govtech review

OPTIMISING ANALYTICS
GETTING BIG VALUE FROM BIG DATA

CYBER ATTACKS
PHYSICAL SECURITY UNDER FIRE

DATA CENTRE SUSTAINABILITY
GET AHEAD OF THE GAME

Q2 2022
PP100021607

Advanced Multi-Circuit Metering for Energy Management Solutions

Unequalled Compliance tested to Australian Standards

AS 62052-11
AS 62053-21
AS 62053-23

SATEC
Powerful Solutions

www.satec-global.com.au | (02) 4774-2959

Q2 2022

INSIDE

FEATURES

6 | From recommendation to regulation: a blueprint for data centre sustainability compliance

With rapid acceleration to a more automated world, efficient and reliable data centres are at the heart of a green future.

14 | How big data improves the citizen experience

Utilising big data and analytics to better understand the citizen journey will deliver better agency impact.

16 | How multi-cloud innovations can unlock the potential of government agency data

An organisation's use of more than one cloud service provider is a convenient way to store and share data.

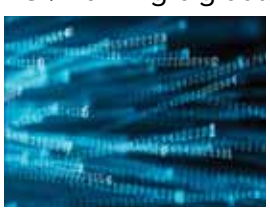
19 | Digital-first, flexible and responsive: the future of e-government

Modern e-government is more complex than streamlining procedures; it involves ambitious goals, numerous stakeholders and a minefield of compliance issues.

21 | Twin strategies to improve the customer experience for government services

A multitude of digital solutions are available to defend against today's most sophisticated cyber threats.

23 | Turning big data into big value with the right technology



Go beyond technology upgrades and transform the entire operating model using the right data.

9 | Does customer experience quality reflect at the polls?

28 | Harnessing big data analytics in the public sector

31 | Evolving government digital services beyond the pandemic patchwork

34 | Disruptionware: preparing for new age cyber attacks

Cover image: © Stock.Adobe.com/au/Fernando Madeira

Insider

As we enter the second half of 2022, there's a lot to ponder. The recent federal election obviously delivered a change in government and all of the adjustments that a shift of that magnitude naturally entails.

For many of the nation's voters, climate was a key decision-driver when it came time to cast a ballot. Unsurprisingly, for an increasing number of organisations and agencies, it's also at the forefront when developing business strategies and practices designed to lessen environmental impact.

With data centres responsible for 1–2% of the world's energy consumption, it's no wonder the regulatory landscape continues to evolve and demands that the industry follows suit. What may have been 'energy efficient' in decades gone by just won't cut it in today's sustainability-focused world. Our cover story this issue outlines a five-step blueprint for organisations aiming to apply a holistic approach to environmental responsibility.

Of course, those data centres only exist because we've become increasingly information-hungry. The public and private sectors are capturing more data every day and bearing the obligation that comes with that collection, including adequate storage and protection.

As AI and machine learning evolve and become a permanent part of the landscape and augment human-based interactions, it's up to agencies and organisations to ensure that they are utilising data in ways that deliver better customer experiences and help improve business decision-making. Data for data's sake doesn't deliver much in the way of advantage, it's only with the application of the right technology and analytics that the true value is unlocked.

We've got plenty of content in this issue to provoke thought around useful utilisation of data and how to meet customer expectation in an increasingly digital world.

Our ever increasing reliance on data is not without its downside, however. Cybercrime is on the rise as would-be attackers find new and more nefarious ways of causing trouble — from physical security to disruptionware, the playing field is ever changing. It wouldn't be an issue of the magazine without a discussion on cybersecurity, so read on for more insight.

I hope you enjoy this issue of *GovTech Review*.

Dannielle Furness, Editor
editor@govtechreview.com.au

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
Dannielle Furness

gtr@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Colleen Sam, Linda Klobusiak

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

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

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

FROM RECOMMENDATION TO REGULATION

A BLUEPRINT FOR DATA CENTRE SUSTAINABILITY COMPLIANCE

Mark Deguara, General Manager Data Centres, Schneider Electric

From electrical safety standards to ensuring equipment can be recycled, the IT sector has a long history of being one of the most heavily regulated industries. When looking at how quickly the criticality of data centres is becoming, it becomes evident why there is a constantly evolving regulatory landscape.

Consumers and environmental groups are becoming well aware that data centres represent 1–2% of total global electricity consumption. With many more Australian data centres being developed nationwide, so too is consumer concern around climate change. As attention from climate 'watchdog' organisations increases, identifying effective and efficient green regulation has never been more important.

Despite being heavy consumers of energy, data centres contribute substantially to energy management in the economy. While some data centres claim energy-efficient designs, it should be noted that the average Australian data centre is now over 20 years old, when sustainable design wasn't a consideration.

With this rapid acceleration to a more automated and digital world, efficient and reliable data centres are at the heart of a green future. As our digital footprint expands, so too will the need for green data centres.

GOVERNMENT AGENCIES ARE IMPOSING REGULATIONS GLOBALLY

While there is a clear course of action in Australia, such as expanding the NSW Government implemented NABERS initiative into all other states, there is much more that can be done to create greener data centres.

Globally, government agencies are facing the same challenges with data centre sustainability. By looking at the regulations imposed by other countries paired with results, Australia can take an evidence-based approach to implementing new sustainability compliances.

In 2019, Singapore raised a moratorium on new data centres to address carbon emission challenges. One of its policies includes ramping up uptake of renewable energy, where Singapore aims to increase its solar capacity by more than seven times by 2030, bringing it from seven-fold to a 2-gigawatt peak (GWp).

Similarly, Indonesia is making good progress with green building standards in its major cities. The country of 270 million people aims to reduce building energy intensity by 1% per year until 2025. Japan and the Republic of Korea have adopted zero net emissions targets to be achieved by 2050, showcasing strong commitment towards driving sustainability.

The EU released its Green Deal in January 2021. It warned Europe may still need to act to make data centres more energy efficient. EU advisors have put the tough measures on a long list of policies the EU could conceivably use that includes a tax on data centre pollution and incentives for owners that invest in green data centre technology. Additionally, in July 2021, they also released 'Fit for 55', which recommends legislative policies to reduce carbon emissions by 55% by 2030.

In China, the Beijing Development and Reform Commission said in April of 2021: "For projects completed in 2021 and after, the proportion of annual renewable energy utilisation in annual energy consumption will increase by 10% every year, and 100% will be achieved by 2030."

IMPOSING A 5-STEP SUSTAINABILITY BLUEPRINT

In addition to taking inspiration from the green regulations of other countries, Schneider Electric has established a clear framework for how data centres can achieve a holistic environmental sustainability approach.

1. Set a bold actionable strategy: Use a data-driven consultation approach to help create an actionable strategy and reach your climate and sustainability ambitions. Ensure you are leveraging data for optimisation, analytics and reporting. Today's organisations are recognising that improved sustainability performance contributes to improved financial performance, and investors have taken notice as well.

While governments are looking to set the bar for sustainability compliance within data centres, industry pioneers are pushing the boundaries of their sustainability goals with climate commitments becoming increasingly expected by employees, customers and investors alike.

For example, while a goal of carbon neutrality was once a differentiator, we now recognise the potential to have even greater impact with carbon negative operations. This year, Iron Mountain joined Google in setting public goals for 100% hourly matched carbon-free energy from local resources.

2. Implement efficient data centre designs: When building or buying into data centres, apply an architectural approach to create customised, efficient, repeatable, serviceable, vendor-agnostic designs. Ensure compliance, transparency and higher environmental performance of products are kept in mind.

3. Drive efficiency in operations with software and digital services to enable remote monitoring capabilities. Optimise the lifespan and efficiency of your systems by defining a clear strategy for maintenance and modernisation to augment the lifespan, inclusive of recycling services for end-of-life products to ensure circular economy best practices.

4. Buy renewable energy (PPA and onsite): Explore a custom renewable procurement strategy that includes: microgrids, PPAs, VPPAs, energy-as-a-service and EACs. In an effort to offset power used by data centres, Amazon recently purchased two Australian solar farms. The most recent solar farm purchased by the company generates 250,000 megawatt hours of clean energy each year, which is the equivalent of approximately 40,000 average Australian homes.

5. Decarbonise supply chains: Evaluate your Scope 3 footprint to help identify and execute strategies to meet decarbonisation objectives, and use digital performance tracking and reporting for your decarbonisation program. Most recently, major oil and gas company Chevron had its board vote to reduce Scope 3 emissions on an absolute basis, reducing the total by 40% by 2030.

Sustainable business practices are on track to becoming standard business, and some may argue they already are. Aside from being the best path towards addressing the most pressing issue of our time, they're often the best solution from a business standpoint. Data centres are the beating heart of the IT sector, and while Australia has a long way to go, sustainable regulations will provide the opportunity for a greener future while pushing the boundaries of Australia's overall sustainability commitments.

DOES CUSTOMER EXPERIENCE QUALITY REFLECT AT THE POLLS?

Just over half (53%) of Australians and New Zealanders said their experiences of interacting with government services directly affect how they vote, according to new Qualtrics research, with 25% saying it has a significant impact.

As government agencies work to modernise and expand services in response to changing resident demands, expectations and behaviours, findings from the study reveal the importance of delivering positive experiences in these new environments. Alongside voting preferences, two-thirds also said the experience provided by government agencies, such as available information and booking systems, impacted their decision to get a COVID-19 vaccine. For 26%, it had a significant influence on their decision. These findings were published in the Experience Management for the Public Sector report.

DIGITISATION A PRIORITY

As part of the transformation of government service delivery, digitisation must be a continued priority. A third (32%) of respondents said they are more satisfied when using digital platforms. Similarly, 48% said they now expect to use digital services most of the time when accessing government services. More than half (58%) said they have increased their use of digital platforms to engage with government agencies since the start of the pandemic.

Government agencies managing health (including tracing and vaccination status), transport and services currently achieve the highest volumes of residents satisfied with the experiences being delivered. They are also the top listed agencies residents prefer to engage with through mobile and online channels, further highlighting the impact of a positive digital experience.

Findings from the study build on Qualtrics' recent Consumer Trends study, where customer service support, communications and ease of use for products and services were highlighted as the top areas for public sector agencies to improve.

