multi-service cabinet role, and appointing a person with an innate understanding of the impact of meticulous cyber defence would be ideal as we produce software at cracking pace in every industry.

CYBER SKILLS

At the moment, we face a global cybersecurity skills shortage, and this is something that keeps CISOs around the world awake at night. From July to December 2020, 38% of all data breaches were caused by human error — namely security misconfigurations — which are usually relatively simple, code-level fixes. If training is made a priority, in conjunction with building company-wide security awareness, there might just be fewer CISOs signing off on breach notifications to thousands of compromised customers.

In a refreshing change, there is an in-depth plan to address the cybersecurity skills shortage over the next decade, by way of emphasis on cybersecurity training from primary and secondary school, through to tertiary education. This foundational learning is sorely needed if we are to build the security superstars of the future, but from a perspective of addressing business needs right now, hands-on training in secure coding for the development cohort is an absolute necessity to start reducing common vulnerabilities, and must be part of a functional security program.

The NSW Government has announced, as part of its 2021 Cyber Security Strategy, to clarify minimum cybersecurity requirements in government procurement processes and aim to enhance the capability of the state's central cyber office, ensuring it can provide support to smaller agencies and local council.

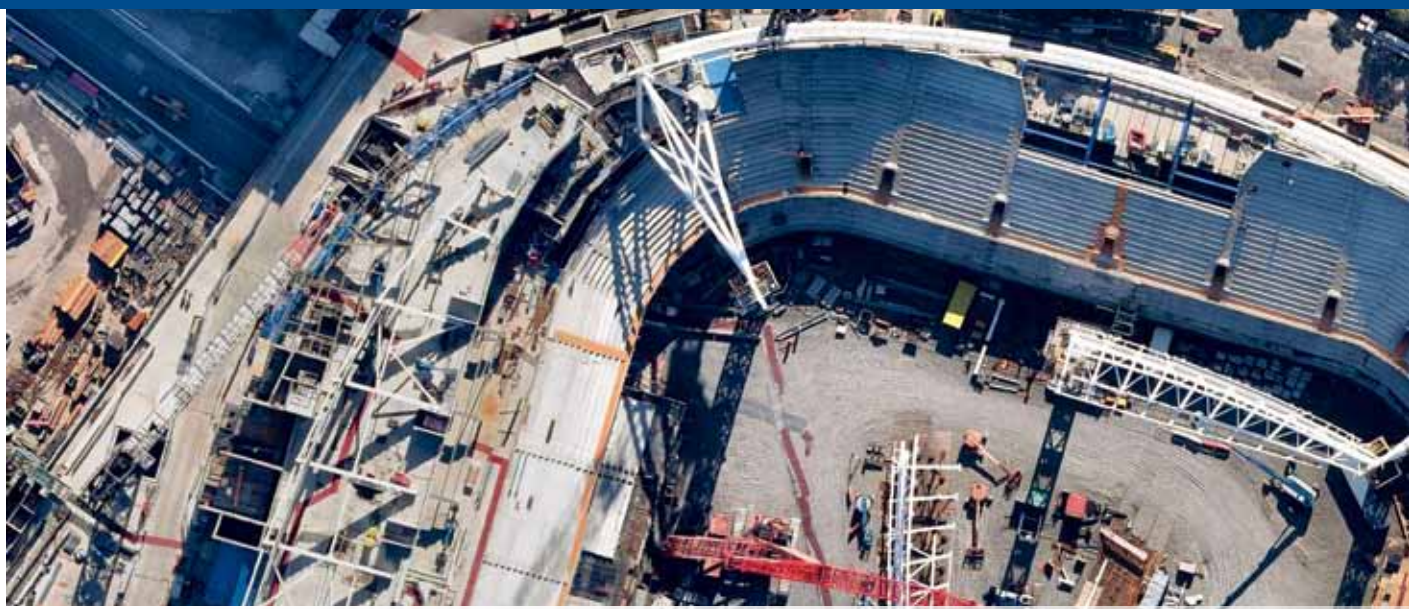
What's more, the NSW Government will establish a 'Cyber Hub' to grow the cybersecurity industry and talent pool within the state and build a workforce capable of operating with fluidity. It's a step in the right direction, but more needs to be done at both the state and federal levels to support Australian cybersecurity start-ups succeeding at a global level. Access to seed funding and even CISOs who are willing to try solutions new to the market and help them mature is an excellent starting point.

For the industry itself, the key thing here is to focus on the root cause of the problem and to focus on how can we prevent cyber attacks happening in the future — that's mainly around creating skilled people who can respond to these types of attacks, but also making sure that mistakes in software development don't happen in the first place.

There is an enormous opportunity here for our government to create a national security skills baseline certification, or regulation, and the Australian Cyber Security Strategy alludes to this as a way to work with finite resources. For now, our beacon of hope lies in the development teams within each organisation, and given the tools and knowledge to succeed, they can cut off common vulnerabilities at the pass and significantly reduce the risk of a data breach within their organisation.

Efforts to create strong policy frameworks, build better and advance Australia's infrastructure is a foundational step that we must take to confront cyber threats that could compromise our most critical systems that are essential to our national prosperity and economic security.

Pieter Danhieux, Co-Founder and CEO of Secure Code Warrior.



Transforming government workflows

Embrace digitisation with current, contextual aerial maps

Local, state and federal infrastructures are being scrutinised like never before in an attempt to keep our nation safe. Government departments are having to evolve what they do and how they do it at an accelerated pace in light of our present-day challenges.

More government departments than ever are using aerial data to achieve a level of insight and intelligence they simply cannot get from ground level. Assessment, utilities, AEC, transportation, public works, public safety — every sector is becoming more reliant on technology to get the job done. GIS in disaster management is expected to hit a global market size of $9.4 billion by 2030*, and government teams across the world are investing in GIS solutions for national security, aerospace, and military applications.

So, how do advances in geospatial technology support digital transformation in the government sector? Nearmap looked at the challenges its customers experience, and dug into what that means to those in the industry.

Challenge #1: Budgets and procurement

Budgets are complicated. Procurement even more so. Government teams are responsible for assets, tools, and systems that are shared with cross-functional teams, and their outputs are usually on behalf of others. This makes for convoluted procurement processes, which can prevent government teams from moving forward with much-needed technologies.

Aerial imagery is essential to government departments. When the truth on the ground forms the foundations of the future, fidelity is not just important: it's essential. Many planning teams need multiple flyovers a year simply to remain up-to-date with development changes. However, most simply don't have the budget to procure one-off flyovers. In the face of procurement challenges, they have to make do with outdated flyovers supplemented with low-resolution satellite imagery instead of the up-to-date high-resolution location data they need.

Poor quality aerials aren't clear enough to make out any detail, and what use are they anyway if the content is incorrect? And if there is budget to procure more current imagery, many departments lack resources to combine the content, digitise it, and update the database.

Nearmap offers a 7.5cm ground sampling distance (GSD) per pixel, so users can literally see when lane markings fade or road conditions change. Nearmap covers 90% of Australia's population, and the data is captured up to six times per year. Nearmap AI (Artificial Intelligence) takes away the hassle of database updates and digitised assets.

