govtech review

ONLINE OVERHAUL
SHARRYN NAPIER ON DELIVERING BETTER ONLINE EXPERIENCES

BUILDING TRUST
WHILE SHARING DATA

DELIVERING BETTER
ONLINE EXPERIENCES

CLOUD RELUCTANCE
CREATES DATA RISKS

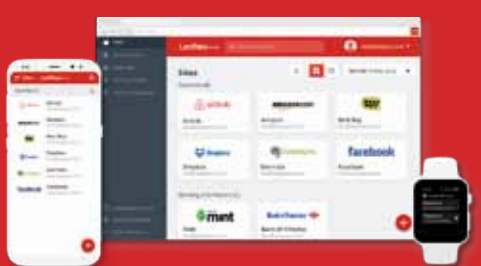
Q1 2021
PP100021607

LastPass •••|
by LogMeIn

Protect and empower the digital identities of your modern workforce.

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

www.lastpass.com



03.09.2020/PDF/LMI1309

Q1 2021

INSIDE

FEATURES

6 | Managing data breach risk in the public sector

Australian Government agencies have obligations to take reasonable steps to protect personal information.

14 | Delivering an improved online user experience

Steps to promote a better user experience now and into the future.

18 | Crisis forces changes to SaaS contract negotiations

Cloud-based centres can facilitate better training and guidance for employees, improve caller interactions, increase efficiency and reduce costs.

20 | Data availability and transparency

Data is the foundation of any customer-centric business, including the Australian Government.

24 | Transforming contact centres via cloud technology

Cloud-based centres can facilitate better training and guidance for employees, improve caller interactions, increase efficiency and reduce costs.

28 | Personalisation in government services

A study has found that 76% of Australians are more likely to use government websites if they are personalised.

26 | Cloud reluctance creates data risks for government

30 | Audits find some SA councils have lax security.

32 | Harnessing data and analytics for citizen health and wellbeing

36 | Public sector cloud adoption guide

38 | Secure IT disposal

38 | Conference calendar

Insider

Building a data-safe public sector

Following the introduction of the Notifiable Data Breaches scheme in 2018, the IT has industry has been alarmed — though certainly not surprised — to see the number of notifications continue to rise. What has been a surprise is that governments had managed to keep themselves out of the statistics. Well, no more.

In the OAIC's report covering July to December 2020, governments make their appearance for the first time. In fact, the public sector made it into the top five sectors for notifiable data breaches. There were 33 reported incidents, 29 of which were put down to human error — only two incidents were the result of a criminal attack. This is very different to the experience of the private sector, where 58% of breaches were the result of criminal or malicious activity.

Data security is a grave issue, and it is one that governments are taking very seriously. In this issue, Connor Dilleen of the Office of the Australian Information Commissioner outlines the policy framework and practical steps that can be taken by everyone involved in all levels of government, to keep citizen data as safe and secure as possible.

Naturally, data is of no use to anyone unless it can be used, and in this issue we're very pleased to have the Interim National Data Commissioner, Deborah Anton, outline the Data Availability and Transparency Bill, the Data Sharing Principles and a Data Sharing Agreement, the latter of which will be a template for government agencies and data users to use when sharing data.

Still on the topic of data, EY's Sonia Sharp also opines on data sharing, with particular emphasis on the human services sector and how its rich data sets can help caseworkers understand the full needs and circumstances of the people they are trying to help. There's plenty of work to be done in making data more usable and less siloed. After all, as Sharp says, "If consumers can find and book accommodation on Airbnb in under a minute, why are our caseworkers spending hours calling around to find placements for at-risk children?"

The other topic that won't go away in the current environment, of course, is the ongoing disruption to workplaces caused by the COVID-19 pandemic. In this issue we present a number of viewpoints on what can be done and which technologies can help, from contact centres to unified communications

Jonathan Nally, 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
Jonathan Nally
jnally@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Colleen Sam, Veronica King

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

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

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

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

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

SOPHOS
Cybersecurity evolved.

Four Key Tips from our Incident Response Experts

Responding to a critical cyber incident can be an incredibly stressful and intense time. While nothing can fully alleviate the pressure of dealing with an attack, understanding these key tips from incident response experts will help give your team advantages when defending your organisation.

01. React as quickly as possible

There are a few reasons why teams may take too long to react. The most common is that they don't understand the severity of the situation they find themselves in, and that lack of awareness leads to a lack of urgency. When an organization is under attack, every second matters.

02. Don't declare "mission accomplished" too soon

Successfully removing malware and clearing an alert doesn't mean the attacker has been ejected from the environment. Our Incident response teams ensure they address the root cause of the original incident, and having remediated thousands of attacks, know when and where to investigate deeper.

03. Complete visibility is crucial

While navigating an attack, nothing makes defending an organisation more difficult than flying blind. It's important to have access to the right high-quality data, which makes it possible to accurately identify potential indicators of attack and determine root cause. Effective teams collect the right data to see the signals, can separate the signals from the noise, and know which signals need to be prioritized.

04. It's OK to ask for help

No organization wants to deal with breach attempts However, there's no substitute for experience when comes to responding to incidents. This means that the IT and security teams often tasked with high-pressure incident response are thrown into situations that they simply don't have the skills to deal with — situations that often have a massive impact on the business.

How Sophos can help?