"Following two years of rapid digital transformation within all industries, residents have high expectations for the services being delivered. This requires a shift in how government agencies manage their programs, with a critical need to rapidly uncover opportunities and take immediate action to improve the services being delivered.

"We are already seeing some government agencies make progress in these new environments, and it will ultimately lead to better outcomes for all involved — from greater trust through to a rise in inclusive citizen access to programs and initiatives," said Phillip Bland, Industry Advisor for Public Sector Solution Strategy, Qualtrics.

IT'S NOT JUST THE RESIDENT EXPERIENCE

As organisations from all industries navigate an increasingly competitive job market, separate findings from Qualtrics' 2022 Employee Experience Trends report found 4 in 10 public sector workers (39%) in Australia and New Zealand could look to switch jobs this year.

For agencies wanting to attract and retain talent, hybrid environments, flexible working arrangements and the opportunity to do meaningful work will be key. More than two-thirds of respondents said they would look for a new job if they were asked back to the office full-time (69%), while the opportunity to do meaningful work, flexible working arrangements and working with great people were the top reasons people would apply for a job in the public sector.

"Competition for new talent is rising, and in the public sector candidates and employees are also all residents. It's therefore especially vital that the public sector gets the experience right for both groups, especially as we know negative experiences can have knock-on consequences. By understanding and delivering the types of experiences people want at work, government agencies will be in a stronger position to attract and retain a purpose-driven, high-performing workforce," Bland said.

RMIT urges Vic Govt to address supply chain weaknesses

RMIT's Blockchain Innovation Hub has urged the Victorian Government to explore the use of blockchain and other advanced technologies to help shore up vulnerabilities in Melbourne's supply chains.

In a new report, the university argued that blockchain and NFTs, as well as AI, drones and autonomous vehicles, are the keys to addressing the supply chain vulnerabilities exposed during the pandemic.

The report, co-authored by RMIT's Centre for Cyber Security Research & Innovation and the Digital Ethnography Research Centre, also includes research opportunities and policy recommendations for building more resilient and just supply chains towards a digital CBD for Melbourne.

Report co-author Dr Tharuka Rupasinghe from RMIT's Blockchain Innovation Hub said the key to resolving disruptions to Melbourne's supply chains is integrating digitalisation.

"Melbourne needs resilient supply chains that respond to shocks and threats with the ability to adapt to changing conditions. The city has the potential to be a testbed for autonomous vehicles and to develop a blockchain pilot," she said.

The report calls on the Victorian Government to create a based supply chain pilot targeting a specific industry, with RMIT suggesting the construction industry.

Meanwhile NFTs can be used as digital twins to mitigate against fraud, theft and loss, while standardising supply chain cybersecurity requirements would support cyber resilience and mitigate against risks when operationalising emerging technologies, the report argues.

ATO selects Qualtrics for citizen experience management

The Australian Taxation Office (ATO) has selected Qualtrics to deliver support and services that help the federal government agency continuously improve its citizen experience, and better connect with the community.

The multi-year agreement with Qualtrics provides the ATO with a platform focused on improving service delivery across channels in real time. Through the ability to capture, analyse and act on feedback shared with the agency, Qualtrics CustomerXM will enable the ATO to rapidly identify and meaningfully address customer issues, streamline processes and provide stakeholders with greater visibility of the citizen experience delivered.

The ATO will use Qualtrics to conduct research among Australians and tax advisers, with insights set to guide and inform product and service innovation. The easy-to-use tools and expert support provided by Qualtrics will allow the ATO to quickly investigate issues, and rapidly access and analyse results from across the user experience.

"By focusing on listening and acting on feedback to continually improve delivery and ensure services and support are able to address evolving and diverse needs, government agencies like the ATO have an incredible opportunity to strengthen relationships with the people they serve," said Phillip Bland, Principal Industry Advisor Public Sector Solution Strategy ANZ, Qualtrics.

acer

Windows 11

ULTRALIGHT PERFORMANCE FOR HYBRID WORKSTYLES

TravelMate Spin P6

Intel® Evo™ Platform Powered by Intel® Core™ i7 Processor[1]
14” 16:10 FHD+ IPS Narrow-bezel Display
Built-in 5G Connectivity[2]
Acer User Sensing Technology

Collaborate with confidence with Windows 11 Pro.

1 - Specifications may vary depending on model and/or region. All models subject to availability.
2 - 5G speed and availability vary on the area. Not all carriers support eSims. Check your telecoms provider for details.

$3.4 million TAFE upgrade for Bowen

North Queensland will become the heart of agriculture training, with the first sod turned for a new $3.4 million Agriculture Centre of Excellence — featuring a tech-focused 'Smart Centre' — in Bowen.

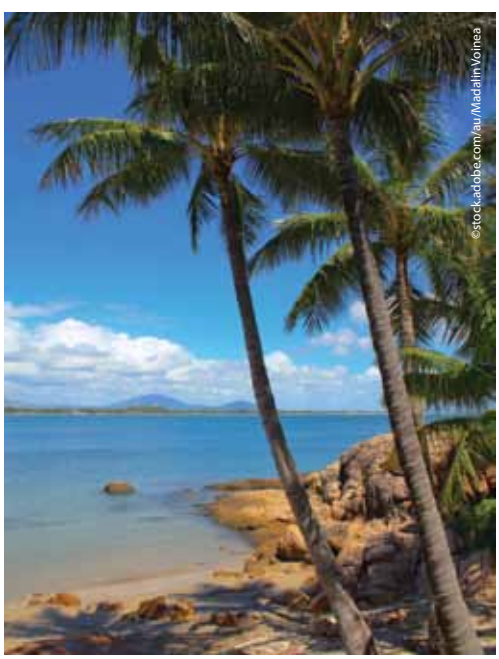
Turning the first sod at the Bowen TAFE campus, Minister for Employment and Small Business and Minister for Training and Skills Development Di Farmer said the state-of-the-art facility would train and prepare Queensland's workforce for growth in the agriculture industry.

"The new centre will offer more than 70 courses related to agriculture and will help trainees and apprentices develop the skills they need to ensure Queensland is ready to capitalise on industry growth," Farmer said.

"Bowen is a prime location for agriculture training and industry expansion and highlights North Queensland as a great place to work, live and invest."

In addition to general learning and workshop areas, the Centre of Excellence will feature a Smart Centre for data analysation and computerised training technologies; a virtual reality room providing advanced tech for emerging industry needs; a science lab; a Farmbot for robotics, nutrition, soil science, biology and coding; and a Growpod for monitoring stable growing environments and producing horticultural and agricultural products in all climates.

Construction is due to be completed in August this year.



Orgs want more government support on security

Australian organisations are cautiously supportive of government mandates demanding cybersecurity standards for software due to concerns over cyber warfare activity in Ukraine and its potential to spread internationally, according to research published by Trellix.

The security company's recently published Cyber Readiness Report, based on research conducted by Vanson Bourne, found that 64% of Australians surveyed would support such mandates.

But at the same time around half of the respondents fear that government software security mandates will be too complex, expensive to implement and have too-difficult-to-meet timelines for implementation.

Meanwhile, 90% of Australian respondents agree that there is room for improvement in the level of cybersecurity partnerships between their national governments and organisations.

Likewise, 56% believe that government should share data on attack vectors used by adversaries to help organisations better protect themselves, and 44% would like to receive more data on attacks in progress.

Globally, 82% of respondents believe ware supply chain risk management is of either high or crucial importance for national security. But in Australia, 63% rate these policies and processes as difficult to implement, with only 40% claiming full implementation of appropriate controls.

Meanwhile, only 41% of Australian reported fully deploying EDR-XDR solutions, only 24% have implemented multi-factor authentication and a mere 16% have adopted zero trust strategies.

One of the biggest barriers to the implementation of these and other advanced technologies is a lack of in-house staff resources, cited by 49% of Australian respondents.

HD4 MBX
HD2 MBX

WirelessTech

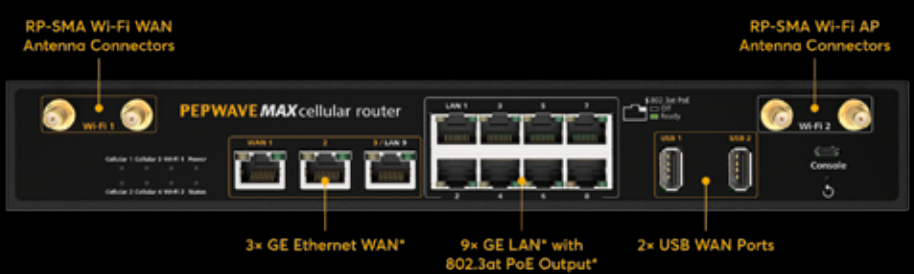
Ideal for On-The-Go Deployments

Dual or Quad Cellular Gigabit 4G/5G 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



+61 2 8605 7787
sales@wirelesstech.com.au
www.wirelesstech.com.au

HOW BIG DATA IMPROVES THE CITIZEN EXPERIENCE

James Horne, CEO, Balance Internet

AUSTRALIAN CITIZENS HAVE BEEN EMBRACING DIGITAL TECHNOLOGIES FOR YEARS. HOWEVER, SINCE THE PANDEMIC HIT, THE COUNTRY'S DIGITAL UPTAKE HAS ACCELERATED AT LIGHTNING SPEED.

More than ever before, Australians expect that they can access just about anything online: from shopping and food delivery, to streaming music and television, right through to accessing government services. They expect a rising standard of online experience.

Whether it's paying council rates or submitting tax claims to the ATO, the digitisation of government services quite simply makes everyday life easier. But as the digital economy rapidly evolves, so must those services and how they are delivered. Creating a digital platform where citizens can interact with departments and agencies is just the beginning — these platforms must be constantly evaluated and adjusted in order to continually improve the citizen experience. And in order to do this, governments need to turn to big data and data analytics.

BIG DATA, BETTER SERVICES

Big data analytics has completely transformed private enterprise, giving companies the ability to establish a 360° view of their customer base, segmenting them by demographics and tailoring products and services based on their customers' specific behaviours, preferences and unique tastes. However, this level of business intelligence isn't reserved for private enterprise — it can also be used by government departments whilst being compliant with privacy requirements, to improve the citizen experience.