Lindsay Mason, Head of the Land Information Team, City of Ryde said, "Nearmap AI has been a key tool for us as we plan for the future wellbeing of our community. We've been able to utilise location data and derived insights to observe trends in order to design smarter green spaces."

Challenge #2: Data accuracy

Government professionals deal with vast quantities of geospatial data — especially

when analysing everything from emergency routes to stormwater runoff. But data is only useful when it's good data: sufficient, accurate, timely, current, and — ideally — comparable. Inaccurate data costs time, resources, and money — three things most teams are in short supply of. Nearmap flies multiple times per year; so you see how much changes in just a few months and the variability between seasons. Adopting technologies that digitally transform data collection allows users to deliver accurate, agile, and informed projects, developments, and analysis.

Nearmap allows users to detect changes more often, in just a couple of clicks, with instant access to our catalogue of current and historical imagery, georeferenced to show truth over time. When the company captures a new area, users receive that data within days.

Peter Bartley, Development Compliance Officer, City of Ipswich said, "Nearmap helps us through most of the compliance process. We don't need to leave our office to gather data for investigations."

Challenge #3: Improving internal communications

Data analysts are at the pulse of every government organisation, deriving data and insights, and creating web applications for these departments. Every piece of data these teams generate, every insight they glean, and every report they publish tells a story that enables someone in another department to perform more effectively. Aerial imagery plays a significant role in this storytelling for many sectors. The tight alignment between the two means that those in government sectors — small, local teams to national agencies — use Nearmap imagery to create detailed base layer maps that integrate directly into their GIS, CAD, and open-source mapping platforms. They then use this content to: create data-enriched maps and apps; provide contextual imagery to support budget, planning, and development proposals; streamline communication and workflow between departments; detect changes and verify permit compliance; and monitor project workflow.

Digital transformation looks like shared, cloud-based internal platforms and processes that make effortless data exchange the new norm. It creates impactful proposal visuals and consistent communication.

Challenge #4: Public communication

The most important stakeholder in government is the general public. Residents want to know what's happening in their communities surrounding publicly funded government initiatives.

Citizens want to know about government plans to tackle zoning or areas of new development; about emergency routes and road closures; updates to land use and land classification; and information on construction delays and events.

However, the way this information is collated would often be unintelligible and, frankly, dull to the average person. The raw data analysts work with isn't appropriate. How you present your story is as important as the story itself if you want people to understand and be interested in what you have to say.

With content that is current and relevant, keep your residents informed about ongoing change with data that's user-friendly.

Load up proposals with the most detailed imagery and ensure those across cities, states or suburbs can stay in the know about upcoming change. Promote a sense of community involvement and build with all community members in mind.

Looking to the future

The government sector has come a long way in adopting new processes and technologies, but it remains a slow journey. Artificial intelligence (AI), a mobilised workforce, Internet of Things (IoT) and cloud computing are some of the key trends driving digital transformation in government. The need for change, however, is accelerating and digital transformation is a necessity, not a luxury. So what's driving that need?

- Governments achieve more success addressing societal needs when they embrace partnerships with third-party technology providers
- Government teams are becoming smarter with how they collect and use data, but risk limitations unless they become more digitised
- Rapid urbanisation, increasing populations, and aging populations have forced governments to look to more intuitive, data-driven solutions
- Connected citizens expect the governments that serve them to be connected too. Many government departments still rely on legacy systems and archaic, manual processes

Moving away from slow archaic processes to technology such as Nearmap can breathe new life into how local, state and federal planners go about the business of creating smart cities, balancing nature with new construction and making decisions grounded in the richest of data.

Nearmap Pty Ltd
www.nearmap.com.au

OPEN SECURITY STANDARDS AND USER EXPERIENCE

Alex Wilson*

Starting first with the broad adoption of the FIDO Universal Second Factor (U2F) standard, followed by FIDO2, and now Web Authentication (WebAuthn), these open security standards bring together new and important security capabilities for authentication, while reducing cost for the modern web. What impact do the open security standards have on the user experience and why should we even care about them?

STANDARDS AND SECURITY

Open standards establish protocols and building blocks that can help make applications more functional and interoperable so that every user has a consistent experience across the board. Take the seatbelt, for example. The three-point seatbelt was invented by Volvo, but Volvo contributed it as a standard so that any auto manufacturer could also adopt and use this same technology. Today, we have three-point seat belts in every single car and they all work the exact same way so as users, we know what to expect and how to operate them.

The same concept of the seatbelt applies in many other industries as well. For example, the reason you can read emails is because of a standard that was originally called USASCII that defined which bit patterns made which characters. The reason that we can communicate via mobile phones is because of the GSMA cellular standard. The list goes on, but internet security is no exception.

The humble password is a decade-old example of an open standard that is used widely across the internet that was initially supposed to fix authentication but did not provide adequate security. New open standards are needed because passwords have become a source of significant problems. Users continue to choose weak or simple-to-guess passwords and reuse the same passwords on multiple services.

The real key is that open standards are implemented reliably and consistently to create efficient and trusted conditions through economies of scale that make it


© Stock.Adobe.com/au/Song_about_summer

possible to implement secure systems. Without open standards, security evaporates.

WHAT ABOUT WEBAUTHN?

In early 2019, Web Authentication, or WebAuthn, became an official World Wide Web Consortium (W3C) standard. The specification allows any service, including banks, email providers or online gaming services, to request an authentication token that the authenticator, including mobile apps, hardware tokens or facial recognition, can provide.

By separating the authentication step from service access, the WebAuthn standard gives users access to a broad range of potential authenticators, most of which do not require passwords. WebAuthn is currently supported in Google Chrome, Mozilla Firefox, Microsoft Edge and Apple Safari web browsers, as well as Windows 10, iOS and Android platforms.

Sites that support WebAuthn include Google, Dropbox, GitHub, Okta, Twitter and Microsoft. Google last year rolled out an update so people with iPhones could use WebAuthn with more types of security keys as the second factor to sign into a Google account.

MFA, THE NORM?

Since the start of the pandemic, remote working has become the new norm, forcing organisations to increasingly rely on accessing business services and data through the internet.

The sudden shift to remote work pushed credential theft to the top of the cyber attackers' focus. This meant that organisations needed to introduce and rely heavily on multi-factor authentication to re-establish trust with their users who were remotely connecting to the corporate network and assets. If the only authentication is a password, they are not protected against the numerous cyber attacks available, including credential stuffing, where bad actors try commonly available stolen usernames and passwords against online services.

The Australian Cyber Security Centre says that our national security agencies receive one report of cybercrime almost every 10 minutes, and many of those attacks are perpetrated using stolen usernames and passwords to access online services.

Adding a second factor is a game changer. Even one of the weakest forms of two-factor authentication, which is two-step verification through SMS text messages, is better than nothing. However, it pales in comparison to other MFA methods, like security keys, that can stop 100% of all targeted attacks, according to a Google security study.

With the significant rise in cyber attacks now top of mind for many organisations, now really is the time to be implementing the open security standards, because it is no longer a matter of if, but when will an attack occur?