Triage, Contain, and Neutralize Active Threats 24/7

MTR Sophos Managed Threat Response

Provides 24/7 threat hunting, detection, and response

EDR Sophos Endpoint Protection and Response

Leading Endpoint and Server Protection with EDR

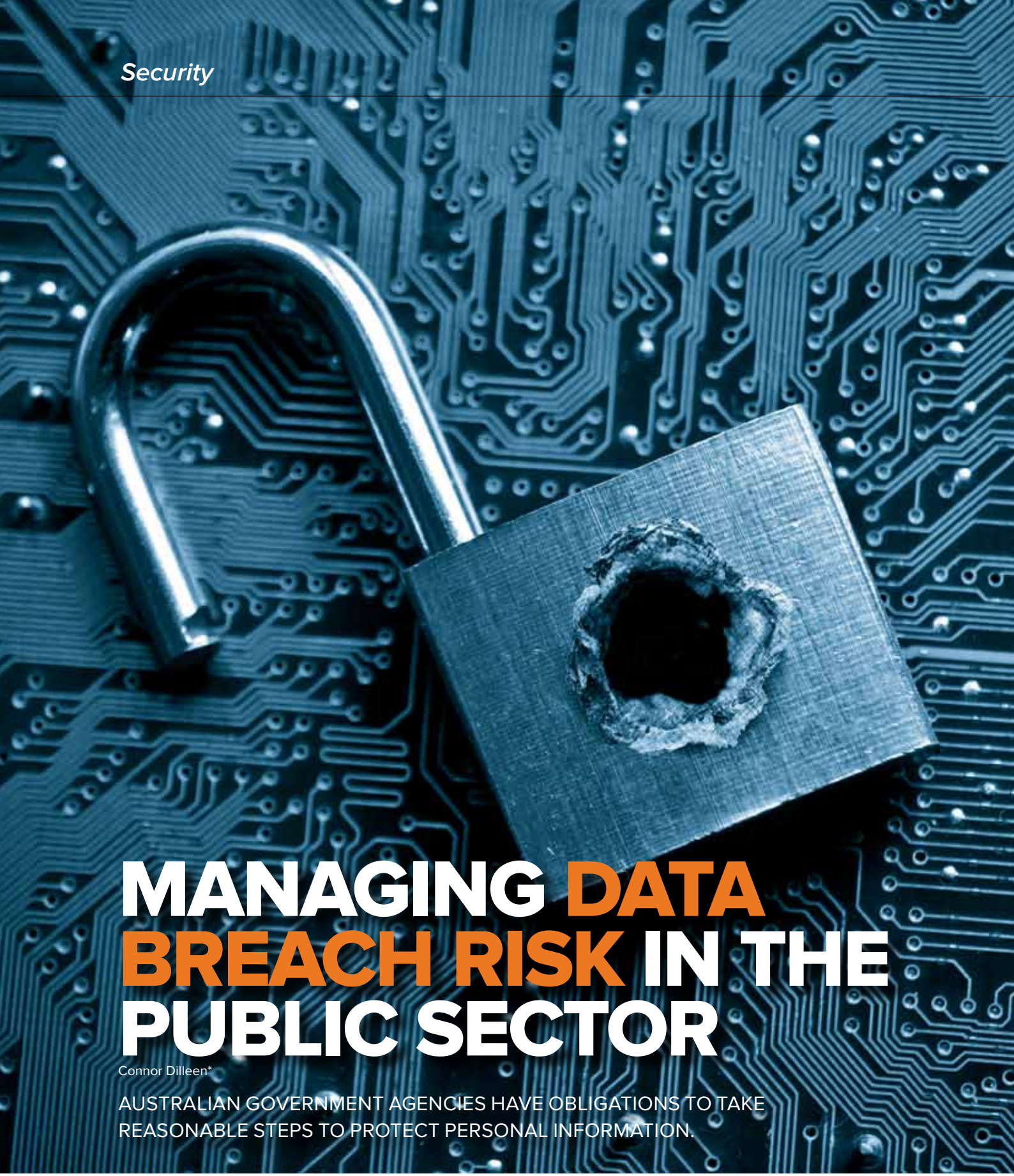
RR Sophos Rapid Response

Immediate response to active threats

Cld Sophos Cloud

Optimize cloud costs and improve security

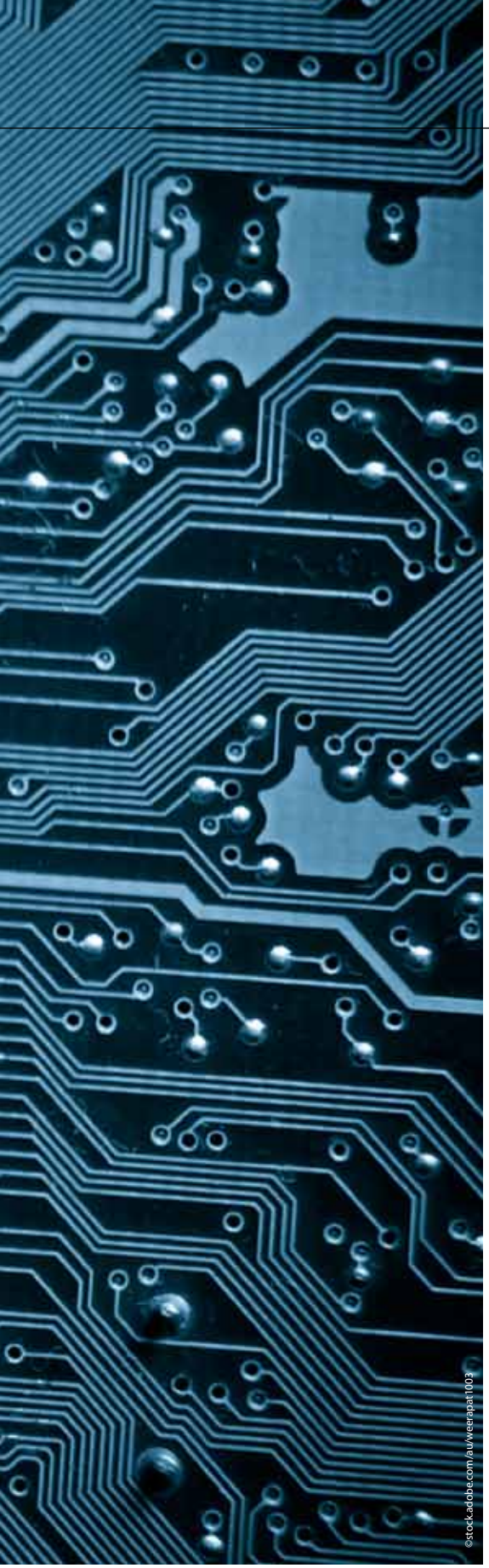
Find out how: www.sophos.com



MANAGING DATA BREACH RISK IN THE PUBLIC SECTOR

Connor Dilleen*

AUSTRALIAN GOVERNMENT AGENCIES HAVE OBLIGATIONS TO TAKE REASONABLE STEPS TO PROTECT PERSONAL INFORMATION.



Strong data management is integral to the operation of government agencies. Data breaches involving personal information can cause serious harm to affected individuals and, depending on an agency's response, diminish community confidence in an agency's information handling practices and disrupt operations.

The Notifiable Data Breaches (NDB) scheme was introduced in 2018 to drive proactive security practices to protect personal information and to require organisations that experience a data breach and are covered by the Privacy Act — which includes most Australian Government agencies — to be transparent and accountable. An agency that experiences a data breach involving personal information that puts individuals at risk of serious harm must notify the Office of the Australian Information Commissioner (OAIC) and those affected. This ensures individuals can take steps to mitigate harm.

The OAIC recently reported on data breach notifications received under the scheme from July to December 2020. For the first time since the scheme commenced, the Australian Government was among the top five industry sectors to notify data breaches.[1]

Australian Government agencies reported 33 eligible data breaches to the OAIC — 6% of all data breaches notified during the period. Human error was the source of 29 Australian Government data breach notifications (88%), while two (6%) were the result of a malicious or criminal attack and two were caused by a system fault.

These statistics contrast with those for the private sector, where malicious or criminal attack, not human error, is the leading source of reported data breaches. From July to December 2020, malicious and criminal attacks accounted for 58% of notifications across all sectors, with human error causing 38% of breaches.

ADDRESSING THE HUMAN FACTOR

Human error breaches generally result from a failure of process or procedure, or simple inattention to detail.

Of the Australian Government data breaches that resulted from human error, approximately half involved personal information being sent to a wrong person either by email or mail. A further nine resulted from unauthorised disclosure of personal information, either because of a failure to redact documents or from their unintended release or publication.

Australian Government agencies should consider introducing technical and process measures that mitigate the risk of errors of this nature. For example, disabling the auto-populate function for the address field for emails will limit the risk of them being sent to the wrong person. For emails with multiple recipients, warnings for the sender to double check the distribution list and to ensure use of the blind carbon copy feature can help to mitigate the risk of a data breach.

Agencies that store and regularly communicate sensitive personal information should adopt systems and processes that ensure its security at all stages of the information lifecycle and that align with the requirements of the Australian Government Information Security Manual and the Protective Security Policy Framework.

Reports received under the Notifiable Data Breaches scheme have confirmed the use of email for storing and communicating personal information is a privacy risk. Particularly for sensitive personal information,

agencies should consider more secure options, which may include encrypting and password-protecting documents containing personal information, or transmitting them via websites, online mailboxes or drop boxes that provide additional security controls. Agencies should also consider introducing storage limits and archiving mechanisms for email accounts to limit the number of emails that staff retain.

Australian Privacy Principle 10 on the quality of personal information requires agencies to take steps to ensure that any personal information collected is accurate, up to date and complete. As this includes key contact information for individuals, agencies should regularly validate the records and contact details of individuals with whom they are communicating to ensure that correspondence is addressed correctly.

Agencies' privacy and security governance arrangements should also include appropriate training and resourcing to foster a privacy- and security-aware culture among staff. This can be achieved through information security programs that recognise that this is not just an issue for compliance or ICT areas, but for all staff. These programs should be driven from the top down — senior management should actively support and promote good privacy and security practices.