Every web click represents a step in a citizen's online journey; a journey which can be collected and stored for future analysis. Over time, the data collected from thousands of citizens' journeys begins to show patterns in their behaviour — highlighting popular products and services, as well as potential issues that may need addressing. Perhaps there's a point where a large number of users suddenly fall off, indicating that the site is lacking the right information and needs to be adjusted in some way. Perhaps a large number of citizens from a particular regional location are all searching for the same thing, indicating that the department may need to rework messaging or add new services to that particular location. The way citizens interact with a platform tells a story — and when the data from those interactions is analysed and actioned appropriately, it can help improve departmental effectiveness.

SEARCH MADE EASY

In a world where there are hundreds and thousands of services available, improving the citizen experience can simply be about making things easy to find. Skill Finder is an excellent example of how data can be aggregated in a way that makes important services — such as free online courses — easily accessible from a single location.

Skill Finder was developed by the team at Balance Internet in 2020 when a significant part of the Australian workforce had been affected by the pandemic, leaving thousands of workers in desperate need of upskilling in order to find new work. In response to a call for action from the Hon Karen Andrews, Minister for Home Affairs (who was Minister for Industry, Science and Technology at the time), Australia's tech industry came together to develop the digital skills marketplace, connecting jobseekers with flexible courses designed around microskills. With thousands of online courses, the platform provides an opportunity for every Australian citizen to level up their knowledge with transferable and useful microskills.

However, Skill Finder wasn't simply a one-off project. Since its inception, the site has been continually tweaked and adjusted — based on the continual analysis of user data — to improve its ease of use. With short, 1- to 2-hour beginner courses by far the most popular, these courses are now flagged to new users to assist with their upskilling journey. The site also responds to particular searches, helping users find courses that will help them on specific career pathways, depending on the search terms the citizen is using. By using data-driven insights to better understand the citizen journey, Skill Finder is continuously being updated to produce better and better outcomes.

MAKING GOVERNMENT SHOPPABLE

In an increasingly digital world, Australians quite simply expect their government's digital capabilities to match those of the private businesses they deal with on a day-to-day basis. There is no reason why citizens shouldn't have the same ease of experience when dealing with the public sector as they do when shopping online. In fact, e-commerce has perfected the customer experience in such a way that it provides the perfect template for government agencies; a way to create their own digital 'shopfront' where citizens can easily search, browse and shop the public services they require.

And just like e-commerce businesses that are continually improving their customer experiences, government agencies should also be looking at ways to improve the user experience and make information more accessible. Through utilising big data and data analytics to better understand the citizen journey, departments will be able to improve these experiences and, ultimately, improve agency impact and mission effectiveness.

HOW MULTI-CLOUD INNOVATIONS CAN UNLOCK THE POTENTIAL OF GOVERNMENT AGENCY DATA

Chris Osborn, Australian Federal Director and WA & SA Regional Director, Dell Technologies, Australia and New Zealand

THE MULTI-CLOUD, OR AN ORGANISATION'S USE OF MORE THAN ONE CLOUD SERVICE PROVIDER, IS A CONVENIENT WAY TO STORE AND SHARE DATA.

Many government agencies have embraced the opportunity to easily share data with remote workforces, choosing multiple cloud services to suit the needs of their various missions.

However, without a clear and cohesive strategy, data stored across clouds can become unwieldy and time-consuming to manage while opening vulnerabilities, increasing the risk of a cyber attack. Advancements in multi-cloud technology, like those recently unveiled at Dell Technologies World, can help connect cloud services and simplify their management.

Embracing innovative multi-cloud software and solutions will improve how government agencies manage their data and applications, which are increasingly spread across multiple, disparate locations. Bridging the gap between cloud services — from data centres, colocation facilities and public cloud to the edge — will allow organisations to manage their data across all sites with ease and agility.

By adopting a multi-cloud ecosystem, government agencies will unlock a unified, secure cloud experience that will improve their cyber security and resilience, and streamline processes while maintaining flexibility and freedom of choice. Ultimately, the advancements will unlock the full potential of government data and prepare agencies for the multi-cloud future.

A MULTI-CLOUD ECOSYSTEM

Work-from-home and hybrid workforces have continued past pandemic lockdowns, becoming permanent fixtures. Sharing and storing data on the cloud has become increasingly commonplace, and often several cloud solutions or platforms are used to take advantage of the benefits of each.

A study by Forrester Consulting commissioned by Dell Technologies supports this, revealing that 83% of organisations in the Asia Pacific and Japan have adopted a multi-cloud approach or plan to within the next 12 months. Government agencies are among the organisations making the move to cloud services — for example, the NSW Government reports that by 2023, all NSW Government agencies will have a minimum of 25% of their ICT services on a public cloud.

The push towards a multi-cloud environment gives agencies the chance

to rethink their data storage in terms of their workloads and specific mission needs. Each cloud platform offers unique benefits that can be leveraged for specific purposes, meaning agencies can get the most value from their data.

However, with a growing number of users and countless Internet-of-Things (IoT) devices connected to the network, handling the data can get complicated, and the risk of a cyber attack grows. Stringent cybersecurity measures are a must for government agencies, which often need to manage sensitive data, making them particularly vulnerable targets. The Australian Cyber Security Centre (ACSC) has encouraged organisations to urgently adopt an enhanced cybersecurity posture following numerous high-profile attacks. One of their top three recommendations is to back up data regularly to the cloud and ensure it's secure to avoid loss of data in the event of a breach.

Unfortunately, backing up data to the cloud isn't enough. Ransomware and malware attacks can infect backup files by spreading to connected hard drives, IoT devices and cloud storage. The ACSC suggests having files backed up offline on multiple storage devices in different buildings or locations and swapping hard drives regularly for maximum security. Though this may be effective, it's inefficient and can be a time-consuming drain on agency resources.

Agencies can benefit from the new vision for the multi-cloud: bringing together the best aspects of public and private cloud to create a unified, secure cloud experience that's more connected and consistent across all environments.

To achieve this vision, cloud service providers like Dell Technologies are championing an open multi-cloud ecosystem, partnering with leading hyperscalers and cloud stack vendors to create a diverse partner community that works together on behalf of the customer. These advancements in multi-cloud storage can protect data in new ways, enhancing an organisation's ability to recover from an attack while giving them the opportunity to effectively use their data — without having to spend countless hours managing the data across services or creating backups.

"Embracing innovative multi-cloud software and solutions will improve how government agencies manage their data and applications."

INNOVATIONS CAN UNLOCK POTENTIAL

Protecting data while getting the most out of it is key for digital transformation, and Dell Technologies' cloud storage software innovations embrace this fact. The multi-cloud management solutions and partnerships announced at Dell Technologies World will provide a consistent operating model across providers to deliver a streamlined cloud experience.

By extending the multi-cloud ecosystem, agencies will have freedom of choice rather than being limited to one service or multiple disconnected platforms, and the management of various services will be an easier task. Agencies can expect to power new levels of automation and security with multi-cloud flexibility.

One of the major partnerships announced — between Dell Technologies and Snowflake, the Data Cloud company — will give agencies the ability to use on-premises data stored on Dell object storage with the Snowflake Data Cloud while keeping their data local or seamlessly copying it to public clouds. The companies will work together to connect data from Dell's industry-leading enterprise storage portfolio with the Snowflake Data Cloud. A first of its kind, this collaboration will help government agencies have greater flexibility operating in multi-cloud environments, meet data sovereignty requirements and easily turn data into insights.

On top of this, Dell announced the new APEX Cyber Recovery Services, plus more than 500 software advancements across Dell PowerStore, PowerMax and PowerFlex, which will deliver faster data insights, better multi-cloud data control, and increased cyber resiliency. These advancements highlight Dell's storage software innovation following the introduction of Project Alpine, which will bring the enterprise capacity, performance and protection of Dell storage software to public clouds.

Implementing a holistic multi-cloud strategy and automating storage operations will give agencies greater data visibility, giving them the ability to fix issues quickly as they arise and maintain compliance across all clouds at the same time. This will significantly reduce manual labour time spent on maintaining, sharing and securing data on the cloud.

Other benefits include improved security and resilience, better application performance, greater storage capacity and less disruption to business operations. Essentially, these innovations will assist government agencies as they navigate the new age of multi-cloud storage and will turn their data into an asset rather than a liability.

THE MULTI-CLOUD FUTURE

The future of data storage resides in the cloud — across multiple, connected platforms. Effective multi-cloud storage can be used to unlock the full potential of agency data while reducing complexity and manual labour and protecting it from cyber threats. With the new partnerships forming between cloud service providers, and innovative software and solutions, government organisations can be free to choose whichever, and as many, cloud platforms and solutions suit their varying needs, equipping them to excel in the multi-cloud future.

Federal election polling day could be done better, technically

Nathan McGregor, Senior Vice President Asia Pacific, Cradlepoint

Every three years, Australians are summoned to polling booths around the country to vote for their preferred political party who will run the country for their elected term. Sausage sizzles and cake stalls are tradition, but one other element of the federal elections has remained a mainstay — the reliance on paper-based voting and identification processes. Some polling booths used digital databases this time around, but these aren't centralised, so there's still nothing stopping voters from voting multiple times.

While setting up a digital identification and voting system across the board seems like an almost impossible task, the sophistication of wireless connectivity today actually means that fully digitising the ID process in most areas of the country is achievable.

United States County Leverages Wireless Connectivity to Secure Voting System

Sacramento County in the U.S. needed to upgrade their voting equipment and model on a short timeline ahead of election day. Network security was mandatory and the solution needed to offer secure connectivity for the 80-plus vote centres, which depended on network connectivity for access to the central voter registration database.

Given the temporary nature of polling booths, vote centres could go up at a variety of locations, and with few to no IT staff onsite, the network solution had to be simple to deploy and easy to maintain.

Day-1 Connectivity at Temporary Locations

Sacramento County implemented Cradlepoint's NetCloud Service for branch, which includes cloud management, end-to-end network security and a wireless edge router with dual LTE modems. Sacramento County was able to set up secure networking for each voting centre and 80-plus devices in 15 minutes.

Bulletproof Security

The County deployed NetCloud Service, which allows it to manage every router from a centralised location.