IMPACT ON USER EXPERIENCE

Generally, the user only has an interest in getting their work done or checking out their social media pages; security is a secondary concern until something bad happens.

The industry and the FIDO Alliance, along with W3C, have focused these modern open authentication standards to be built with ease of use in mind. There is no sense in implementing harder-to-use security standards when the target audience will just find a way around them. Defining this open standard has realised a simpler user experience, reduced cost of ownership and strong security to minimise adoption challenges.

The user experience must be easier than what is in use — a PIN (similar to a credit card), a biometric or a touch, alongside a secure external hardware device (security key) will ease the current pain felt by users struggling to keep up with ever-increasing demands for password complexity and differing methods of getting access to their daily online activities.

WHAT'S NEXT?

Throughout 2021, companies and their security teams should take extra steps to protect every user with multi-factor authentication, which will eliminate most of the threats to their cloud services and virtual infrastructures.

Ultimately, open standards have benefits for user experience, identity and authentication, and provide stronger security. Our belief is that open security standards are actually more secure, not less than the closed proprietary ones, combined with the ease of use and convenience, which makes them a win-win for users and their organisations.

Alex Wilson, Director of Solutions Engineering for Asia Pacific at Yubico.

THE ROLE OF AI IN PUBLIC SECTOR

Peter Hughes, Vice President Sales, APAC, RingCentral

The 2021 federal Budget was notable for the $1.2 billion funding support provided for the Digital Economy Strategy, which forms the basis of the federal government's vision for Australia to be a leading digital economy and society by 2030.

One of the more significant investments in the Budget — $124.1 million — is for artificial intelligence initiatives, with a view to drive greater AI adoption across the economy.

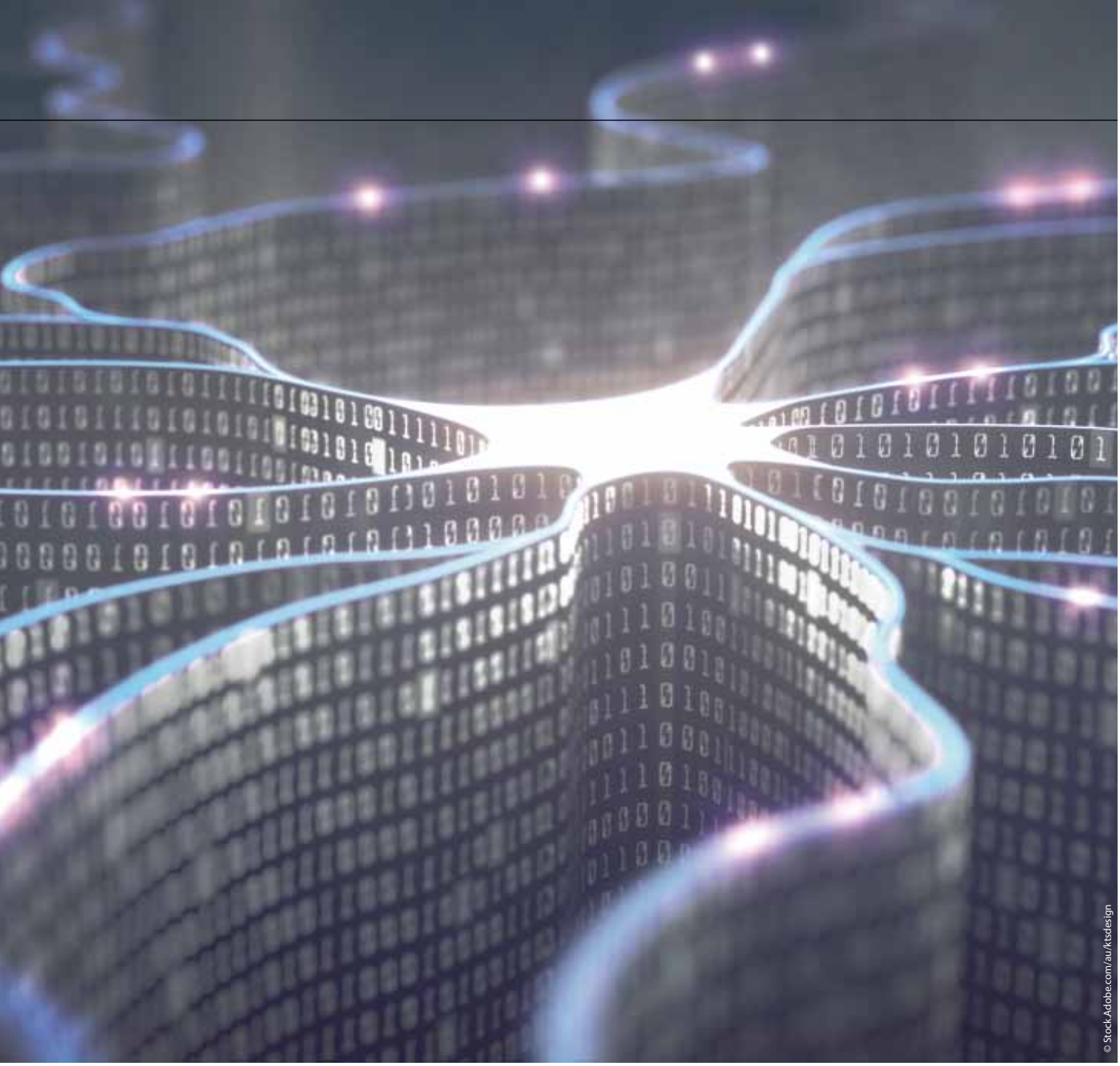
There are any number of applications for AI across industry sectors, but the role of AI in the public sector itself shouldn't be overlooked, particularly in the area of customer service.

Two years ago Gartner predicted that by 2021, 15% of all customer service interactions globally would be handled completely by AI, an increase of 400% from 2017. While that prediction might have been a little ambitious, particularly as it applies to the delivery of government services, there is incredible potential here with the right investment.

The Digital Economy Strategy has frictionless government service delivery as one of its goals, with 100% of Australian Government services available online a measure of success. To achieve this, the government at the same time needs to focus on more foundational digital transformational activities, such as consolidating and integrating IT systems and data, and improving information sharing and analytics. The good news is that this is being done, and there are also a number of specific announcements in the Budget, including $120 million for the Department of Veteran's Affairs to consolidate its IT system and create a data sharing analytics solution.

Once you have integrated systems in place that can access and share data both within specific agencies and also across departments, tremendous opportunities open up to deliver increasing levels of automation and self-service — and to do this across all forms of communication, from social media queries and live web chat, to email and telephony interactions.

Within many contact centres today, AI is already in use, particularly in the area of efficiency, such as skills-based routing or workforce management. Where AI can start to play a much bigger role in customer service is in the routine enquiries that up until now have been dealt with by live agents. AI also allows government agencies to scale up and be far more responsive to spikes in demand from the community, such as information or advice with regards to COVID-19. AI can also be applied to automate the post-call process where an agent needs to enter additional notes about the



© StockAdobe.com/au/ktsdesign

interaction they have just had — saving them time, which increases the agent's availability for the next call. Instead of typing in the notes, the agent can review the comments entered automatically by the AI bot and simply click 'OK' if everything is in order.