MINIMISING CYBER RISK

On face value our statistics suggest that human error breaches pose the most obvious risk to Australian Government agencies. However, findings by both the Australian National Audit Office and Australian Cyber Security Centre (ACSC) on cyber maturity and resilience in the public sector suggest there is a need for agencies to continually improve how they manage the risk of cyber-enabled malicious and criminal attacks.

According to the ACSC, Australian Government agencies reported 436 cybersecurity incidents during the 2019–20 financial year — 220 of which resulted in "data exposure, theft, or leak". This confirms that Australian Government agencies continue to confront an ongoing risk of data breaches from cyber attacks.

As with human error, agencies should put in place controls and technologies to mitigate the risk of cybersecurity incidents occurring. The ACSC's Essential Eight should be the baseline for agencies.

DATA BREACH RESPONSE

Australian Government agencies must also have effective systems for detecting, containing, assessing, notifying and reviewing data breaches. The capacity of agencies to identify and respond to data breaches promptly and move to notify affected individuals as quickly as possible is fundamental to their ability to meet the Notifiable Data Breaches scheme's requirements and objectives.

From July to December 2020, the Australian Government was at the bottom of the top five industry sectors when it came to the time taken to identify that a data breach had occurred, and the subsequent time taken to notify the OAIC.

Sixty-one per cent of government agencies identified an incident, subsequently assessed to be an eligible data breach, within 30 days of it occurring, compared to 75% across all sectors. And 58% of government agencies notified the OAIC within 30 days of becoming aware of the incident, compared to 78% across all sectors.

These figures suggest that Australian Government agencies should check that they are equipped to ensure an efficient data breach response. An agency's capacity to mitigate the risk of data breaches and respond effectively when one occurs is as dependent as much on work practices and the associated human factor as it is on technological controls. Both must be factored into agencies' processes and plans.

When designing a data breach risk mitigation and response plan, agencies should consider the entire spectrum of the information lifecycle, including what personal information they collect, how and where they store it, how they secure it, how it is transmitted and how long it is retained.

Australian Government agencies have obligations to take reasonable steps to protect personal information. Upholding a consistent, high standard of personal information handling practices to meet expectations for security, accountability and transparency in data breach prevention and management will maintain and build community trust.

** Connor Dilleen is a Director in the Office of the Australian Information Commissioner's (OAIC) Dispute Resolution branch. He leads the OAIC's work program for the Notifiable Data Breaches scheme.*

The OAIC has a range of guidance, advice and resources on data breaches, including a data breach preparation and response guide and a guide to securing personal information.

In addition to notifying the OAIC if a cyber incident results in an eligible data breach under the Notifiable Data Breaches scheme, agencies are encouraged to report the incident to the ACSC through cyber.gov.au or 1300CYBER1.

1. Government statistics in the OAIC's Notifiable Data Breaches reports relate to agencies that are covered by the Privacy Act. The Privacy Act covers most Australian Government agencies. It does not cover a number of intelligence and national security agencies, state and local government agencies, public hospitals and public schools.

HOW TO BOOST DATA CENTRE RESILIENCE AND SUSTAINABILITY

As digitisation and technological advances bring us hurtling towards a new, more integrated future, not all data centre owners will be equally equipped to handle the new levels of operational agility required. However, if risks and shortcomings within existing data centre systems and related management strategies are recognised early enough, stakeholders will improve their chances to engineer a smooth transition to the more dynamic future.

According to intelligence and advisory firm Arizton, the global data centre market will reach $174 billion by 2023. As disruptive IoT technologies create a spike in demand for data centres and as data continues to become more valuable, more sustainable, efficient, adaptive and resilient data centre infrastructures will be needed if owners are to cash in on this growth opportunity.

Users will be looking for data centre owners to implement more diverse approaches to enable their cloud and edge migrations, will look to data centres to help them build stronger partner ecosystems and will expect more support in their efforts to incorporate as-a-service offerings for their customers.

To accommodate these rising marketplace demands, data centre owners will be required to step up performance in these four important areas:

1. Sustainability — The data centre of the future will be expected to both integrate into and accommodate a company's complete upstream and downstream supply chain sustainability data. Above and beyond just tracking company-based emissions, the notion of Scope 3 emissions (or supply chain-based emissions) will need to be monitored, captured, analysed, benchmarked and published.
2. Efficiency — Data centre efficiencies, which often encompass only process and hardware performance efficiencies, will soon have to include human resources, Capex and TCO efficiencies. By instrumenting devices with intelligent sensors, and by adding more digital services and remote monitoring capabilities, data centres will be able to drive more efficient human resources workflows (faster alerting, more precise predictive diagnostics) which will result in far fewer instances of unanticipated downtime.
3. Flexibility — As businesses across the globe scramble to increase flexibility while navigating unorthodox working conditions and unpredictable supply chains, a new mentality for remaining in business has emerged: accelerate your ability to deliver goods and services with speed and precision. As customers adapt to these new marketplace realities, so must their data centre facilities. Much more flexible data centre designs will emerge that allow data centre owners to pivot and quickly scale up or down as needed to handle the uncertain future.
4. Resilience — By bringing in processes, programs, tools and resources that both enable minimum exposure to hazards and associated risks (like unanticipated blackouts) and rapid reaction and recovery from unplanned events, data centre owners will be in a much stronger position to control their destinies during times of crisis and uncertainty. Even today, powerful AI-based monitoring tools offer new ways to remotely manage at-risk data centre assets.

Schneider Electric's EcoStruxure IT, for example, automatically collects critical infrastructure sensor values on a regular basis and submits that data to a centralised data lake in the cloud. That data is then pooled with other data collected from thousands of other Schneider Electric customer sites.

To find out more about the power of digitisation across the spectrum of energy management and automation in data centres, visit se.com/au.

Image courtesy Macquarie Data Centres

Macquarie opens $17m secure data centre in ACT

Macquarie Data Centres and Macquarie Government have jointly launched a new $17 million data centre in Canberra to store classified government data.

The new Intellicentre 5 (IC5) data centre has been purpose built to house the most highly classified federal government workloads.

The fully sovereign data centre has been built to Tier IV and to Security Construction and Equipment Committee (SCEC) Zone 5 specifications, and will be supported by over 150 Defence Negative Vetting 1 (NV1) certified government-cleared engineers operating a 24x7x365 support centre.

According to Macquarie Telecom, the project alone supported over 400 construction and related industry roles in the ACT, and the company has increased its workforce of cybersecurity engineers by 25% since construction commenced in July 2020.

The build forms part of the more than $100 million invested in the construction of secure, sovereign Australian data centres in Sydney and Canberra by Macquarie in 2020, marking a record investment year for the company.

Construction of the facility was completed on time and on budget by December 2020 despite the challenges posed by COVID-19, and in contrast to the overall industry-wide 10.4% decline in data centre infrastructure spending during the year, as estimated by Gartner.

"Data and cloud demand has skyrocketed as the pandemic continues to bring forward years' worth of IT and digital transformation projects," Macquarie Data Centres Group Executive David Hirst said.

"Ensuring that data remains secure, sovereign and within Australia's borders is vital to protecting our national security and privacy interests — this facility embodies that need in every way."

Service NSW app used by four million citizens

The NSW Government's Service NSW app has been downloaded more than four million times, approximately 75% of NSW's adult population. The app has been used by patrons across the state for more than 117 million COVID-safe check-ins. Premier Gladys Berejiklian said the technology has been a game changer for businesses during the pandemic, while keeping the community safe.

Premier Berejiklian said the technology has been used to enhance the user experience and prioritise public safety, with figures indicating that citizens have embraced the technology.