A layered security approach was used that included:

- A cellular network, a secure overlay network, access control, and monitoring functions to ensure complete isolation from the Internet to eliminate the threat of rogue access at the vote centres.
- Encrypted private IP-VPN overlays connecting each wireless edge router to the data centre and routing that blocks the possibility of direct Internet access.
- Access control layer within the NetCloud edge firewall to block any unsanctioned traffic flowing from the LAN to the WAN.
- Real-time monitoring of the system with NetCloud Manager.

Multi-Carrier Connectivity

With Cradlepoint's dual-modem/dual-carrier capabilities, Sacramento County could connect two carriers for constant connectivity. The automatic switch from one carrier to the other occurs in mere seconds and both modems can be active at the same time, allowing for more bandwidth.

Remote Access

Cradlepoint NetCloud Manager helped with the deployment of the 80-plus vote centres by improving automation and making issues easier and faster to fix. Because Sacramento County needed to have the networks up and running for at least 11 days in locations staffed with non-technical people, the ability to use NetCloud Manager to log in and see the status of each network helped to confirm that everything is running accurately.

Voter Fraud Detection

With the new vote centre model, anyone in the county might show up at a voting centre. With the help of Cradlepoint's solutions, Sacramento County was able to connect back to headquarters without leaving the secure network to look up a voter and determine if they had already voted and what kind of ballot they should receive.

We are lucky to live in a country that has a true democratic process for electing national leaders, however our government and electoral process has some catching up to do in regard to incorporating digital technology into that voting process.

cradlepoint

Cradlepoint Australia Pty Ltd
www.cradlepoint.com/au

DIGITAL-FIRST, FLEXIBLE AND RESPONSIVE

THE FUTURE OF E-GOVERNMENT

Sebastian Krueger, VP APAC, Paessler

SIGNIFICANT ADVANCES IN DIGITAL TECHNOLOGIES HOLD THE PROMISE OF ENHANCING INTEGRATED CITIZEN-CENTRIC INFORMATION AND ONLINE SERVICES. MODERN E-GOVERNMENT IS A LOT MORE COMPLEX THAN STREAMLINING SOME PROCEDURES; IT CONSISTS OF AMBITIOUS GOALS, NUMEROUS STAKEHOLDERS AND A MINEFIELD OF LEGAL AND PRIVACY COMPLIANCE ISSUES.

The term e-government describes the use of technical resources to provide public services to citizens in a suburb, city, region, state or across the entire country. In principle, this covers all mutual relationships: it consists of the digital interactions between citizens and the government, between a central government and government agencies

or regional institutions, between a government and its citizens, between the government and its employees, and also between government and businesses.

To truly address the changing needs and expectations of their constituents, government agencies must be digital-first, flexible and responsive. Siloed, legacy systems are unable to support much-needed agility, but also pose a greater privacy risk and increased challenges for data sharing and service delivery.

However, for e-government to live up to its smarter public service delivery promise and play a role in enhancing the technical possibilities of citizen-centric services securely, it needs to function efficiently and effectively and be available on multiple channels. Therefore, sophisticated and constant monitoring of government IT is an essential part of maintaining citizen-centred e-government services for every public sector organisation.

THE TECHNICAL POSSIBILITIES OF E-GOVERNMENT

Areas such as big data analytics, artificial intelligence (AI) and machine learning, the Internet of Things (IoT), administrative and business process management and blockchain are all driving innovation in the public sector. Now collectively referred to as Government 3.0 — initially by Gartner, who coined the phrase — they are creating vast improvements in service delivery, resource management and decision-making in government entities.

For instance, 5G AI drones are now set to help with gathering images relating to damaged power and utility infrastructure due to floods and bushfires, following a successful trial of new technology by power company Endeavour Energy, alongside partners Amazon Web Services (AWS), Optus and Unleashed Live.

Digital government is not a set-and-forget investment and government organisations that evolve constantly and meet citizens on their own terms by engaging with them via their preferred channels — either in person, by phone, via a mobile device or through smart speakers, chatbots or augmented reality — will exceed their citizens' expectations. However, there are significant technical and compliance challenges to contend with when introducing this level of multichannel citizen engagement.

"Siloed, legacy systems are unable to support much-needed agility, but also pose a greater privacy risk."

THE CHALLENGES OF MONITORING GOVERNMENT IT

The following key issues are intended to provide an initial overview of regular challenges that the government sector faces in IT service delivery.

1. MANY DISTRIBUTED LOCATIONS

Whether it's the branch office of a public authority, a local authority in a regional district or several public data centres, almost all IT departments of public institutions are faced with the task of managing and maintaining distributed locations.

One solution to this is to have satellites at each location (not to be confused with agents, which must be installed on each monitored device). The satellites collect the monitoring data at the locations and send it in an encrypted form to the central instance that is responsible for the complete evaluation and storage of the data.

This helps keep costs low and expenses for operation and maintenance manageable, while at the same time the entire IT infrastructure is centrally monitored.

2. HETEROGENEOUS IT LANDSCAPES

The integration of branch offices, existing structures, hardware and software, virtualisation: networks of public institutions are heterogeneous. Devices and applications offer their own monitoring tools. Although these give us some insight, they contribute little to an overview of the entire IT system.

This calls for universal solutions that can monitor devices and applications independently of manufacturers as well as integrate special solutions into the overall monitoring process. The decisive factors here are, on the one hand, the standardisation of the solution in order to keep the costs low and, on the other hand, the flexibility to connect existing special solutions via the appropriate interfaces.

3. DATA PRIVACY

Government organisations manage and secure the sensitive data of their citizens using firewalls, virus scanners and backup systems, which are the standard building blocks of an integrated security concept.

However, for e-government to work effectively it is important to ensure that these systems work reliably. Did the backup work? Does the firewall work? Is the virus scanner up to date? A comprehensive monitoring system will include all of these elements in the monitoring process.

THE TAKE-OUT

Both internal processes and citizen services highly depend on an available and high-performance network. In order to guarantee this is fully functioning, IT teams need the appropriate information at their fingertips. A sophisticated monitoring system should therefore be at the heart of e-government because its IT infrastructure is the most important asset that enables it to provide digital services to all of its citizens, 24/7, 365 days a year.

The ability to leverage that monitoring data strategically in real time will significantly improve a government entity's ability to seamlessly deliver services, despite the increased strain on finite IT teams and technology resources in an era of post-pandemic budget cuts.

TWIN STRATEGIES TO IMPROVE THE CUSTOMER EXPERIENCE FOR GOVERNMENT SERVICES

Chrystal Taylor, Head Geek at SolarWinds

Government agencies today face ever-increasing pressure to deliver positive customer experiences to the public, more so than their corporate counterparts. Unplanned service outages don't just lead to frustrated users — they also invite elevated public scrutiny and inquiries over the use of taxpayer funds. This is not to mention the damage to agency reputation, erosion of public trust and doubts about the agency's ability to serve the general public.

These table stakes will only grow as federal, state and local agencies continue to digitise and bring public services, databases and information online. Can government agencies deliver an exceptional customer experience without breaking the bank?

Below are two key strategies they can employ to achieve this outcome.

EXPECT THINGS TO GO SOUTH — AND PLAN FOR IT

As the popular adage goes, "hope for the best, plan for the worst". Expect an outage to happen at some point, and

establish a crisis management and disaster recovery plan to ensure digital infrastructure can be rapidly restored and services can be brought back online. Informing agency employees about this recovery plan also minimises panic, reduces the risk of misinformation and allows customer support to confidently assure users things will return to normal within a short period of time.

Instead of troubleshooting and discovering the root cause of outages, such a recovery plan is meant to reinstate agency infrastructure, digital services or IT assets back to an acceptable level of operation, allowing the agency to continue delivering quality service to the public. To achieve this, the plan should include the following:

- Regular backups of mission-critical systems and assets. Schedule regular tests for backup restoration and assign agency stakeholders to understand and execute the various steps needed to restore these systems and assets.
- A response plan for different scenarios or threats. Responses to outages caused by human error will differ from responses to cyber attacks. Train agency stakeholders to identify and differentiate these scenarios and have detailed response plans for each.
- Infrastructure and data monitoring solutions. Monitoring should form the bulk of preventive measures. Studying correlations in monitoring data shows patterns and reveals the reason for outages, which informs troubleshooting and future prevention measures.
- Service redirects and messaging to users. Ensure redirection of affected public-facing sites to a temporary webpage with messaging, customer support and updates on the outage. User communication is key — keep users in the loop and be transparent to avoid excessive complaints.
- Procedures for third-party service outages. What happens when outsourced cloud or software as a service (SaaS) solutions go down? In addition to enforcing third-party service-level agreements (SLAs), keep an alternative list of providers or vendors the agency can rapidly switch to as a backup.