Some of the other applications of AI to enhance customer service include virtual agent learning engines to improve performance over time based on customer interaction, improving the time taken to solve the customer's query. That could also include behavioural analysis to ensure that the resolution isn't just achieved more quickly, it's also producing more positive customer satisfaction as well.

Of course, the other foundational component that's needed to implement AI-enabled automation is a single unified communications platform, which ensures that the service experience is consistent and the interactions are managed and captured across all channels. The level of integration that's already possible today with AI apps in cloud communications platforms like RingCentral allows for a much fast implementation of AI capabilities and an acceleration in the agency's customer service abilities.

This acceleration will be critical, when we consider the opening paragraph to the Digital Economy Strategy: "Australia's place in the world will be defined by how we adapt to digital technologies and modernise our economy. The next 10 years will determine whether we lead or fall behind."

WA HEALTH SERVICE PAVING THE WAY FOR DIGITAL HEALTH CARE

© Stock.Adobe.com/au/ipopba

AN ABORIGINAL COMMUNITY HEALTH SERVICE IN PORT HEDLAND, WESTERN AUSTRALIA, IS USING TECHNOLOGY TO ENSURE BETTER CONNECTED CARE FOR LOCAL PATIENTS.

The Wirraka Maya Health Service relies on My Health Record to keep up to date with patient pathology, imaging, medication, dispensing and history records. Over 2020, the health service uploaded the ninth highest number of shared health summaries in Western Australia, recorded the highest number of event summaries and viewed more uploaded documents than any other primary care provider in Western Australia.

Dr Yolande Knight, Senior Medical Health Officer at Wirraka Health Service, said My Health Record helps the health service see what other doctors have requested and performed, and overcome delays while waiting for records requested from other practices and providers.

"We find it helpful because a lot of our patients are transient, moving from one region to another, so it can be difficult to get their comprehensive files. We can also upload and share what we've done, so when the patient attends elsewhere, their record is current and available to other practitioners," said Dr Knight.

My Health Record also displays which scripts have been dispensed, with PathWest results automatically available. Dr Knight said this has helped with the recent COVID-19 test results, where it was quicker to see the result on the patient's record than to join the phone queue to get the result.

Another key benefit for patients is that they can use the shared health summaries and prescription information that has been uploaded by Wirraka Maya as proof of any underlying health conditions, which can enable them to obtain an early COVID-19 vaccination.

Wirraka Maya Health Service originated from the efforts of Aboriginal people to establish a health service to address the unmet needs of Aboriginal people in the Port Hedland and South Hedland areas and surrounding communities. It commenced clinical services in 1996 and now has more than 7000 residents registered and actively engaged in wellbeing, primary care and prevention programs across the region.,

Australian Digital Health Agency Consumer Advocate Steve Renouf said, "It's great to see an Aboriginal-controlled health service leading the way in achieving outstanding results in the use of digital technology. This commitment to digital service delivery will continue to enhance clinical outcomes in local communities and help breach the digital divide that can disadvantage remote patients."

Aboriginal Health Council of Western Australia (AHCWA) Public Health Medical Officer Dr Marianne Wood said the AHCWA has been very active in supporting the Aboriginal Community Controlled Health Services (ACCHS) and wider WA health sectors in the My Health Record project, recognising that the benefit of the record is greater when there is a collective effort.

"The ACCHS sector in WA has been a leader in the use of My Health Record and we are very proud of the great work by Wirraka Maya. Many ACCHS recognised, early on, the enormous potential of the record in improving the care of Aboriginal patients, particularly for those who travel widely and receive care from many different healthcare providers across this enormous state," said Dr Wood.

WA Primary Health Alliance General Manager (Primary Care Innovation and Development) Bernadette Kenny commended Wirraka Maya's use of My Health Record, adding that it ensures that clients are supported throughout their health journey in the Pilbara and beyond by providing vital clinical information when it is most needed.

"This is the result of the whole team at Wirraka Maya working together and understanding the real benefits to their community when it comes to utilising the digital health services available to them," said Kenny.

A louder drumbeat to achieve national cyber resilience

Nick Lennon, ANZ Country Manager for Mimecast

The risk of cyber attacks on critical infrastructure is on the rise. All countries must heed the wake-up call that no nation is immune from attack, and act with a sense of urgency to strengthen cyber resilience at national, organisational and individual levels.

While recent cyber attacks appear sophisticated, many hacks are the result of poor cybersecurity hygiene, and a breakdown in cybersecurity processes and procedures. A case in point, the hackers that took down Colonial Pipeline — the largest fuel pipeline in the US — accessed the network using a compromised password through a VPN account. A textbook breach that can keep every cybersecurity professional awake at night.

The federal government has proposed new laws to harden Australia's cyber posture, recognising that threats are evolving rapidly, and criminals are expanding their targets.

Under the Security Legislation Amendment (Critical Infrastructure) Bill 2020, government departments — and the soon-to-expand list of sectors deemed 'critical national infrastructure' — will need to scrutinise supply chain partners and their security protocols. It underscores the importance of keeping internal security incidents to a minimum to reduce lines of attack.

Critical partnership in cybersecurity supply chain

Individual companies will need to review cybersecurity practices to ensure they align with government and industry standards. Government departments need to carefully review and vet security partners in their own supply chain to ensure they satisfy the requirements of robust cyber resilience.

In an effort to lead by example, the federal government is investing in the cybersecurity posture of its own agencies through the National Data Security Action Plan, ensuring that governmental departments walk the talk.

Privacy incident reporting — individual weaknesses

Resilience across private and public sector organisations and departments, while guided by a national security framework, involves day-to-day protocols around managing privacy. This is where Australian organisations have weak links, according to Mimecast privacy research, which revealed around one-third of organisations fail important security provisions by not providing detailed privacy briefings when on-boarding new staff, regular training on privacy and protecting personal information, secure data transfer processes and comprehensive remote work protocols.[1]

Mimecast's research also found government fared better than most industries at committing to awareness training[2]. However, public sector staff fell short when it came to reporting all privacy incidents, with 31% not declaring an incident, compared to 19% across all sectors, indicating a real need to address this element of training.

Other Mimecast research shows that 76% of companies have been hurt by their lack of cyber preparedness[3]. Human error has been found to be involved in the majority of cyber incidents, and the risk increased drastically as remote and hybrid work patterns became the norm. With the wave of cyber attacks, many government departments and organisations are simply struggling to keep up, which is why we've designed an Enterprise Cybersecurity Platform to help mitigate cyber risks and address the ongoing cybersecurity challenges.

Slip, slop, slap for cyber

To navigate this complex and higher-risk environment, investment in a broad public awareness and education strategy, much like the hugely successful 'Slip, Slop, Slap' sunscreen campaign of the 80s — or the more recent 'Dumb Ways to Die' Melbourne Metro safety campaign — is essential. Cybersecurity now requires the same constant awareness and reminders of responsible behaviour as sun and transport safety.