"I want to thank the people of NSW for downloading the Service NSW app more than four million times, accounting for around half the state's population, which continues to keep our community safe from COVID-19. The app has not only provided an easy solution for businesses and customers for checking in, it importantly assists NSW Health and the contact tracing team in the event of an outbreak," said Premier Berejiklian.

Minister for Customer Service Victor Dominello said more than 80,000 businesses are using the check-in feature, with 94% giving it the thumbs up. Minister Dominello added that the app has been updated to enable customers to save the details of their dependents, with a reminder notification to help users check-out to be introduced soon.

"We want the customer to be at the centre of everything we do, which is why we are constantly bolstering the app in response to feedback. You can also use the app to download a Digital Driver Licence, renew registrations and find out the latest COVID advice," said Minister Dominello.

©stock.adobe.com/au/Skyelar


Smarter technology for all
Lenovo
You don't have to be together to work smarter together.
Simpler, safer, and more reliable collaboration. Our ThinkSmart devices are easy to manage and enable seamless teamwork...from wherever your people connect.
Learn more
www.techtoday.lenovo.com/smartoffice
Lenovo recommends Windows 10 Pro for Business.
Windows 10

©stock.adobe.com/au/paul

DTA releases Hosting Certification Framework

The Digital Transformation Agency has released the Hosting Certification Framework for providers of hosting services to government organisations.

The new framework aims to help agencies mitigate against supply chain and ownership risks and enable them to identify and source appropriate hosting and related services.

It is designed to reduce agencies' data sovereignty, ownership and supply chain risks while ensuring that government hosting services are more efficient and cost-effective.

The framework has two certification levels. The basic 'Certified Assured Hosting Provider' arrangement is designed to safeguard against the risks of change of ownership or control by imposing financial penalties or incentives.

Meanwhile, the 'Certified Strategic Hosting Provider' arrangement represents the highest level of assurance and is only available to providers that allow the government to specify ownership and control conditions.

The latter certification level was previously referred to as 'Certified Sovereign Data Centre', but the name has been changed based on industry feedback.

The DTA plans to commence certification of hosting providers on the current Data Centre Facilities Supplies Panel as a first step towards the implementation of the framework.

Other providers of hosting services such as managed service providers and cloud service providers can register their interest now for inclusion of the Phase 2 certification process, which is expected to commence at the end of the year.

Services Australia has most readable government website

Services Australia has the most readable government website in the nation, according to a new scorecard released by Ethos CRS.

The 2021 readability scorecard for Australian government agencies ranked the Services Australia website as having a readability score of 119.3 — higher than the benchmark of 100 and more than double the score of the next highest agency, the ATO (51.2).

The Australian Securities and Investments Commission was ranked as having the most readable documents, with a readability score of 34.5. Meanwhile, Defence Housing Australia had the best grade level score — a measure of how well text is tailored to people with a lower education level — of 13.0, and the best score for short sentences, with just 21.9% long sentences.

Finally, the Department of Industry, Science, Energy and Resources had the highest use of the active voice at 85.1% of all sentences.

But the report also identified significant room for improvement, with all 136 documents in the survey falling below benchmarks for good readability to varying degrees.

Services Australia website Product Manager Julie Watkins-Lyall said Services Australia is careful to take a human-centric approach to designing webpages.

"In 2019–20, people with a range of diverse backgrounds and reading abilities viewed pages on our website 324 million times. We have to make sure they can find and understand the information they need quickly, so they can get on with their lives," she said.

"Content designers, communication specialists and subject matter experts develop content, with our delivery team doing a final check before it's published."

©stock.adobe.com/au/vege

HITACHI ABB

DESIGNED FOR MISSION-CRITICAL APPLICATIONS IN HARSH ENVIRONMENTS

HITACHI ABB POWER GRIDS ADDS MOBILE WIRELESS CAPABILITY FOR FULL TROPOS PORTFOLIO

Tropos outdoor mesh routers deliver high reliability and performance in extreme application environments.

Mobile capability is immediately available on the full Tropos portfolio. Mobile use cases supported include fleet management, telematics, autonomous vehicle control and Wi-Fi hot spots for mobile workers. The routers can be mounted on service vehicles, drilling rigs, mining equipment, and cranes, providing mobile communications within the Tropos broadband mesh cluster. Mobile capability or fast roaming will be made available through the latest firmware release, 8.9.3. Customers with an existing software maintenance plan can download the update free of charge and install it remotely via the Hitachi ABB Power Grids' Supros network management system.

The industrial-grade Tropos portfolio is specifically designed for mission-critical applications in harsh environments such as mining, oil & gas, utilities and smart cities. Products supported include Tropos 6420-XA for extreme outdoor environments including salt fog resistance and ATEX Zone 2 for explosive atmospheres, Tropos 6420 and 1420 for external mounting, and Tropos 2420 for mounting inside a vehicle. All are dualband routers operating at 2.4 and 5GHz, providing an extremely reliable and secure self-healing broadband mesh network.

Wireless Tech Australia Pty Ltd
Unit 1/63-79 Parramatta Road
Silverwater NSW 2128,
Australia

Phone: +61 2 8741 5080
Fax: +61 2 9648 4500
Email: sales@wirelesstech.com.au
Web: www.wirelesstech.com.au

WirelessTech

DELIVERING AN IMPROVED ONLINE USER EXPERIENCE

Sharryn Napier

© Stock.Adobe.com/au/Song_about_summer

A number of Australian government agencies are struggling to keep up with technology rollouts, with the COVID-19 pandemic only compounding existing issues. Counter to the proactive approach taken by many businesses in the private sector to rapidly implement digital transformation initiatives, agencies such as Centrelink and the Australian Taxation Office (ATO) have struggled to keep up with increased demand.

From the MyGov website crashing at the outset of the pandemic as thousands of recently unemployed Australians rushed to gain access, to the ATO website being targeted by criminals seeking to defraud citizens taking part in the COVID-19 early superannuation access scheme, the legacy systems supporting government offices across the country pose a myriad of problems.

As we begin a new work year and look to the future of online government services, there are three steps that agencies should take to prevent such problems from taking place and promote a better user experience now and into the future.

OVERHAUL SYSTEM SECURITY

The federal government's June 2020 report revealed that the Australian Cyber Crime Security Centre (ACSC) responded to 2266 cybersecurity incidents in just one year, receiving an average of one cybercrime report every 10 minutes. Which two sectors reported the most incidents? The Commonwealth and state governments.

ACSC provides guidance to organisations on how to avoid issues with system security, and while it does caution that there is no single strategy which can prevent cybersecurity incidents from taking place, it does provide suggested mitigation strategies for adoption.

The main strategies for overhauling system security that have been outlined by the ACSC — and which can be adopted by government leaders — include application control to prevent the execution of unapproved or malicious programs, and web and email filtering that only allows for approved types of web content from websites that hold strong reputation ratings.

Additionally, the Centre recommends categorising and only allowing approved attachment types, as well as the implementation of multi-factor authentication for any virtual private network users.

IMPLEMENT REAL-TIME OBSERVABILITY

Implementing continuous incident detection and automated responses to issues is crucial, and this can be done with automated, real-time analysis. If a website suddenly gets thousands more hits than normal, immediate alerts can be sent to the IT team to investigate such a spike.

The problem with modern technology systems is that they have become so complex that oftentimes there's a critically long delay between detecting an issue, pinpointing its location and resolving an incident. In days gone by, an organisation typically had a set number of desktop computers running programs from their hard drive and using local file servers to store and share files. Everything

was on-premise and it was relatively easy to troubleshoot an issue. Today, there are a myriad of different devices connecting to corporate networks, with a mix of local and cloud-based apps and software, and everyone is heavily reliant on the internet and remote services.