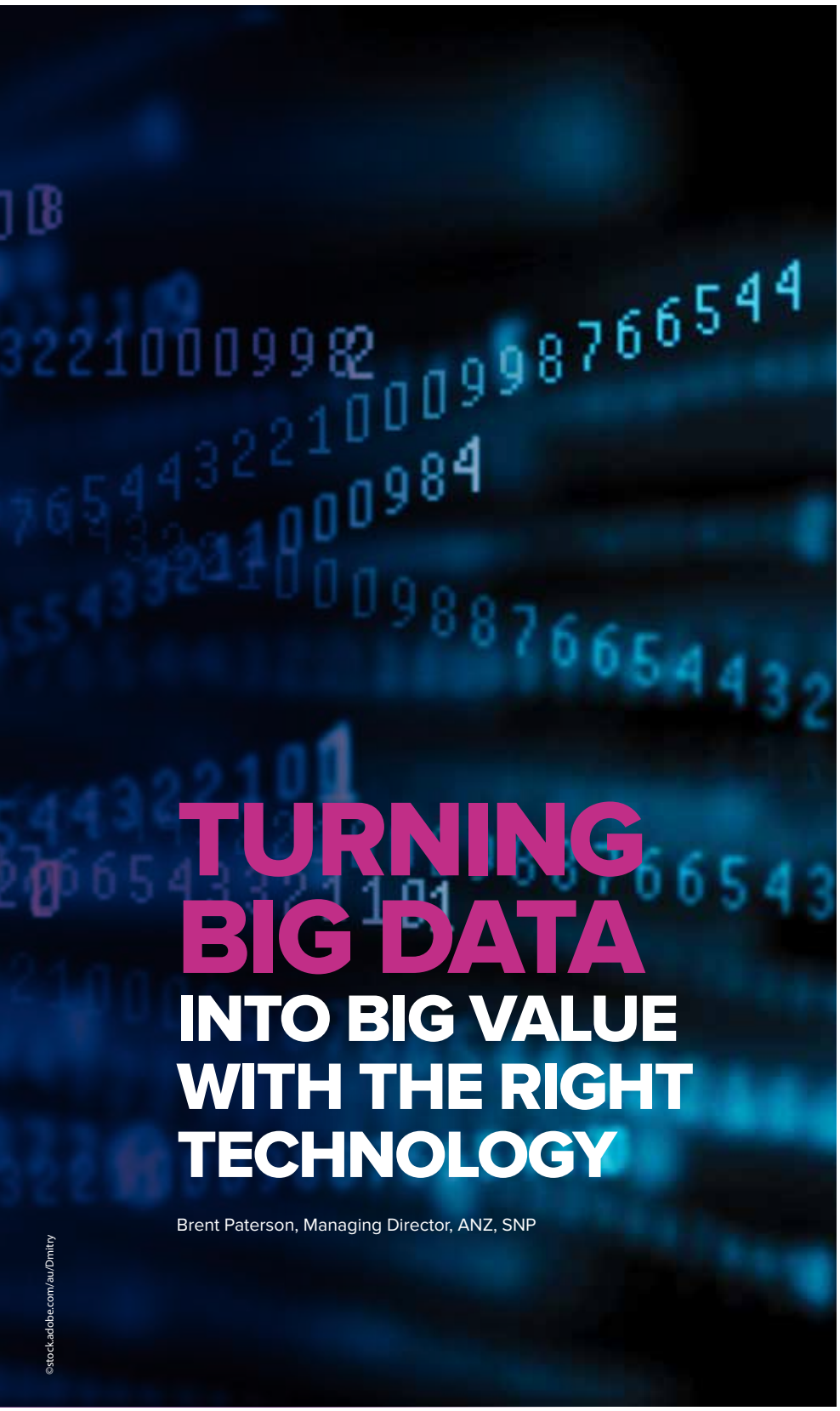
BUILD SECURITY INTO EVERYTHING

It goes without saying cybersecurity is non-negotiable for government agencies, especially for those with databases of sensitive citizen or federal data. Without strong cyber defences, agencies are vulnerable to bad actors and cybercriminals who will attempt to bring public services offline to access data or disrupt national stability. The fallout is obvious: public outcry over the ability of government agencies to safeguard sensitive data and protect vital services against external threats.

Fortunately, government agencies have a multitude of digital solutions at their disposal to defend against today's most sophisticated cyber threats. Some of the measures they can implement immediately include the following:

- Establish an internal cybersecurity team. The remit of this team includes reviewing and implementing cybersecurity practices and solutions, threat monitoring and ensuring compliance with data or cybersecurity laws.
- Employ a zero-trust mentality. Educate and train government employees to never click links, download files or provide access to anyone until verification and authorisation have been given by internal cybersecurity teams. Ensure access to resources is granted on an as-needed basis, regularly reviewed and revoked when no longer needed. Grant only the minimum required permissions to reduce risk.
- Monitor, monitor and monitor. Employ a security monitoring solution designed to log user behaviour and automatically analyse data to identify suspicious activity, notify IT personnel and record threats and bad actors in an internal database for future reference or audits.
- Consider new measures like application containerisation. Placing critical services and applications within containers allows cybersecurity teams to treat them as 'endpoints', which can be monitored and secured with greater intensity than if they were in a virtual machine with a hypervisor.

Implementing the above strategies in tandem will better equip government agencies to meet public expectations for more accessible and stable online services — expectations that have only increased over the pandemic. Agencies capable of meeting these expectations with stability, security and speed will obtain the favour of the general public, better secure their funding and become a shining example for others to emulate.



TURNING BIG DATA INTO BIG VALUE WITH THE RIGHT TECHNOLOGY

Brent Paterson, Managing Director, ANZ, SNP

To keep pace with changing organisational needs and working environments, government departments are increasingly prioritising digital transformation. However, digital transformation has become so common that many departments are upgrading or adopting new technologies and processes without having a clear understanding of the real value it delivers. Failing to understand this can lead to gaps in processes and missed opportunities to maximise on the value of digital transformation.

The key to the success of any digital transformation project lies in the data. Government departments can go beyond technology upgrades and transform their entire operating model with the right data. However, turning data into value requires government departments to have the right underlying technology in place to extract insights from that data.

ELEVATING GOVERNMENT DEPARTMENTS WITH DATA-DRIVEN TECHNOLOGIES

By taking the path of least resistance or choosing solutions purely based on cost, government departments can miss out on the potentially revolutionary capabilities that would let them turn data into value quickly and relatively easily. Comparatively, departments that have a good understanding of how data-driven technologies can help them to achieve greater insights can ultimately deliver more streamlined processes and results by instead deploying solutions that can more seamlessly integrate into the technology stack and deliver the processes and tools they need, as well as delivering on budget.

For example, government departments can gain significant value from SAP S/4HANA's data analytics capabilities. However, it's essential to set the expectations clearly and

upfront in the project to get the most out of the move. While this can determine the type of implementation the department chooses and, in turn, affect costs, it will also dramatically affect the return on investment that the department achieves as a result of the implementation. As such, it's essential to spend time on due diligence before setting a migration plan in play.

FOUR WAYS GOVERNMENT DEPARTMENTS CAN MAXIMISE THE VALUE OF DATA

To gain maximum value from transformational projects, government departments must understand what measurable results they want to see from the initiative. This helps to determine what kind of data and analytics should be used. To achieve this, departments must start with the end in mind or risk a failed project. And, above all, it's essential to focus on maximising the department's ability to extract value from data.

This can be achieved in four ways:

1. DATA STORAGE STRATEGIES

Data storage strategies must include ways to easily access and work with that data. Corporate data lakes provide one way to aggregate data from various systems to deliver a more comprehensive, overarching view of data that can help drive data-driven operations and decisions. Examples include predictive analytics that let businesses make smarter decisions, faster, as well as Internet of Things (IoT) applications.

2. DATA ARCHIVING AND DECOMMISSIONING OF LEGACY SYSTEMS

Data has a shelf life and there comes a time when it needs to be archived. Legacy systems may need to be decommissioned, especially in the case of a merger or acquisition or a system upgrade or transformation. Data can't simply be deleted; it usually needs to be retained for a set period under legislation. Therefore, government departments need to ensure they're moving outdated data to a data lake. This way, the department can still access and manage that data without incurring high costs associated with keeping legacy systems running.

3. DATA SECURITY AND PRIVACY

Digital transformation projects can open up data to the risk of being lost or hacked. It's essential to put data protection measures in place to safeguard data during the transformation process. Data migrations can create considerable costs and risks, especially in the context of a department merger. Data handovers and migrations must be managed properly to avoid data privacy issues.

4. END-TO-END DATA LIFECYCLE MANAGEMENT

As government departments work with different types of data across the entire departmental ecosystem, the vast volume of data can quickly spiral out of control. This can lead to risks in terms of data privacy, access and governance. It's essential to manage the end-to-end data lifecycle with a solution that covers archiving, management and decommissioning of data to maintain compliance and maximise the value of the data that is used to drive decision-making.

By automating data migration and management processes, government departments can reduce risk and make data more accessible for decision-making and transformation projects. However, departments need to understand how to use data for analytics using innovative data science applications such as machine learning and artificial intelligence to maximise the value of data.

Managing data effectively takes a clear strategic approach and the right technology. Applying automation where possible can help minimise the burden on government departments while they leverage data for greater value. It's important to choose a solution that reduces complexity along with a provider that is an expert in managing data transformation projects that help government departments reach their ideal outcomes.

Data Center Security to Combat Cybercrime Break-ins

George Moawad, Country Manager ANZ, Genetec

Data centers are at the core of most business operations today. With servers connected through networks and communication equipment, they allow organisations to store, transfer, and access digital information. While the kind of data they protect and manage can vary, it is safe to say that it is often important and sensitive.

Naturally, with the increased threat of cyberattacks, the majority of attention for data centers is often on the IT elements of cybersecurity. However, there's a new threat vector that's coming into the spotlight: physical security.

While video surveillance, access control, alarms, communications, and more are often considered bastions of security, it might seem ironic that these physical security solutions designed to protect people and property can provide a simple entry point for cybercriminals and ransomware attacks.

A lingering but erroneous view is that only limited threats can be made through a physical security device, such as the ability to remotely stop the video feed from a camera. However, most cyberattacks on physical devices such as cameras can find their way through the network to block access to critical applications, lock and hold files for ransom, or steal personal data, and IT has limited visibility until after the damage had been done.

All physical security devices — from security cameras, to access control readers, and alarm panels — are IoT devices that run software that could be exploited by attackers and should be considered critical network devices. That means they need to receive a high level of protection and monitoring for operations and cybersecurity.

Ensuring that these devices are running on the latest firmware and that they aren't using default passwords can eliminate many of the risks associated with device vulnerability.

It sounds straightforward, but an analysis by Genetec found that too many security cameras offered this opening for attack. According to the company's study, nearly seven in 10 cameras had out-of-date firmware.

Additionally, now is the time to actively explore how physical security and IT departments can be brought together into a single team to develop a coordinated strategy for hardening systems based on a common understanding of risk, responsibilities, strategies, and practices.

An integrated security team can review how to improve security monitoring across all network-connected physical security devices, strengthen protection measures for these devices, implement encryption on video streams and data, enhance access defences with multifactor access authentication and improve updates management.

It's also worth considering unifying cybersecurity and physical security devices and software on a single platform, with centralised management views and tools.

The most appropriate is an open architecture that will support a cloud-based or hybrid deployment of security solutions, as well as flexible integration options for future devices and management systems.

Essentially, it's all about layering security, managing the overlapping perimeters of IT and OT to help reduce security risks, improving decision making, and enhancing compliance.

Genetec™

Genetec Australia Pty Ltd
www.genetec.com

Data Transformation & Migration — A business imperative to transform challenges into opportunities

Digital transformation has changed the way we do business over the last two years, ushering in a digital-first world fuelled by an increasingly digital-first economy. The most significant impact of digital transformation is the way it has changed how we use data and analytics to inform and guide our decisions.