At Mimecast we process tens of millions of emails every day across Australia and from around the world, allowing us to see and block many attacks before they impact local organisations. We are part of the national threat intelligence community, sharing our own intel and receiving insights from the government to help better protect all levels of Australia's government, industry and citizens. This is what we call "community defence".

[1] Source: ACA Research commissioned by Mimecast April 2021

[2] Source: ACA Research commissioned by Mimecast April 2021

[3] Source: Mimecast State of Email Security Report 2021

mimecast

Mimecast

www.mimecast.com

PUTTING PEOPLE AT THE CENTRE OF AGED CARE MEANS INVESTING IN TECHNOLOGY

David Deakin, Transformation and Healthcare Industry Director,
Dell Technologies Australia & New Zealand

THE STORIES OF LIMITED ACCESS, SUBSTANDARD CARE AND SYSTEMIC PROBLEMS IN AUSTRALIA'S AGED-CARE INDUSTRY UNVEILED IN THE ROYAL COMMISSION INTO THE SECTOR HIGHLIGHT THE NEED FOR AN IMMEDIATE CALL TO ACTION.

The federal government's Budget injection of $18 billion to better support home care and free up staff to spend more time with residents in care is a welcome one.

But this investment is the start of the conversation, not the conclusion. We need to ensure these funds deliver tangible outcomes for all aged Australians, particularly the one in three people in aged care estimated to be experiencing neglect or abuse.

One of the aims of this investment is that, by 2023, aged-care residents will receive at least three hours and 20 minutes of staff interaction. However, staff shortages will be a major challenge; it is expected that an additional one million aged-care roles will be needed by 2050 to service the needs of an ageing population with increased life expectancy.

Attracting more people to work in aged care is important, but it can't be the only answer. As the Royal Commission into Aged Care Quality and Safety report notes, in 2019, there were 4.2 working-age people for every Australian aged 65 years or over, but by 2058, this is expected to decrease to 3.1. The maths of having a smaller talent pool to fill more positions simply doesn't add up.

On top of that, there's the fact that Australia is a big country with a small population and older Australians are less likely than the general population to live in major cities. So, the need for access to aged-care services is spread across areas that are not always well serviced for healthcare and other support services.

Technological innovation is going to need to carry the burden of addressing many of these issues.

AGED CARE IS ABOUT PEOPLE, NOT BUILDINGS

In the year from the start of the COVID-19 pandemic until March 2021, Australian medical professionals conducted 52.9 million telehealth appointments. While the primary purpose of this shift to telehealth was to contain the spread, it proved a leap forward in how Australians use technology to manage their health and hints at what we can achieve in the aged-care sector by embracing the digital and virtual.

Of course, phone or video consultations are just the tip of what technology can enable but, just as there are some types of consultations better served in a face-to-face setting (what that rash is, for instance) than a telehealth one, there are a range of virtual care opportunities that can complement the face-to-face services. Hybrid clouds and the Internet of Things mean that instead of the patient coming to the carer, care can now come to the patient.

For instance, a virtual assistant that can interact with people in their homes provides a cost-effective way to ensure they are taking medication, building healthy habits or monitoring their vitals, with the ability to easily escalate to an appropriate healthcare professional when required.

This provides people the independence of staying in their own homes for longer, reducing the demand for places at aged-care facilities. It also lets them stay in their communities longer if facilities are not locally available.

SIMPLIFYING THE WORK

One of the ambitions of the federal government's investment in aged care is that carers will be able to spend more time with those in their care. The simplest way to make that happen is to eliminate as much of the non-client-facing work as possible.

For instance, the staff in an aged-care facility may currently spend a portion of their shift taking paper-based notes on the care provided to each resident that day and then handing over to their teammates on the next shift. If they can instead quickly input that information to a resident's profile via an app as they work, then the staff on the next shift can access that and other relevant historical data quickly, which not only improves the quality of information on each patient but frees staff to deliver personal care.

DATA IS THE BEST MEDICINE

For innovation like the above to deliver the best outcome, it's not just about the tech in the hands of the patient or carer, but the systems and infrastructure that underpin it.

Having to fill in similar paperwork for each new institutional encounter is tiresome for recipients and their families, and it also leads to incomplete information, especially if they're relying on human memory. Secure universal digitisation, systems interoperability and data integration across the sector will improve communication and lead to better outcomes for those in their care.

More meaningful data will also drive informed, measurable decisions, especially as the sector can increasingly call on AI and machine learning to uncover insights that might not be readily discovered through human analysis alone. And with cloud services increasingly able to deliver compute intensive projects such as AI, the costs of engaging this technology will go down and it will also be available no matter where patients or facilities are located.

SIMPLIFYING DIGITAL TRANSFORMATION

With much of the aged population living outside major cities, changing the way we fund and support the digital transformation of aged care is a key consideration to how we support them. If care is going to happen in the communities in which people live, as-a-service offerings, such as Dell Technologies APEX, simplify how organisations consume and manage technology. Resources no longer need to be concentrated in big city hubs.

It means resources can scale up or down in response to the shifting needs in the community. Consumption-based technology also addresses the challenge of finding the right tech skills, especially in regional areas, in an increasingly competitive market. According to RMIT and Deloitte Access Economics, Australia will need 156,000 more digital technology workers by 2025 to meet demands.

With organisations able to leave the deployment, ongoing management and support, and implementation of upgrades with providers such as Dell Technologies, it not only frees them from having to find those skills themselves, but it also means head count can be skewed towards those who spend face-to-face time with those in their care.

The Royal Commission recommended that Australia needs to put people at the centre of aged care. The way we do that is by investing in the smart, accessible and innovative technology. Dell Technologies APEX is simplifying digital transformation with an end-to-end as-a-service solution, making it easier for organisations to scale up and down as needed and only pay for the resources they use with flexible consumption.

CREATING A SEAMLESS **COVID-19 VACCINE ROLLOUT**

Sharryn Napier is the Regional Vice President for Australia and New Zealand at New Relic. With over 20 years of experience in the IT industry, she has worked in senior leadership roles at Qlik, Serena Software and CA Technologies.

The COVID-19 vaccine rollout is underway, amid difficult delays. But as the Australian Government continues the next phases of vaccine delivery, they have been faced with challenging technical issues. Just hours after the Department of Health released its vaccine eligibility checker, multiple users said that they received error messages when attempting to make a booking.

MyGov struggled to keep up with demand at the height of the pandemic in March last year when they were faced with similar website crashes. These continued outages should be a red flag to government agencies — if the technology is broken, it needs to be replaced. It's also vital that the Australian public is informed through automated alerts, and that the lines of communication are continually open.

CLEAR, 24/7 COMMUNICATIONS

Government agencies have the means to communicate with citizens, but need to ensure that this outreach is automated. It can be complex having to manage a wide range of communication channels, from traditional post to email, SMS and in-app messaging, but the right technology solution can manage this and automate communication efficiently.

By having reliable, timely messaging regarding any changes in scheduling or service delivery delays, the Australian community will continue to feel connected to the government at all times. This makes it much more likely that a seamless user experience can be achieved and it also builds trust, which is critical for encouraging people to participate in vaccination programs.