To immediately detect suspicious activity, organisations need to know what exactly is taking place across their technology stack. This can be done by deploying an observability platform that monitors each part of the system, creates user-friendly dashboards to visualise the technology landscape, and displays alerts that indicate where problems are occurring. By implementing this real-time technology, government agencies will gain insight into how their technology is being used and pinpoint issues long before they become problematic.

LEVERAGE DATA TO PLAN FOR THE FUTURE

By taking the time to debrief after large spikes in website traffic or a website crash, teams can better understand what they must improve on for the future. Such peaks and troughs in website traffic and demand are bound to continue in the coming years, but by being able pinpoint what has worked in the past to address such spikes — and looking at what could be improved on for future technology iterations — data can be used to plan ahead.

Over time, using machine learning and other technology tools can also help spot unusual patterns as soon as they begin. If an Australian government website suddenly starts getting tens of thousands of hits from IP addresses outside of Australia, at a time of day when it usually gets only a few thousand hits from Australian users, this could indicate that a cyber attack is taking place. By comparing historic web traffic patterns, AI can immediately detect such an irregularity, and isolate potentially infected devices, quarantining them before malware spreads across an entire network.

By failing to stay in lock step with modern tech environments, Australian government agencies are providing a poor user experience to its citizens. The online consumer experience is nothing new — we've been using the internet to do practically everything for over 25 years. Yet despite this, black swan events are still causing websites to crash, and data to be exposed.

By overhauling security, implementing real-time observability and using data to drive decision-making, government agencies will be prepared for future challenges, while delivering a stellar user experience. Australians need access to online services and communication more than ever, yet government websites have continued to fail them. The tools and technology to prevent such issues are out there, and it's time that they are deployed.

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

CLOUD PLATFORM SUPPORTS CUSTOMER SERVICE IN VALLEJO

For most cities, the fees associated with permits and licenses are vital revenue generators. Given growing fiscal uncertainty in the wake of the COVID-19 pandemic, it's more important than ever for cities to have solid systems in place to promote economic development. At the same time, office closures in response to COVID-19 have made it more critical for governments to collect fees virtually. The Planning and Development Services Department in Vallejo, California, is currently implementing a cloud-based online solution to address both these challenges.

Vallejo, located in the northern part of the Bay Area, is known as an affordable alternative to San Francisco. As such, the area has experienced steady construction growth over the last several years, which has put pressure on its Planning and Development Services Department to deliver more with less. Until recently, the city relied on a legacy computer system that couldn't accommodate online services or payments.

"The legacy system created customer service challenges," said Leslie Trybull, administrative analyst in the Vallejo Planning and Development Services Department.

"We wanted something that was more modern and could enable online permit services, help us promote economic development by making it easier to conduct business with the city, and deliver a better user experience overall."

A ONE-STOP SHOP

In late 2018, department leaders began looking to modernise compliance and regulatory processes for land-use and building infrastructure, permits, and inspections.

"We were very excited about the idea but concerned about our capacity to do it while maintaining day-to-day operations," said Anne Cardwell, assistant city manager for the city of Vallejo.

"But we knew we needed to make a change. We had to bite the bullet and get it done."

City leaders considered several options but ultimately landed on Oracle Community Development, a platform designed to help cities manage planning entitlement, building permits, and code enforcement processes.

The platform, which was built specifically for government, offers citizens an exceptional user experience on any device, including simple, guided interactions. It also includes omni-channel engagement capabilities that allow cities to connect with citizens via their channel of choice: social media, phone, email, web self-service, or virtual assistant.

"We chose Oracle Community Development because it would allow us to become a one-stop shop for citizens looking to get business done in the city. It was also user friendly and responsive. It checked a lot of the boxes in terms of what we were looking for and what we were missing in our existing systems and processes," said Cardwell.

Because the Oracle Community Development platform is built on a cloud-based infrastructure, it would also give the

department an opportunity to leverage innovative technologies like chatbots, artificial intelligence (AI), machine learning, and a next-generation user experience. And the fact that the solution came from Oracle helped put leadership unease about the migration to rest.

"There are a lot of other products on the market, and while they may look awesome, we wanted to be cutting edge, but not bleeding edge. We were reassured by Oracle's track record, experience, and reputation," said Cardwell.

Working with Oracle would also provide the city additional resources it needed to complete the implementation.

"We have smart, motivated people, but as a city we don't have a lot of bandwidth. We wanted to partner with somebody that would support us. Oracle fit that bill," said Cardwell.

MODERNISATION, INTERRUPTED

Department leaders decided on a two-phased approach to implementation, with each phase expected to take approximately 12 months. The first phase would focus on enabling online building and public works permits.

But just as the city dove into the project, the COVID-19 crisis closed city offices and city employees shifted to remote work. Department leaders realised the pandemic brought an added incentive to make self-service permits available online. The new cloud platform would allow residents, inspectors, contractors, and others to continue to conduct their business with the city. Department leaders adjusted rapidly and analysed the permit types in highest demand during the crisis.

"The original plan was to release all three of our trade permits at the same time. But because of the pandemic and the challenges it created for us and our customers, we decided to release the electrical permit early," said Trybull.

The electrical permit process went live in June 2020, allowing residents to apply and pay for electrical permits online. They can also follow the progress of those permits and request inspections online.

Trybull said the Oracle team was instrumental in helping the city get the electrical permit online ahead of schedule.

"The Oracle team has been very responsive and helpful all along. They explained things thoroughly from day one. They were there step by step as we transitioned from concept to production," said Trybull.

"When we run into issues, the Oracle team is all over it. They get it done. Their team feels like an extension of our team," said Cardwell.

REDUCING BACKLOGS

Three months after the Planning and Development Services department moved its electrical permit processes online, the number of permits applied for and processed grew by 11%.

"It's definitely had a streamlining effect. Our staff has fewer calls to make and we are able to process permits faster and reduce backlogs. That also frees up staff to focus on the permits and the people that are not yet online," said Trybull.

The department has since made plumbing permits available online and plans to make engineering permits available soon.

"We'll release several other permits over the next couple of months. We plan to be done with phase one in early fall," said Trybull.

Once phase one is complete, phase two — which includes fire prevention, planning and zoning, and code enforcement permits — will commence. Planning and Development Services staff are already working closely with Oracle's product development team to iterate on the design elements of those services.

"It's exciting for our staff to know they have an impact on software that we're going to use, and that other jurisdictions will use as well. That's pretty powerful. And it's a great way to get staff excited about it, too," said Trybull.

MOVING THE CITY FORWARD

The new online services will make it easier for residents to do business with Vallejo's Planning and Development Services Department, while also allowing projects to be completed and code cases to be resolved faster and more accurately. In addition, the online self-service portal will result in improved financial and operational efficiencies because it will allow staff to focus on processing applications rather than assisting customers with routine requests.

Planning and Development Services leaders also expect the project to encourage other city departments to adopt cloud-based solutions. In September 2019, the city created the position of chief innovation officer and hired Naveed Ashraf, an executive with more than 20 years of public- and private-sector experience, as its inaugural chief innovation officer. Ashraf's plans include adopting cloud-based platforms to modernise the city.

"This solution is consistent with where our new chief innovation officer sees the rest of the city heading. Having this experience in our department will be helpful to other departments in the city looking to modernise," said Cardwell.

Most importantly, the new solution will enhance the customer experience, offering tools that make the journey through the permitting or service request process predictable and intuitive, while also providing the city better flexibility.

"Ultimately it's all about that user experience and making it very welcoming, friendly, and responsive. This solution will be helpful on the front end for the users, but it will also help our staff that assist residents in making it all happen," said Cardwell.