Data helps organisations understand their customers, generate new leads, and improve their bottom line. To stay competitive in the constantly evolving world of data, businesses must transform collected data into actionable insights that can be used to make informed decisions. This aligns to the Australian Government's ambition to be among the top 3 digital governments in the world by 2025 and some of their efforts in developing a government architecture to provide a "personalised experience that is stable, secure, reliable, and ultimately anticipates the needs of every user."

As a global leader in Enterprise Data Management, Syniti previously partnered with SAP to successfully deliver SAP data initiatives for thousands of clients within ANZ. Not only does SAP resell Syniti software such as SAP Advanced Data Migration by Syniti, but they also offer a wider range of accelerators to deliver customer SAP programs predictably and reliably.

With enterprises at the fore, emerging technologies have created great impact on product and service production and consumption, resulting in over 65% of Asia Pacific's GDP being digitalised by 2022. However, increased integration and use of digital technology have presented companies with an abundance of data that they struggle to store, manage, and analyse. The need for data transformation and migration solutions has thus never been greater, and has created demand for data-driven solutions that can help companies clean, organise, and extract value from their data.

What is Data Migration

Data migration sees the moving of data from one system to another — involving a change in storage and database or application. Common causes of organisations migrating data are the desire to move to a newer system, upgrade current systems to newer versions, or to better support the organisation's needs. Regardless of the exact purpose of data migration, the goal is generally to enhance performance and competitiveness among other benefits such as:

- **Agility** — As technology evolves, there is a need to upgrade to the best possible platform or application. The agility of seamlessly transferring data across different platforms and applications serves as an asset.
- **Cost savings** — Moving data to the cloud, for example, reduce costs on both hardware and labour. Extract, Transform and Load (ETL) tools move data to a cloud data warehouse, allowing organisations to cut data storage costs.
- **Collaboration** — Breaking down data silos ensure better collaborations between departments, and provide visibility into processes across the organisation.

Less successful migrations can produce inaccurate data that contains redundancies and unknowns — even when source data is fully usable and adequate. Existing issues in


© StockAdobe.com/au/andrankl23

the source data may also be amplified when brought into a new, more sophisticated system.

How Does Data Transformation Play into Data Migration?

Data transformation makes data more organised, making it easier to use and comprehend for both computers and humans. This involves processes like data integration, data migration, data replication, and data wrangling. Without data transformation, integrating and moving data across sources will be challenging. Apart from the immediate financial impact, poor data quality or siloed complex data can lead to ill-informed decision-making in the long run.

Successful data transformations can yield enormous benefits, and the value of that accurate data only grows over time. Many organisations, however, struggle to capture real value from their data programs and thus see scant returns from investments totalling hundreds of millions. Without a clear inventory of available data, data users can spend between 30–40% of their time searching for data and 20–30% cleaning it.

Syniti Knowledge Platform and Syniti Migrate

Selecting the right data management platform that considers your organisational needs is crucial. It should simplify your transformation journey, and deliver advanced enterprise data migration, data management, governance, and analytics capabilities all with one unified, cloud-based solution. Thankfully, there are tools available today to automate much of this transition and migration. Comprehensive solutions like the Syniti Knowledge Platform have a proven reputation for reducing transformation risks with a targeted, data-driven approach to upgrading systems.

Syniti Knowledge Platform helps customers avoid the complexity, sprawl, and cost of multiple systems — by delivering a single, tightly-integrated solution with all necessary functions for frictionless data migrations in one location. Capabilities include migration-specific tooling, powerful data scanning and profiling, data replication, data cataloguing, data matching and deduplication, data quality, real-time project and data analytics, and built-in best practices.

In collaboration with SAP, Syniti also previously announced a premier service offering for customer migration to SAP S/4HANA, utilising a selective data transition approach with SAP Advanced Data Migration by Syniti. This offers SAP customers a trusted, flexible, and efficient way to migrate — whether on-premise or in the cloud. Research indicates that clients using SAP Advanced Data Migration by Syniti experienced significant business value, including:

- 303% three-year return on investment with an average eight-month payback on investment
- 46% faster completion of data migration projects
- 96% reduction of unplanned downtime

As part of their suite of solutions, Syniti also offers a fully cloud-based version of the Syniti Advanced Data Migration called Syniti Migrate, delivering frictionless enterprise data migrations in the simplest or the most sophisticated of scenarios.

In the past Syniti data migration platform has proved beneficial for organisations. For example, property Developers Australand, headquartered in Melbourne, underwent a major refurbishment of its IT systems when it switched from an existing ERP platform to SAP. As Australand's business grew, its existing IT systems became increasingly fragmented and unstable. A decision was made to move to SAP, and at the heart of that undertaking was a complex data conversion effort lasting 14 months. Using Syniti's data migration platform, the project ran smoothly, on time, and provided a rolling graphical update of the progress.

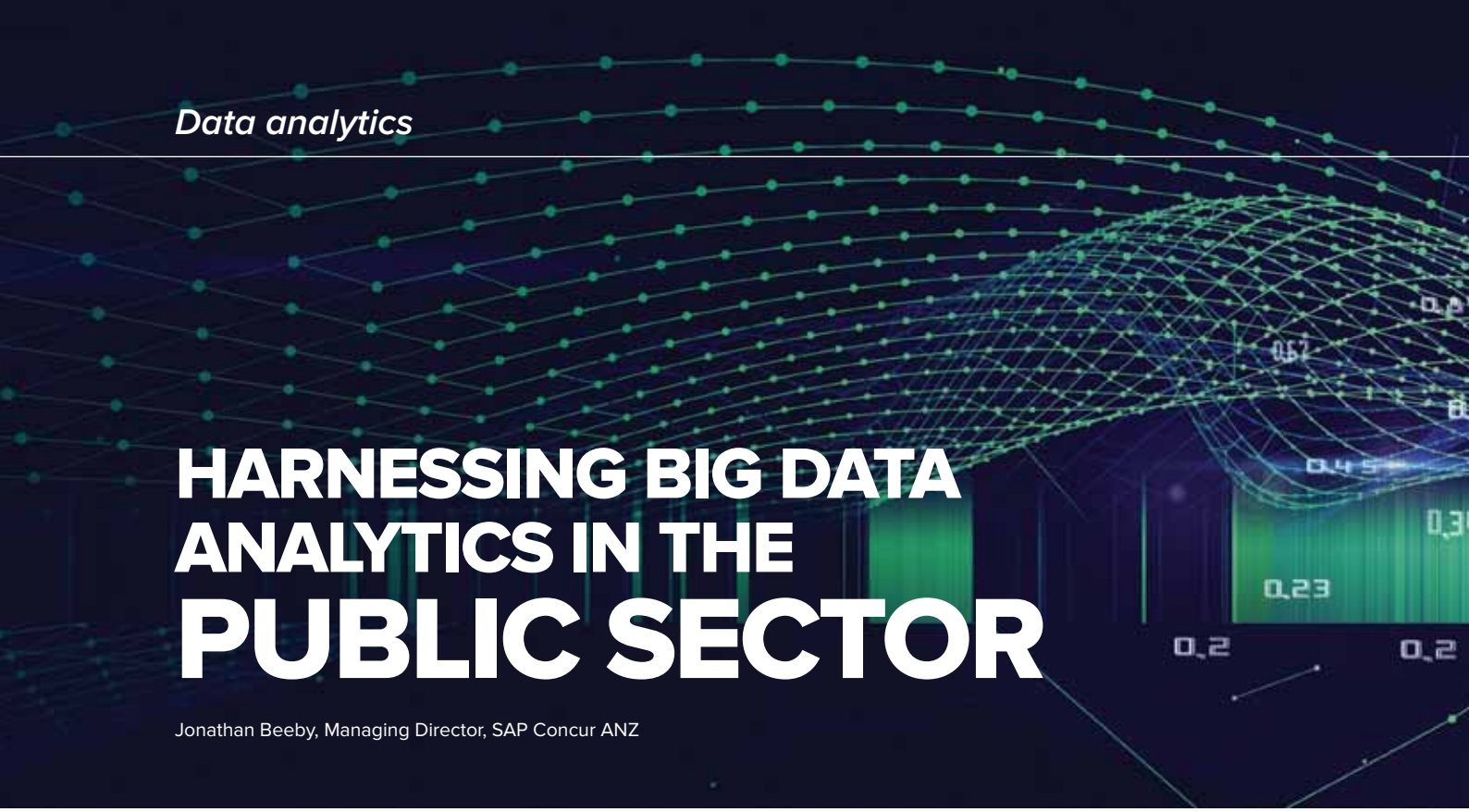
How will this pave the way for organisations in the new digital age

The digital world has shifted, making data migration more critical than ever. However research has revealed that ANZ organisations are lagging in modernising their mainframes, with only 16% having completed or nearing completion of their mainframe-to-cloud migration.

Data transformation and data migration are required to keep pace with the new digital age. The rapid pace of change in the digital world creates new opportunities and challenges that require new skills and expertise. Modern systems and infrastructures are built to enable modern methods of working — whether it's flexibly, remotely, or across a variety of devices. Data migration, done with the right specialised tools and teams, not only improves productivity and performance, but also ensures security, accessibility, and efficiency. Together, data transformation and data migration allow organisations to adapt and evolve to the changing landscape of the digital world, enabling them to deliver better services to their customers and increase their profitability.

Syniti

Syniti Australia Pty Ltd
www.syniti.com



HARNESSING BIG DATA ANALYTICS IN THE PUBLIC SECTOR

Jonathan Beeby, Managing Director, SAP Concur ANZ

AUSTRALIAN PUBLIC SECTOR ORGANISATIONS BEAR THE RESPONSIBILITY OF STORING AND PROTECTING MASSIVE AMOUNTS OF DATA. HOWEVER, MANY GOVERNMENT AGENCIES ARE FAILING TO ACHIEVE THE FULL POTENTIAL AND VALUE OF THAT DATA WHEN IT COMES TO IMPROVING OPERATIONAL EFFICIENCIES, REDUCING COSTS, AND ENHANCING EMPLOYEE AND CUSTOMER EXPERIENCES.