SIMPLIFY SIGN-UPS

While the rollout of the COVID-19 vaccine is a Department of Health initiative, there are many internal and external stakeholders involved. Such a project provides an excellent opportunity for stakeholders — such as GP clinics and government agencies — to collaborate and simplify the sign-up process.

One of the challenges of government services is that various departments and agencies have traditionally used a range of different sites and apps. The federal government has brought various services together under the banner of MyGov, such as Centrelink, Medicare and the ATO. But not everyone has log-ins for these yet. Other apps may only be state based, such as Service NSW. The Service NSW app has been very successful, having now been downloaded four million times, representing 75% of the NSW adult population. But there hasn't been equivalent success in every other state. Finding a way to link all these disparate contact points to a central sign-up database is crucial, even if this is done state by state rather than nationally.

© Stock.Adobe.com/au/Gorodenkoff

For sign-up to be successful, it also has to be a simple process. This includes making it accessible for people whose first language may not be English. It's also vital that any sign-up process can cope with uneven spikes in demand. Multiple sites and apps, not just government sites, crash immediately after going live due to a rush of visitors. Planning extra capacity for the first hours and days is crucial, as is real-time monitoring to avoid any problems cropping up.

DASHBOARDS TO DETECT ISSUES

The COVID-19 pandemic proved a fertile breeding ground for cybercrime, and regrettably — if not surprisingly — vaccination programs have also been attacked by cybercriminals. The Australian Competition and Consumer Commission's Scam Watch has been notified of over 6415 scams since the COVID-19 outbreak last year, with multiple phishing texts and emails being sent by criminals impersonating the Australian Government.

One of the biggest problems for government agencies across the globe is cyber espionage to steal data and deliberately disrupt vaccination programs. According to US security experts, many pharmaceutical companies, vaccine researchers and organisations involved in vaccine storage and transport have all been targeted by multiple cyber-espionage groups in recent months.

To immediately detect suspicious activity, tech teams must have visibility across an entire technology stack in real time. Creating dashboards via an observability platform allows these groups to grasp the size and scale of the technology landscape. It can be used to display alerts and point to when and where problems are happening.

Vaccinating over 20 million people is far from an easy task. But if government agencies are experiencing issues with their technology providers, they must look to alternative suppliers who can provide a robust, secure and reliable service. Then, they can truly focus on the practical challenges of logistics and education that's needed to support a successful vaccination rollout.

DIGITAL GOVERNMENT DURING AND AFTER COVID-19

Luke Thomas, Regional Vice President APAC, Appian

The COVID-19 pandemic has forced government organisations to reassess their strategies, plans and aspirations for digital transformation. Despite the uncertainty, IT leaders must quickly identify and act on strategies and plans that lead to positive outcomes.

Some organisations are embracing digital transformation and accelerating the adoption of new technologies for service and program delivery. In several scenarios, organisations will expand the role of digital government platforms.

Gartner advises government CIOs leading the transition to digital government to assess all strategy-driven initiatives, both planned and in progress. They can then choose to continue, suspend or cancel existing initiatives while identifying new opportunities.

THE IMPORTANCE OF CITIZEN EXPERIENCE

Many government organisations' approach to service and program delivery focuses on improving service delivery and shifting to be more citizen-centric. Government IT organisations are creating citizen experience (CX) management roles, digital product teams and employing user experience (UX) techniques including journey mapping, persona development and A/B testing.

This is because the average Australian engages with government for a variety of services throughout their lives: voting, taxes, health care, social security and welfare, and more. However, interacting with the government has historically meant encountering disparate websites, multiple logins, hard-to-find or hard-to-use tools, and little or no transparency into processes or the status of requests.

The rise of millennials and Gen Z combined with the way commercial companies do business has forced the government to reimagine its customer service. Think of a food order from your smartphone. You enter in your basic information, select your items, watch as the order is accepted, prepared, driver en route, and when it is time to meet the driver at your door. Then, with just a few taps, an incorrect order can be redelivered or refunded in a matter of seconds. People expect everything to work this way now. This is considered good customer service, which leads to high customer satisfaction, which leads to repeat business.

JOURNEY MAPPING

Often we hear about citizen experience (CX) upgrades in reference to making websites easier to use or moving

© Stock.Adobe.com/au/photon_photo

away from paper processes. But the experience doesn't end with entering information into a website or completing a digital form. While it begins with those things, CX goes much further.

Journey mapping is an exercise to map the step-by-step experience or 'journey' that a customer takes from start to finish of a process. For the government, it's putting itself in the shoes of the citizen, living the experience moment by moment to reimagine the process through empathy.

Focusing on the journey seems simple in concept but execution is much more complex within government where processes often touch multiple organisations, systems, databases and people, and consist of many steps and various outcomes. And while journey mapping is a step in the right direction, more must be done.

DIGITAL GOVERNMENT TRANSFORMATION IN THE POST-COVID-19 WORLD

Government organisations need a fast, flexible way to bring IT, business and program staff together to ensure new and overhauled systems meet program, outcome, accountability and government efficiency requirements.

A proven approach to successful government digital transformation is introducing low-code automation, to build new applications that execute on top of legacy systems. This allows IT to be more responsive to rapidly changing needs and reduces technical debt, while quickly delivering value, new services and cost savings.

Low-code automation quickly improves citizen experience by delivering the following:

Unified data — Leveraging a low-code automation platform means government organisations don't have to spend time, money and resources to migrate data living in multiple, disparate, legacy systems (unless they want or need to). A low-code automation platform can pull data from anywhere into one unified record for organisations to take action, then send the data back to where it lives.

Flexible delivery — Data anywhere, host anywhere, run anywhere. A low-code automation platform allows organisations to connect and extend existing IT investments. Solutions can be deployed in the cloud, on-prem, or span a hybrid environment. Low-code developers need only build customer-facing applications once, and automatically they are delivered across the range of citizen devices: smartphones, tablets, personal computers and beyond.