This article was developed and written by the Government Technology Content Studio, with information and input from Oracle. For more information, visit Oracle.com/communitydevelopment.

CRISIS FORCES CHANGES TO SaaS CONTRACT NEGOTIATIONS

Jo Liversidge*

NOW COULD BE THE RIGHT TIME TO TAKE ANOTHER LOOK AT YOUR ORGANISATION'S SaaS CONTRACTS.

The impact of COVID-19 has highlighted the ever-increasing costs, high degrees of lock-in and inflexibility of SaaS contracts. Organisations are realising that many current contracts aren't fit for purpose, especially in times of crisis.

With many organisations forced to look at ways to optimise and cut costs in their IT budgets, future software and SaaS contracting must be looked at in a different way to ensure that costs align with value.

Gartner talked to many organisations over the past year that approached their major software and SaaS providers for relief, only to be left disappointed when offered extended payment terms in response. Only in very few instances have organisations — even those in dire financial distress — been able to align their costs with usage or make dramatic reductions commensurate to their current needs.

Some had an expectation that they could more easily right-size their SaaS contracts if they were negatively impacted by the pandemic. However, the contract the customer signed was typically very clear: no downward flexibility and no termination for convenience.

Customers found their contracts wanting in other ways. Some, for example, had even signed contracts that had no concept of force majeure and a right of termination linked to that. Almost no contracts have business downturn language.

Despite these issues, a large majority of large software and SaaS vendors very publicly offered 'free' software to clients for a limited time shortly after COVID-19 made the headlines. This was only 'free' if you weren't already using the software and offers came with certain monetary strings after the free-of-charge period.

We're now starting to speak with organisations whose free-of-charge periods are almost at an end. Not surprisingly, they really want to keep using the software and, in most cases, have little leverage to negotiate reduced fees.

Some still believe that a contract renewal is an opportunity to negotiate the cost of a contract downward, when keeping volumes flat. In reality, most SaaS vendors applied increases to unit pricing for the majority of renewals in 2020, within the range of 5 to 25% — and in some cases even more. The majority of customers have little leverage at renewal.

If your renewal is due in 2021, there will most likely be insufficient time to introduce and evaluate true competition, so that you could move away from your expensive and inflexible incumbent vendor to an alternative. The cost of switching may be prohibitive.

One option is to sign one- or two-year deals if your current vendor won't negotiate more flexible or equitable terms, so you have time to go to market, plan your exit and migrate to an alternative provider in a controlled fashion. This threat alone may be sufficient leverage to get a more equitable deal with your incumbent vendor.

If switching from your incumbent, negotiate additional discounts or a one-off payment to offset potentially large migration costs with any new SaaS vendor. Negotiate appropriate robust exit provisions, such as free-of-charge data extraction and transition assistance, so future migrations can be achieved with less risk and cost.

Don't forget to negotiate language in your contracts that allows commitments to reduce if there is a business downturn by including a structure to change quantities, price per unit or contract duration.

Jo Liversidge is a Senior Director Analyst at Gartner, focused on IT procurement. She provides expertise in the areas of software licensing, pricing and contract negotiation strategies for Salesforce, Microsoft, Oracle and other SaaS providers.

Intel® Core™ Processors

FLEXIBLE FUNCTIONALITY IS AT YOUR FINGERTIPS

TravelMate Spin P4 NEW

Rugged performance

Boasting up to the latest 11th Gen Intel® Core™ i7 processor, get mobility and performance within this highly compact, ultra-light 14" business-grade convertible laptop. With a semi-metal, versatile design, the TravelMate Spin P4 has built-to-last durability, security, connectivity, and a highly refined user experience.

Weight Starts at 1.5kg, 18mm Thick

MIL-STD 810G Compliant

Durable Hinge

Multi-touch Panel

eSIM-enabled 4G LTE and NFC (optional)

Acer Active Stylus

Touch fingerprint reader

Up to 14-Hours Battery Life

DATA AVAILABILITY AND TRANSPARENCY

Deborah Anton

DATA IS THE FOUNDATION OF ANY CUSTOMER-CENTRIC BUSINESS, INCLUDING THE AUSTRALIAN GOVERNMENT.

Data is an asset, and we need to be using it more effectively. Over the last three years in my role as the Interim National Data Commissioner, I've heard this statement uttered on an almost daily basis. No matter where someone works — research, business or government — the value of good data is always a talking point.

The Productivity Commission's 2017 report into Data Availability and Use turned the volume up on the "data conversation" for the Australian Government. The report included a suite of recommendations aimed at improving data sharing processes and their regulatory frameworks, to help Australia realise the full potential of its data.

An insight that has stayed with me from the Productivity Commission's report was that the Australian Public Service has a risk-averse culture.

It is an observation often made of public servants, but in this instance I'm not sure that "risk-averse" is the right term.

My ongoing conversations with Australian Government agencies point to a culture of mistake-aversion. Agencies are apprehensive about sharing data because they want to be certain they are sharing the right data for the right reasons, and most of all, sharing it with people they know they can trust.

Organisations know the value of data, but the trust gap between businesses, researchers, governments and the public has resulted in lack of data sharing between these sectors.

To reduce the trust gap and build consistency in the system, long term, incremental change is required. A key element of this change is the Data Availability and Transparency Bill (DAT Bill).

This law will create a new government data sharing scheme, which will help approved people and organisations request controlled access to government data.

The DAT Bill is currently before the Australian Parliament for consideration, and my team and I are busy thinking about how we will implement the new scheme.

The DAT Bill will drive changes that are relevant to government IT professionals:

- New systems and processes for government agencies to manage data sharing.
- An opportunity for government agencies to strengthen their data management and governance skills and practices.


© Stock.Adobe.com/au/metamorworks

CHANGE 1: NEW SYSTEMS AND PROCESSES

Many government agencies have their own processes for considering and managing data sharing requests. These are often linked to existing legislation and systems.

This is why my team and I have been working on a suite of initiatives to reduce the complexity of navigating the system and create some consistency across government.

Our key initiative is the design and delivery of a new digital platform to support the implementation of the reforms.

The platform will support users to:

- submit accreditation applications and
- submit, manage and track data sharing requests.

In upcoming co-design work, we will explore with the APS the utility of it managing and/or being a repository for any data sharing requests agencies may receive from others through pathways other than the DAT Bill.

The system will ensure that any data sharing done through the scheme is well structured, well governed and supports a safe approach to data sharing. It also has the potential to support agencies manage existing data sharing activities in one place.

Other initiatives that are already available as drafts and will be finalised alongside the Bill include:

- the Data Sharing Principles, which set five firm criteria all government agencies should assess data sharing requests against, and
- a generic Data Sharing Agreement, a template for government agencies and data requesters to use to agree to share data.

CHANGE 2: DATA SKILLS AND PRACTICES

The need to improve the data skills of the public service is a challenge we share with all other businesses in the economy. In 2020 the Australian Public Service Commission surveyed a sample of Australian Government agencies on critical skill shortages, with 70% of them identifying data skill gaps.

My team and I understand that organisations don't always know where to start when it comes to strengthening skills, which is why we've released a product called the Foundational Four.

The Foundational Four is a set of, you guessed it, four essential data management principles that we are encouraging all government agencies to adopt.

These principles are:

- Leadership — a senior leader is responsible and accountable for data across the agency.
- Data strategy — an agency has a clear vision and plan for using data to achieve objectives.
- Governance — mechanisms exist to oversee data management.
- Asset discovery — data assets have been identified and recorded.

Adopting these principles will give your agency a clear baseline for your data practices: what are the "must-haves" in your business? You can then build on this baseline with mature and specialist data skill sets that are going to add additional value to your organisation.