Due to legacy processes, government agencies struggle with simply managing their data, so they are missing the opportunity to use it to benefit their agency, its employees and customers.

As well as optimising day-to-day operations, big data can deliver significant value in guiding the government response to major events such as pandemics, economic disruptions and natural disaster response.

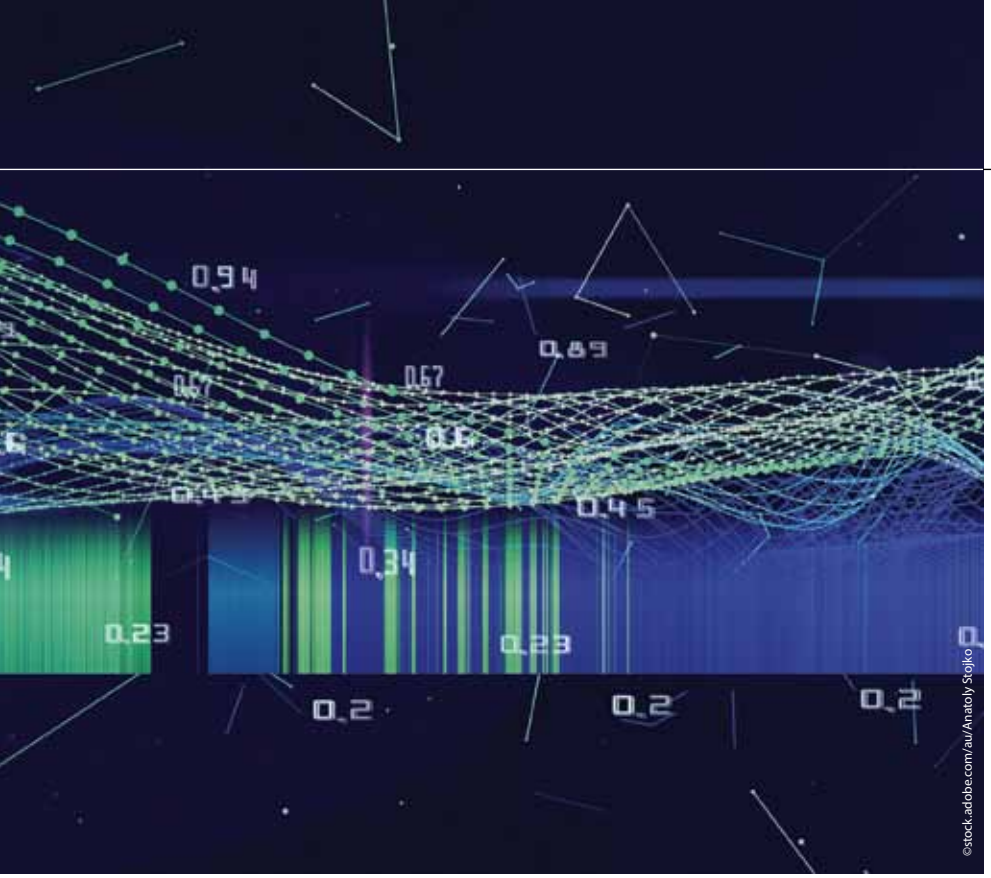
In an attempt to address big data challenges, the federal government has implemented numerous measures that aim to improve the way data is shared and released. These measures include:

- the Consumer Data Right, which gives consumers more control over their data and transaction activities;
- an ethics framework in partnership with industry and research organisations to address the use of data, with a focus on artificial intelligence (AI) and machine learning; and
- legislative reforms to streamline the management of public sector data while maintaining the protection of data privacy.

One of the biggest challenges for government agencies is how they can effectively manage the collection and storage of vast volumes of structured and unstructured data, which continues to double every three years.[1] Legacy manual processes have left public sector organisations with siloed data storage. This has resulted in double handing of tasks and workloads, causing duplication that impacts cost and operational efficiencies and affects customer and employee experiences.

Public sector agencies were gradually automating backend processes before COVID-19, and the shift to remote work caused by the pandemic has accelerated the need to centralise, organise and leverage data across organisations.

In the fast-paced digital business landscape that has emerged in the past two years, manually sifting through vast data files and organising them in a way to improve decision-making is now too much



©stock.adobe.com/au/Anatoly Stojko

for humans to handle. This is where AI becomes the key to taking working hours out of the equation and instead adding accuracy, unification, personalisation and risk tolerance, with the added bonus of predicting upcoming trends.

HOW DATA IMPROVES GOVERNMENT DECISION-MAKING

Due to the pure speed of the capture, storage and consumption of big data, extracting information from it manually, or even with traditional software, is almost impossible.

Government organisations are now realising that leveraging automated processes to input and analyse data reduces the risk of human error and fraud, and breaks down information siloes.

This delivers real-time data analytics and information insights that help agencies improve business efficiencies to better meet customer service expectations.

For example, financial processes driven by artificial intelligence are letting government agencies centralise, organise and access financial data securely in real time. This facilitates a more streamlined flow of information that helps public sector agencies make decisions based on real-time insights.

In turn, it delivers much greater levels of transparency that build trust with community stakeholders. More specifically, in areas such as fraud detection, automated finance solutions use big data to help government agencies uncover the potential for criminal activity early. This helps guide decision-making to mitigate the risk of data breaches and financial loss.

USING BIG DATA TO IMPROVE CUSTOMER EXPERIENCES

How government agencies acquire and leverage comprehensive, relevant data to drive smarter decision-making is key to improving customer interactions.

In the digital economy, both public and private sector customers expect highly responsive and personalised services in near-real time. This includes expecting government agencies to anticipate community needs, even before the community has expressed those needs.

Big data management gives public sector agencies necessary information to clearly review the current performance of government programs, and identify where there may be gaps or opportunities to enhance customer experiences.

E-invoicing is one area where government agencies can achieve quick wins with suppliers and customers, by significantly improving invoice processing times. This has a direct impact on returning and reinvesting cashflow back into communities faster. The data collected through e-invoicing processes can also be used by public sector agencies to identify where the most money is being invested, and where there may be opportunities to redirect funds to projects that better meet community needs.

The fastest and most effective way to harness and capitalise on big data in the public sector is by starting with financial processes such as travel, expense and invoice management. These processes sit at the core of every government agency and can provide the easiest and best opportunity to use automation to maximise big data benefits.

To achieve sustainable data management outcomes, and reduce costs, public sector agencies should seek a big data management expert that has proven success in automating Australian government processes. This approach will achieve the highest level of success, with minimal risk, for government agencies as they embark on their digital transformation journey.

[1] https://www.researchgate.net/figure/Global-growth-trend-of-data-volume-2006-2020-based-on-The-digital-universe-in-2020_fig5_274233315

Public sector strategies for 2022

After two especially challenging years for public sector organisations, the pressure isn't getting any lighter. Many organisations are still managing the effects of the pandemic, while tackling age-old challenges such as tightened budgets, limited resources and growing demand from citizens.

Too often, public sector professionals take the growing burden of these sector-wide pressures. In our recent survey of more than 100 professionals in the sector, more than half said they'd taken on extra responsibilities to support their organisation during the pandemic — and 92% also said these new responsibilities had increased their workload.

If public sector organisations are to retain their skilled professionals and boost productivity in their teams over the next year, they'll need to consider where they can better support their employees in their day-to-day roles.

Admin workloads contribute to public sector stress

Administration tasks are a crucial part of almost every public sector role, helping ensure services run smoothly, teams work efficiently, and public needs are met.

But as demand for public services scales, the administration workload scales with it. More than three-quarters of respondents said they'd experienced work-related stress at some point in their careers — and 67% claimed their admin workload contributes to their stress.

Unexpected events like the pandemic and natural disasters only increase these workloads further, often putting huge additional pressure on public sector professionals at short notice. For example, the Australian Public Service Commission reported that the higher demand on its services during the pandemic was largely met through longer hours, less leave, and reliance on proven performers.

Of course, many events like these can't be predicted and solved before they happen. But by addressing some of the challenges in professionals' everyday responsibilities, public sector leaders can equip their teams with the tools they need to respond effectively.

Public sector professionals' typing time is holding them back

One of the biggest workload challenges public sector professionals face is the sheer amount of time spent typing. The survey revealed that 70% of public sector employees spend at least four hours a day typing for work, with 58% spending a further hour or more typing for personal reasons once the workday ends.

Looking more closely at this time spent typing, the survey revealed that report writing took up the most time in public sector professionals' roles, closely followed by internal correspondence. Filling out forms and note taking also made the top five typing tasks.

These tasks can't just be removed from the working day, and over a quarter of public sector professionals reported the struggle to complete them quickly was due to their typing speed. 40% of respondents said their typing speed was either average — at 40 words per minute — or slow.

So with public sector professionals at their typing limits, and workloads showing no signs of slowing down, how can organisation leaders ease the burden on their employees?

Speech recognition offers a solution — but it's misunderstood in the sector

Some forward-thinking public sector organisations are helping their employees spend less time typing with speech recognition solutions, enabling professionals to complete documentation faster using speech-to-text.

However, many public sector organisations have been slow to adopt the technology — mostly due to a lack of experience with professional-grade speech recognition tools.

The survey revealed that despite all respondents stating they've used voice-based technologies of some kind professionally, only 13% were using speech recognition where their spoken words appeared on the screen immediately.

In many cases, the reluctance to embrace speech recognition professionally was due to the respondents' previous experience with tools that weren't fit for purpose. In fact, 67% of public sector professionals said the speech recognition tools they've encountered in the past struggled to recognise the specialist terms they use at work.

Public sector leaders do have an opportunity to help their teams complete administration workloads more efficiently and deliver more effective services — but if they're to convince their professionals of speech recognition's potential, they'll need to find the right solution.

Learn how the right speech recognition tool can help your team

Explore the report to see the complete results from the survey, and understand the administration pressures public sector professionals are facing today.

You'll also get an insight into how professional-grade speech recognition tools like Dragon Professional Anywhere can help your teams reduce their reliance on typing, tackle their admin tasks more efficiently, and focus on delivering standout services to the Australian public.