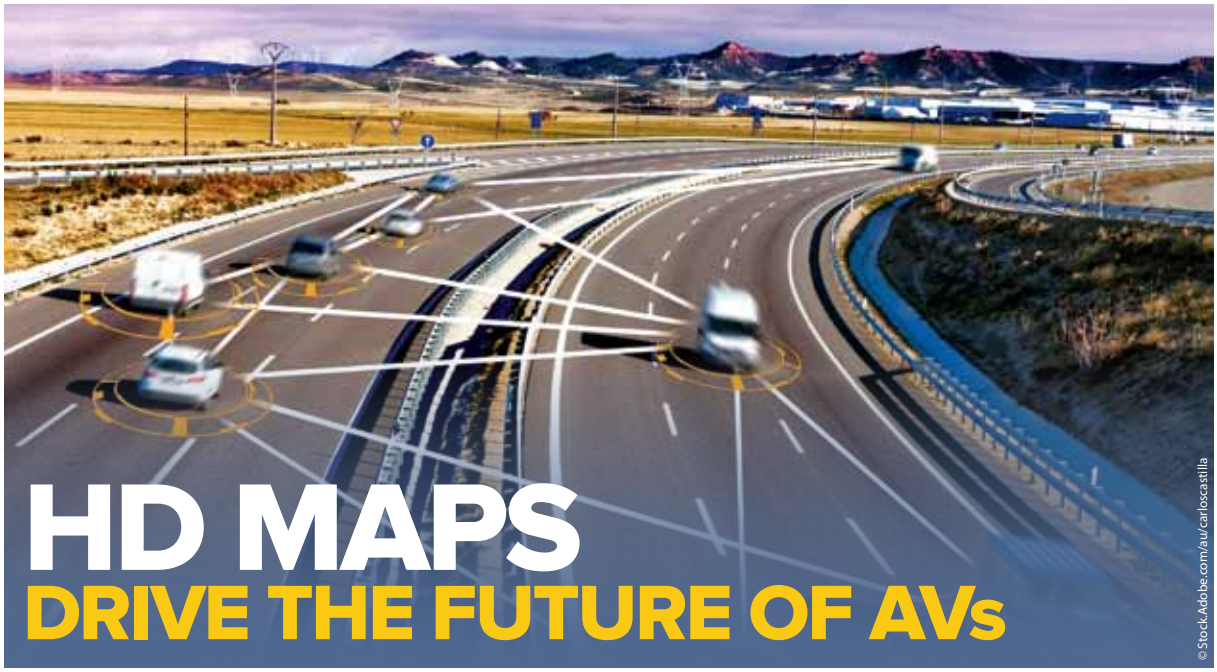
Speed to production — Multiply your development workforce through reusable drag-and-drop components that empower more people to build applications quickly. With this type of rapid development, organisations can turn ideas into applications 20x faster than with traditional development methods.

Automation — A low-code automation platform can improve CX by combining the power of artificial intelligence (AI) and robotic process automation (RPA) with enterprise workflow, case management and low-code development to enable the journey map. AI can route emails quicker by performing sentiment analysis while RPA eliminates the need to re-enter the exact same data (name, phone, address, etc) across multiple systems, as well as reducing the time it takes to route and respond. Additionally, the number of calls into a call centre to check the status of a service request can be reduced by providing communication and transparency throughout the entire process.

With increasing shortages of talent, time and money, government organisations must shift from custom code to low-code ways of thinking or it will never reduce its technical debt. Modernising government technology with a low-code automation platform gives IT the power to accelerate digital transformation projects.

The Appian platform combines RPA and AI with iBPMS, application platform as a service (aPaaS) and low-code development to deliver digital government initiatives with a high ROI. By adding Appian RPA and AI to their applications, government agencies can dramatically improve operational efficiency, citizen experience and staff engagement.

For more information: https://appian.com/solutions/industry/government/overview.html.



HD MAPS
DRIVE THE FUTURE OF AVs

HIGH-DEFINITION (HD) MAP CREATION COULD BE AUSTRALIA'S CHANCE TO LEAD A CORE ASPECT OF THE AUTONOMOUS VEHICLE TECHNOLOGY SPACE, SUPPORTED BY GOVERNMENT–INDUSTRY COLLABORATION.

Professor Michael Milford, a robotics expert and Acting Director of the QUT Centre for Robotics, has conducted research projects into mapping for autonomous cars and the use of artificial intelligence (AI) to see how autonomous cars could handle Australian roads.

"Map updating is a major challenge to autonomous vehicle adoption everywhere, including Australia, but it's not yet a mature field globally so there's opportunity for us to catch up quickly," he said.

Professor Milford noted that current European mapping solutions don't recognise unique Australian signs or infrastructure and require customisation. He noted that although widespread autonomous vehicle use is some time away, the primary aim now is to ensure that the digital, physical and regulatory infrastructure is ready to go.

"We need to plan and design technology that is fit for purpose from the very beginning, not shoehorn it in at the very end when we realise the tech doesn't do what it's meant to do," he said.

Professor Milford believes that collaboration between map creators, localisation services and governments for infrastructure updates and privacy regulation would be the ideal solution.

"Current maps do not have all the information necessary to be full HD maps, or links to information about infrastructure changes. Unless a car knows explicitly about environmental changes like road works, for example, positioning systems will find it hard to work well," he said.

Government notifications around these events could be very important, with Professor Milford adding that meaningful government involvement or oversight is vital due to the significant data and privacy implications of these maps.

While positioning is a core part of the technology offering from autonomous vehicle companies, it may also need improving to provide accurate services in Australia. Professor Milford notes that while current positioning systems work well most of the time, there are failure points, like heavy rain and tunnels, where the technology is not reliable enough.

"There'd be nothing worse than a car thinking it's in one location but actually being in another, and erroneously referencing the wrong section of the HD map as a result of that positioning error," Professor Milford said.

QUT, which specialises in robotic and autonomous vehicle positioning research, is working with government and industry on the future of HD maps and investigating the ideal models for government–industry collaboration.

"If we started a staged approach toward this collaborative model now, within two years we would have a working prototype for how information from private map providers, the government, and possibly from vehicles on the road could be shared between all of those key stakeholders to ensure maps are as accurate and up to date as possible," Professor Milford said.

Keep the cybercriminals at bay

Mimecast is the enterprise cybersecurity platform designed to protect government departments from a wave of cyber attacks.

mimecast.com/GovernmentAU

High-resolution dual thermal sensor

The FLIR Vue TZ20 is a high-resolution, dual thermal sensor gimbal purpose-built for the DJI Matrice 200 Series and Matrice 300 airframe. Featuring both a narrow and wide field of view (640 x 512 resolution) FLIR Boson thermal camera module, the Vue TZ20 offers greater situational awareness with a 20-times digital thermal zoom capability for public safety and industrial inspection missions both near and far.

The plug-and-play gimbal system for the DJI Matrice 200 Series and Matrice 300 is now available in Australia. With the FLIR Vue TZ20, users have a FLIR dual thermal gimbaled payload option for the DJI Matrice 200 Series and Matrice 300 airframes. This enables public safety drones from police, fire, and search and rescue teams to have greater awareness to complete their missions.

IP44 rated to provide operability in poor weather conditions and weighing just 640 g, the Vue TZ20 includes a wide-angle Boson with a 95-degree field of view and a narrow-angle Boson with a 19-degree field of view.

The Vue TZ20 was developed with the DJI Payload Software Development Kit (PSDK) and DJI Skyport 2.0 platform, offering simplified plug-and-play operation through the DJI Pilot Software. Payload functions include thermal video streaming, video recording and still-image capture with 20-times zoom, helping operators to conduct missions at safe distances while capturing the thermal data and detail required.

Teledyne FLIR
www.flir.com.au

Facial biometric authentication technology

iProov's facial biometric authentication technology, Genuine Presence Assurance, is designed to provide a secure and effortless way to verify user identity online. It is used by governments, banks and healthcare providers around the world to authenticate citizens and provide secure access to digital services.

Genuine Presence Assurance enables organisations to confirm that the person they are interacting with online is the right person (does this person exist and have the right to access the online account or service?), a real person (is this person a human being and not a photo, a mask or other presentation attack?) and authenticating right now (is this person authenticating themselves right now and not a deepfake or other synthetic media attack?).