Importantly, these principles will also prepare you to respond to and manage any data requests you may receive through the new government data sharing scheme.

You can find the Foundational Four on the Data Commissioner website at https://www.datacommissioner.gov.au.

CONCLUSION

COVID-19 has proven that data is critical to the successful delivery of government services, accelerating existing trends to ensure Australians could access services in a socially distanced environment.

Data from government services such as Single Touch Payroll has helped us to understand the economy and make crucial policy decisions.

Academics will also need data from this time to understand the impacts that COVID has had on our economy and our lives.

Data is the thread that ties together all of our efforts to understand the world around us and move seamlessly through it with our services. It's the foundation of any customer-centric business and it's essential the Australian Government is one of these businesses.

Ms Deborah Anton was appointed as the Interim National Data Commissioner on 9 August 2018. One of her many career highlights includes establishing the Government's Computer Emergency Response Team (CERT).

Public sector modernisation: how governments should think about cloud in 2021

Government agencies need to develop a comprehensive, forward-looking cloud plan that provides flexibility and security.

Government agencies and institutions in Australia have traditionally been quite cautious when it comes to migrating to public cloud solutions.

The juggernaut offerings from major industry players such as Microsoft, Oracle, Google, and AWS certainly have the potential to drive real innovation for government departments. Although there has been a distinct lack of fervour over the years, for a variety of security and compliance-related reasons, as well as difficulties fulfilling skills requirements.

However, the tide may now be turning. Back in October, the NSW government announced a new cloud strategy that mandates the adoption of a "public cloud first" ideology. The framework urges NSW government entities to migrate their services to public cloud, only allowing private cloud deployments "by exception".

"It is a move that will accelerate innovation, modernise service delivery, and create better outcomes for the citizens of NSW," Minister for Customer Service Victor Dominello said in a statement accompanying the announcement. "A modern and reliable cloud strategy and cloud policy will enable government-wide adoption of public cloud services in a united and secure manner."

The new cloud strategy is likely to trigger a lot of innovation within NSW's public sector. Although the announcement has sparked a wider conversation around the state of digital transformation in all state and federal government departments.

While it's true that a lot of progress has been made on cloud migration in the last few years, most government agencies still have some work to do before they could be considered 'cloud-first'.

"They still have a long way to go," says Derek Paterson, Public Sector Lead at Equinix. "There are newer applications built from the ground up to be digital inside and out, so a lot of those can go straight to 100% cloud platforms.

"Having said that, there are thousands of complex, legacy applications that will be quite difficult to migrate and there are still a lot of 'un-digitised' systems that agencies still rely on today."

In order to manage these cloud migrations, government agencies will need to develop a comprehensive, forward-looking plan. This isn't about making one 'set and forget' decision, it's about forging an elastic approach that provides flexibility and security for years to come.

Key challenges

As with any policy announcement of this variety, securing an adequate amount of funding to enable these transformations will be a challenge. There will be a few key pain-points here, including getting detailed funding applications through central agencies such as Treasury, lengthy procurement processes and shifting from a CAPEX to an OPEX model and accurately forecasting expenditure growth.

The new cloud strategy makes it slightly easier to apply for funding through cabinet

© Stock.Adobe.com/au/Warod

in NSW, especially for smaller agencies and departments, as they can use the announcement as a proof point.

"It can be difficult, as the government bodies making the decision that agencies must modernise aren't the same people who administer budgets," Paterson continues. "Although agencies can certainly use the announcement as a trigger when they approach cabinet."

Another major challenge will be around strategy and how to modernise legacy applications. Agencies will need to take a risk-based approach, assessing all of their mission-critical applications in terms of which ones can be migrated to public cloud and which should stay in GovDC data centres (private cloud).

If agencies have ageing, monolithic applications that just won't be suitable to go straight to a cloud environment, they'll need to think about a long-term modernisation strategy or possible retirement of those applications.

With any migration, security is also going to be a major pain-point, as government always needs to know where its data is stored. As such, data sovereignty becomes a crucial part of the story.

Everyone can appreciate that data is stored in the cloud, and even housed in Australia, but who else has access to it for administrative or support purposes? It's vital that they have complete visibility and control over that.

Forging a best-of-breed hybrid/multi-cloud strategy

Government can be a scary place. Major Machinery of Government (MoG) changes mean departments can merge and priorities can rapidly shift, so flexibility and agility should be the defining elements of cloud migrations for government agencies.

That's why a hybrid/multi-cloud (HMC) approach is the one to chase. These architectures allow agencies to be as dynamic as possible, especially when MoG changes occur. Agencies shouldn't rely too much on one vendor for their cloud deployments, as feature sets are constantly changing and the services that department may be providing to citizens may also change.

If, for any reason, agencies decide that a certain vendor isn't best meeting their needs, having a flexible HMC strategy enables them to seamlessly and rapidly switch up their providers. Deploying these workloads within interconnection facilities will provide even more flexibility, as it allows government to integrate cloud seamlessly with other infrastructure capabilities.

Interconnection provides the necessary collaboration to streamline information exchange across multiple agencies. It also allows agencies to quickly build high-capacity links to thousands of different cloud providers, including all of the major public cloud players, who are already housed within co-located interconnection facilities.

"Whilst Interconnection, accessibility and flexibility are enablers, they can't come at the cost of control, security and governance," adds Matthew Hurford, Regional APAC CTO at NetApp. "One way agencies can address both ends of this spectrum is to hold their data 'next to' the cloud.

"This is an effective strategy for agencies to preserve control over their data, whilst being able to expose it to the appropriate cloud provider for the right use case. All while avoiding the risk of potentially high egress charges."

These 'cloud-adjacent' HMC architectures provide capacity to fulfill any requirement agencies might need, within much faster timeframes and at much lower cost.

Getting started

Ultimately, these cloud migration efforts are going to take time. The process to conduct application feasibility studies, funding assessments, funding applications and finalising procurement agreements can take up to two years, based on complexity. This means, if started now, transformation efforts might not actually begin until 2023.

Importantly, agencies can't do everything on their own. They need to choose a partner with demonstrated public-sector expertise.

At Equinix, we want government to maintain ownership over their own data, while also being able to take advantage of cloud's feature-set through HMC deployments. We recognise the security-related priorities governments need to think about — including information classification and aggregated data risk — and we have a track record of fulfilling those requirements.

As a co-located interconnection facility, Equinix provides high-capacity links to all major public clouds and thousands of private cloud service providers (CSPs). We also have all of the required accreditation applicable to the housing and storage of government data, as we already hold the vast majority of NSW state government hosted data through GovDC.

Not only can Equinix work with agencies to get their workloads to the cloud, we can foster a tailor-made hybrid/multi-cloud strategy suitable for any specific requirements. This is important for ensuring an agile approach that will cater to shifting priorities for years to come.

EQUINIX

Equinix Australia Pty Ltd
www.equinix.com

TRANSFORMING CONTACT CENTRES VIA CLOUD TECHNOLOGY

Rod Lester

CLOUD-BASED CENTRES CAN FACILITATE BETTER TRAINING AND GUIDANCE FOR EMPLOYEES, IMPROVE CALLER INTERACTIONS, INCREASE EFFICIENCY AND REDUCE COSTS.

When the Australian Government formed the Digital Transformation Agency (DTA) in 2016, its purpose was to oversee the government's overarching Digital Transformation Strategy and, by 2025, become a leading digital government.[1] Since its formation, one of the DTA's primary functions has been to improve the Australian Government's digital services. The adoption of cloud-based services and technologies across different government departments, including government contact centres, has been critical to this.