NUANCE

Nuance Communications
www.nuance.com/governmentreport

EVOLVING GOVERNMENT DIGITAL SERVICES BEYOND THE PANDEMIC PATCHWORK

Dustin Laidsaar, strategic business consultant, Avaya

Government digital services have undergone considerable transformation in the last three years. While agencies have maintained a digital presence to varying degrees for some time, it was only at the onset of the COVID-19 pandemic that investment boomed.

With Australians impacted at unprecedented levels, state and federal governments were forced to expedite the online delivery of programs like JobSeeker and JobKeeper, stand up check-in systems, and make available an array of resources and support.

Now it's a matter of turning digital patchwork into sustainable digital services, underscored by reliability, accessibility and uncompromising attention to customer experience and privacy.

According to Irma Fabular, research vice president at Gartner, "The disruptions caused by the pandemic have also reinforced a key digital government tenet, which is public policy and technology are inseparable".

The analyst firm now forecasts Australian government sector IT spending to surpass $15.5 billion in 2022, an 8.8 per cent jump on the year prior. A majority (72%) of that investment will go towards software and services, motivated by the desire to "improve responsiveness and resilience of public services", the firm says.

Digital can no longer be treated as only something we should have because technology just so happens to be popular. It must be regarded as a critical asset in everyday Australia, and policy makers need to connect the digital dots to meet the expectations of taxpayers.

The importance of this approach was again highlighted during the recent east coast floods, as tens of thousands of Australians displaced by the natural disaster required financial assistance in the aftermath.

"Agencies must also ensure their digital services cater to Australia's plethora of demographics."

The appetite for digitalisation is a sentiment reflected in Services Australia's corporate plan. The agency lists 'customer services delivery' and 'technology and transformation' as two of its three key activities for 2021–22. A major performance measure for the latter is "to drive the agency to ensure that our digital services are stable and available for customers to use when they need them".

Meanwhile, Service NSW proved particularly innovative in developing new and refining existing services, with its mobile application as the centrepiece. Digital driver's licences were among the early tools to become available through the app, and features such as COVID Safe Check-in, voucher and support services have been introduced since, with NSW Minister for Customer Service and Digital Government Victor Dominello consistently pushing for further additions.

DIGITAL SUCCESS RESTS IN CITIZEN EXPERIENCE AND TRUST

With millions in taxpayer funds to be dedicated to digital services in coming years, it's critical for those investments to be made with citizen experience and trust at the forefront. It must be quick, easy and convenient to access information and help, and Australians need assurance their private data will not just be kept onshore, but that it won't be viewed or used without their consent.

Agencies must also ensure their digital services cater to Australia's plethora of demographics. For example, older citizens can't be forced to get lost in online resources when there can be the option to have a human contact them proactively to overcome technology challenges. In addition, a variety of accessibility and language options need to be built in to ensure no community becomes isolated in our digital economy.

Creating this type of citizen-focused experience means balancing internal and external investments with emphasis on modernisation and systematic data-sharing across all levels of government, according to Dean Lacheca, a senior director at Gartner.

In simple terms, technology spend must be geared towards improving the quality of life for the staff providing services as well as giving Australians the best digital experience.

Like consumers of any brand, citizens expect to be able to engage with organisations through their preferred channels, on their own time, and ideally without needing to go through multiple departments to have their issues resolved. By equipping government employees with comprehensive capabilities — including digital sidekicks powered by machine learning and artificial intelligence — they will actually have the means to meet those expectations.

Lacheca also says: "This requires the adoption of widespread anything-as-a-service policies, adaptive security programs and an increased level of composability across government solutions."

The composability element is particularly pertinent; it fosters a technology backbone that allows agencies to be flexible and adaptable in the applications and services introduced into government, whether it's for the benefit of public sector workers at the forefront of customer services, or the digital assets through which Australians interact.

With demand for government services through digital channels at a record high, state and federal agencies must build on the often ad hoc efforts of the last three years. It won't happen overnight, but there is a tremendous opportunity to establish a more uniform and consistent public service, led by what citizens want and underscored by trust.

Promoting IBC and Public Safety

In a world where cars can drive themselves and identities can be verified with a retina scan, it seems almost inconceivable that people are still struggling to use their mobile phones indoors — especially considering the expanding global market for smart buildings, which is expected to reach more than $37 billion by 2023 according to the Globe Newswire.

Ironically, new buildings continue to be plagued by poor signal propagation, because of the very same features that brand them eco-friendly and attract potential occupants: low-emissivity (Low-E) glass, galvanised steel, metal roofs, and concrete walls are but a few common culprits. In the case of older properties whose designs simply did not take mobile coverage into consideration, building materials such as stone, concrete, and brick are notorious signal blockers, especially in densely populated urban areas.

We depend on our Public Safety Agencies to protect the Australian community, and they do it every day. Around the country over 550,000 women and men work selflessly to uphold and protect our Australian way of life. Communication is critical to that work. Smart, strong, and fast systems enable better decisions that save lives. Over 6.3 million Triple Zero (000) calls are made every year in Australia. Each one of those calls triggers a complex systematic response underpinned by mission-critical grade radio communications. Put simply, these communications systems have been built not to fail.

"If someone is attacked in the basement carpark of a building and can't call 000 because there was no mobile phone signal, the body corporate managing the building could be sued."

If someone is in distress and unable to place an outgoing call, first responders will not be aware there is an emergency that requires their response. For this reason, the Safer Buildings Coalition defines three pillars of in-building safety communications:

- Mobile 000 calls must get out with location accuracy.
- Mobile Mass Notifications must get in.
- First Responder communications must work.

If a building cannot deliver these basic characteristics, the environment puts the occupants and the property itself at risk.

Anyone who has ever tried to place a call from an elevator is not surprised that indoor coverage can be much worse than outdoor coverage. And the deeper into a building you go, the worse the signal typically gets.

Penetrating walls is difficult for a mobile signal, though some of the RF spectrum blocks that the Australian mobile network operators have licensed are better for this task than others. Low band (longer wavelengths) spectrum tends to be much better at penetrating concrete and brick than high band (shorter wavelength) spectrum, such as 5G.

5G has been hailed as a saviour for those 'screenagers' amongst us, but the benefits of faster data may well be offset by an increase in problems caused by poor coverage due to the reduced ability of this bandwidth to penetrate. It is very much a wait and see approach to determine how much of a coverage problem 5G will actually cause.

The Federal Government is making a significant investment to improve wireless network coverage in rural areas; the Government has committed $380 million to the Mobile Black Spot Program to invest in telecommunications infrastructure to improve mobile coverage and competition across Australia. However, poor wireless coverage can be experienced in big cities as well. The networks were originally designed to work well in a "mobile" environment — namely outdoors while in moving vehicles or walking. As indoor usage has grown, the networks have densified, and greater efforts have been made to provide a signal strong enough to penetrate buildings. Providing high-quality indoor coverage is much more difficult.

Understanding which buildings fall short of providing adequate service can assist local governments in working with building owners and mobile operators to make needed improvements.

In Australia, there is no building code, regulation or legislation that mandates In-Building Coverage (IBC) to support operational communications.

For building owners, the benefits of providing reliable high-speed wireless coverage are clear: apart from the OH&S liability associated with poor IBC, there is increased tenant retention and recruitment rates, increased workforce productivity, and more attractive property for visitors. Many building owners and operators believe having a strong indoor wireless network increases the value of their buildings by as much as 28%, according to CommScope.

For more information on In-Building Coverage solutions talk to our team of experts today on 1300 769 378, email sales@powertec.com.au or visit www.powertec.com.au to view the full range of products.

powertec
WIRELESS TECHNOLOGY

Powertec Wireless Technology Pty Ltd
www.powertec.com.au

DISRUPTIONWARE: PREPARING FOR NEW AGE CYBER ATTACKS

Ram Vaidyanathan, IT security evangelist, ManageEngine

Cyber attacks continue to increase in both frequency and impact, as attackers use more sophisticated and dangerous methods. One of the most common types of attack uses ransomware, though it is just the top of the cybercriminal iceberg. It is easier than ever to launch an attack on an organisation, even without high-level knowledge.

Cyber attackers have a new weapon in their arsenal: disruptionware. A whole new class of cyberthreat, disruptionware aims to sabotage critical networks and operations, making it exceptionally damaging. As it grows in popularity, it's developing into a significant cyberthreat that is considerably more malicious. Unlike ransomware, which is designed to encrypt files and render them unusable until a ransom is paid, disruptionware targets its victims' information and operational technology networks. It attacks the integrity of data, systems, and networks along with the physical infrastructure.

Disruptionware has gained more significance since the outset of the pandemic because of the shift to remote working environments. It is a significant concern for the safety of citizen and government data and for the security of critical systems. This emerging threat cannot be reversed like ransomware and can completely cripple networks.

DECREASING THE RISK

Combating disruptionware requires departments to fortify baseline cybersecurity with additional measures:

1. Implement a backup system that stores multiple iterations of data both on-premises and in the cloud and ensure backups are airgapped.
2. Assemble an internal or outsourced team that can monitor for unauthorised access attempts into critical networks with a detailed incident response plan.
3. Identify assets and ascertain the criticality of data stored on them. Prioritise protection accordingly.
4. Leverage security analytics and event management solutions that detect the adversarial techniques that malicious actors rely on for obtaining initial network access.
5. Set up patch management routines to keep security up-to-date.
6. Use threat intelligence feeds that can secure against emerging threats.

It is also vital to create human firewalls to help prevent cyber attacks. A focus on educating staff on cyber attacks and defensive habits will reframe attitudes around cybersecurity and establishing best practices.

Recovering from a disruptionware attack can be complex. Even if government agencies can remove the adversary from the department's operational technology, there may be too much damage to recover from, which is why prevention is always better than cure. It's essential to devise and implement an effective government agency response plan that will help minimise the effects of a disruptionware attack and ultimately allow operations to continue.

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

Rittal – The System.

Faster – better – everywhere.

Discover more:
www.rittal.com/rimatrix-ng

RiMatrix Next Generation

Modular is the way forward

Rittal's system platform RiMatrix NG offers flexible, powerful, future-proof data centre solutions for a secure, scalable infrastructure tailored for your business processes.

ENCLOSURES | POWER DISTRIBUTION | CLIMATE CONTROL | IT INFRASTRUCTURE | SOFTWARE & SERVICES

FRIEDHELM LOH GROUP