Together, these make up Genuine Presence, which lies at the heart of the unique assurance iProov is designed to deliver.

Genuine Presence Authentication is designed to enable organisations to offer a secure online authentication process. It also maximises organisations' online customer completion rates with effortless usability, while reducing fraud risk and providing compliance with regulations. Genuine Presence Assurance also futureproofs businesses against machine-driven attacks from deepfakes and other emerging threats.

iProov works with governments globally, including the Australian Taxation Office, the US Department of Homeland Security, the UK Home Office, the UK National Health Service (NHS), Singapore GovTech and Estonia.

iProov Ltd
www.iproov.com

How sharing is changing the way governments are using data

As a result of a growing reliance on IT systems to support day-to-day activities, government departments and agencies are awash with digital data.

From policy documents and financial records to activity schedules and citizen communication, this data is growing in volume and importance. It not only supports current activities but also provides a platform for strategic planning.

Much of this data is stored centrally and then shared with those people who require access. This can be achieved using a variety of mechanisms from email and FTP to cloud storage and APIs.

While these methods work, they come with restrictions. Sharing data in these ways requires copies to be made which then end up in multiple locations. Security can be compromised, and users are never sure whether they are actually viewing the most up-to-date version.

The situation becomes even more complex when different departments and agencies need to share data sets with others. Files in different formats arrive via different mechanisms and then must be combined and standardised for use.

A new approach to data sharing

To overcome these challenges, increasing numbers of public-sector organisations are exploring the potential of a new approach to data sharing. The approach overcomes the cumbersome existing processes and allows more flexible and valuable sharing to be achieved.

The approach also makes data available in real time. In this way, those using it can be confident they have the very latest versions of files or database entries. This improves the accuracy of work based on the data and minimises risks.

This new approach involves the decoupling of storage resources from compute resources. This differs from traditional databases and data lakes but delivers sizable advantages. Users are able to directly access shared data and then use their own compute power to examine and manipulate it.

As a result, large numbers of users can access the same data set at the same time without causing any performance issues. Because there is no competition for compute resources, everyone can work at full pace all the time.

Security is maintained as the data owners can be very granular about exactly what resources can be accessed and by whom. If a user has not been granted permission, they simply can't get to the data in the first place.

The democratisation of data

Sharing data between departments and agencies in this way essentially democratises access to it across the board. As a result, collaboration can increase and insights gained that previously would have been impossible to obtain.

For example, agencies can compare their performance with others in critical areas. The impact of a policy change in one area can be assessed to determine whether it should also be introduced in others.

External parties can also benefit. Commercial organisations can be granted access to relevant data to support their forward planning. By understanding the steps being taken by government, they can better guide investment and activities to maximise commercial returns.

It also brings the potential for data to be monetised. If external parties can see a commercial advantage in its use, they are likely to be happy to pay for access. This can open up a new and potentially lucrative opportunity for the public sector.

The rise of the data exchange

Taking this approach another step forward, increasing numbers of organisations are taking advantage of emerging data marketplaces and exchanges. Through these mechanisms, data holders can make known what data sets they have available and how much access might cost.

They operate in the same way as eBay or Amazon. Those looking for data query a catalogue and select the data sets that are most relevant to their requirements. This takes data democratisation a step further and means even more value can be achieved.

The ongoing rise in data sharing will have lasting impact on governments at all levels. By taking time now to understand the implications, those in the public sector will be much better placed to reap the benefits.

snowflake®

Snowflake
www.snowflake.com

WHAT DO PUBLIC SECTOR CDOs DO?

ASIA–PACIFIC (APAC) PUBLIC SECTOR ORGANISATIONS HAVE YET TO DEVELOP A CLEAR UNDERSTANDING OF THE IMPORTANCE OF DATA AND THE EMERGING ROLE OF THE CHIEF DATA OFFICER (CDO) TO THE ORGANISATION.

A recent report by Qlik and Omdia found that 47% of APAC CDOs feel their roles lack clarity in job definition, job execution or both. The report also revealed that 75% of CDOs regret not having invested more in data-driven initiatives before the COVID-19 pandemic, which could impact their ability to use technology to develop better citizen services like public health.

The 'Emergence of the Public Sector Chief Data Officer in the APAC' report analyses the state of the public sector CDO community in APAC. It surveyed 103 senior public sector data executives across Australia and New Zealand, India and Singapore, revealing the concerns, challenges and priorities of these CDOs.

The report found that only 44% of APAC organisations rely on data insights when making mission-critical decisions, while 62% of public sector organisations have yet to establish a data governance body, despite proof that such a body can build management support and broader awareness of the value of data in decision-making. Almost two-thirds (62%) of APAC CDOs felt that leadership support is crucial to help them perform in their role.

Alongside organisational support, CDOs cited analytics and business intelligence technology as the top resourcing priority (73%) to enable data use within their organisations. CDOs had technical and strategic concerns for implementing data technology, such as integrating data, finding the right technology partner and upskilling public sector workers.

Data science (50%) and data policy (49%) were the most sought-after skills among public sector organisations. The CDOs surveyed also expressed the need for establishing a corporate culture of using data to support decisions (71%) and a more data-literate workforce (68%).

As public sector organisations in APAC reposition themselves beyond COVID-19, data initiatives are forecast to become more strategic and outcome-focused. Key priorities include improving data quality (51%), introducing new technologies (49%) and achieving a data strategy with a one-year action plan (42%).

Geoff Thomas, Senior Vice President (APAC) at Qlik, noted that public sector CDOs in APAC need to help their organisations understand the value of data and create a data-literate culture that enables employees to act on it.

"CDOs don't have to go on this journey on their own. There's a multitude of resources from the community to help public sector agencies, executives and staff get started. At the same time, technology partners can consult on the most effective data strategy to inform decision-making. APAC public sector CDOs have a real chance to apply the lessons learnt during COVID-19 to rethink how to serve citizens in new ways, using data as the foundation for innovation," said Thomas.

The public sector CDO is an emerging role within APAC organisations; though these executives have prior experience in the broad government sector, they are relatively new to the CDO function, with 57% of CDOs having less than two years of experience in that role.

Another Qlik study found that US public sector organisations are more advanced in developing strategies to establish a framework and standards for cross-agency data sharing, improving the efficiency of data collection and secure sharing of protected data. The report found that 71% of US public sector organisations see data as a priority, as opposed to 36% in APAC.

FREE

for government and industry professionals

The magazine you are reading is just **one of 11** published by Westwick-Farrow Media. To receive your **free subscription** (print or digital plus eNewsletter), visit the link below.

wfmedia
connecting industry

www.WFMedia.com.au/subscribe

AUSTRALIAN MADE

MFB

DESIGNERS & MANUFACTURERS
OF 19" RACK SYSTEMS

50 YEARS ANNIVERSARY

PROUDLY MANUFACTURING IN AUSTRALIA

bsi ISO 9001 Quality Management ISO 14001 Environmental Management

19" Rack Cabinets Licence No. 84394

mfb.com.au **VIC** (03) 9801 1044 / sales@mfb.com.au **NSW** (02) 9749 1922 / sydney@mfb.com.au