With widespread adoption of distributed and remote workforces in 2020 — a trend set to continue into 2021 and the foreseeable future — contact centre managers embraced cloud-based technologies that let employees work from anywhere without reducing their ability to manage call volumes. In government contact centres in particular, investing in cloud-based technologies has the potential to significantly enhance and improve caller interactions in a number of ways.

EMBRACING DIGITAL SOLUTIONS FOR A DIGITAL FUTURE

One of the most effective ways of enhancing the customer experience will be through the continued investment in and optimisation of automation, artificial intelligence (AI) and other cloud-based digital solutions. While these are by no means new concepts to government agencies, as technologies continue to evolve, so too will their functionality and the benefits they provide to government contact centres.

Augmented intelligence especially will provide significant benefits to government, particularly when combined with automation. Through the combined use of automation and virtual assistants, government can essentially turn their agents into 'super' agents, by placing more specific information about caller interactions at the agents' fingertips.

To meet surging demand for government services in response to the COVID-19 pandemic, the Australian

Public Service Commission redeployed more than 2200 public servants to other agencies, according to a report from the Australian National Audit Office.[2] This move understandably left many government employees operating with different functions and needs from their home agencies and roles, and required training to support their temporary roles in new agencies.

Redeployment of public servants is common in government, and the COVID-19 response won't necessarily be the last time such a redistribution and rapid training of staff will be required. However, by integrating new cloud-based tools and technologies, government contact centres can better prepare for future redeployments and ensure staff have access to the information they need, when they need it, wherever they need it.

INTEGRATING TECHNOLOGIES FOR ENHANCED EXPERIENCES

Investing in cloud-based technologies will let government agencies provide a better experience for both citizens and agents by facilitating access to better support and training. Modern technologies that integrate AI and automation for a more comprehensive and efficient virtual assistant let staff access more real-time guidance than they have been able to previously. AI can learn by analysing caller interactions on a deeper level and provide immediate assistance and guidance for agents. The driver of this 'insight to impact' approach is to assess how quickly an impact can be made on calls, and how quickly employees can act on caller interactions.

The latest AI solutions can leverage past interactions with callers — analysing qualitative metrics including call sentiment, caller behaviours and more, which could not previously be analysed easily or cost-effectively — bringing the right messaging and conclusions directly to agents in real time. With the support of automation, government contact centres will be able to provide on-call training and support, letting them understand what they need to do, say or think about before the call is completed.

Essentially, this will create a digital twin for contact centre agents, providing more personalised and instant assistance that will help agents learn faster and reduce mistakes while serving callers better. This strategic technological integration will be critical in the future to help streamline redeployments of government staff and help provide more assistance to employees that don't have the extensive training that they would have if operating for their home agencies.

INVESTING IN COST REDUCTION

Investing in contemporary cloud-based technologies will also help government departments reduce costs in the long run and better prepare for the future. By integrating solutions that can provide ongoing, real-time guidance and support to contact centre agents, government agencies can reduce the time and costs associated in training new staff. Reducing these time costs will also be incredibly beneficial in terms of redeployments, as it will let agencies bring more agents onboard in less time, letting contact centres provide more support to callers.

Similarly, such technologies can be used to reduce the need for contact centre managers to closely monitor caller interactions, instead letting managers dedicate their time to more sensitive, time-intensive tasks. In addition, integrating smart, cloud-based technologies driven by AI and automation will help support agents working remotely, in the event of continued lockdowns or changing workplace practices.

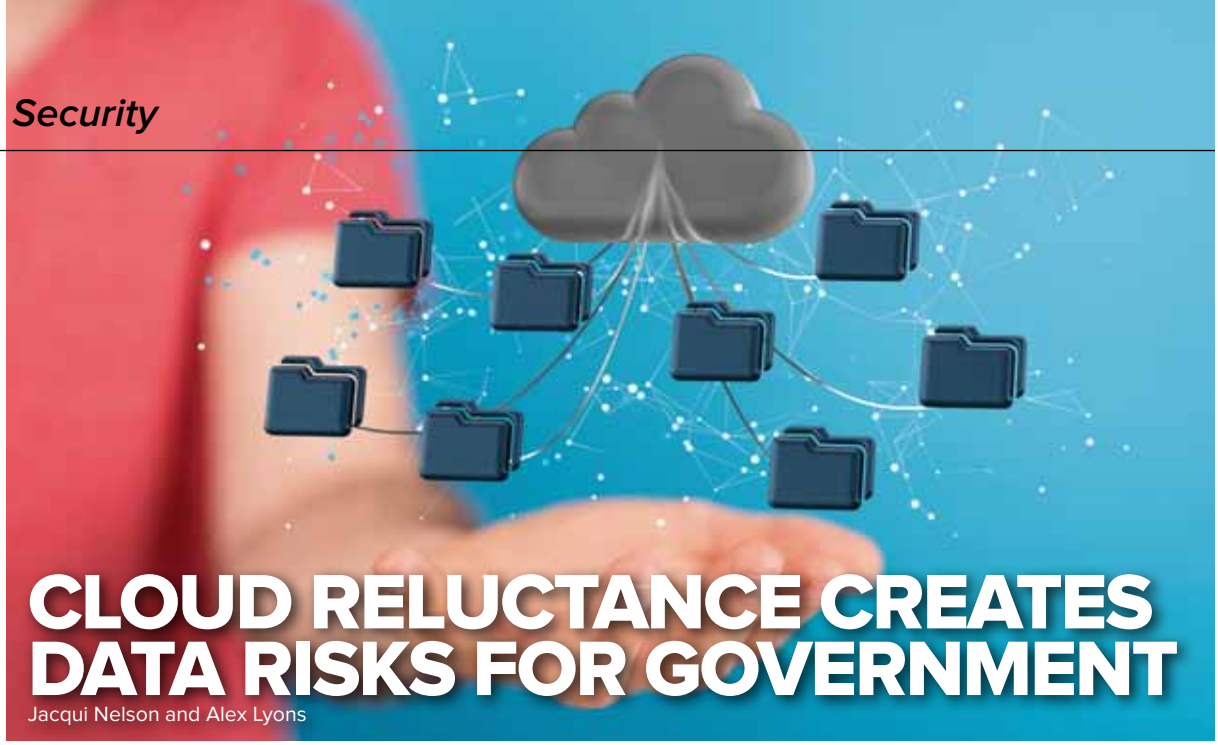
While reducing the time and financial costs that can be associated with contact centres and training, smart technologies can also increase customer satisfaction and improve the overall caller experience. Integrating analytics capabilities provides an added layer of AI to talk to and invoke automation with more context and engagement. In particular, the combination of AI, automation and analytics in the latest contact centre technologies provides new opportunities for government contact centres to measure previously unquantifiable metrics and soft behaviours, including call sentiment and caller and agent behaviours.

Where previously these would be measured by another agent listening in and monitoring the call for training purposes, values can now be put to these behaviours to automatically quantify, analyse and report on behaviours, giving agents the tools to adapt in real time for better, more efficient call interactions. This can also decrease the need for redeployed staff to rely on support from colleagues in their new agencies, which can reduce the time needed to complete calls while sourcing expertise and answers from other agents, and also reduce the associated costs.

By investing in cloud-based technologies that support contact centre agents, government can facilitate better access to training and real-time guidance for employees now and into the future, which will improve caller interactions, while also increasing efficiency and productivity and reducing costs. Government departments can use cloud-based technologies and the benefits they provide to enhance and transform contact centres and provide a better overall experience for callers and agents, without increasing costs long-term.

Rod Lester is Managing Director ANZ for NICE.

References
1. https://www.dta.gov.au/about-us/reporting-and-plans/annual-reports/annual-report-2017-18/annual-report-2017-18-1-agency-overview
2. https://www.anao.gov.au/sites/default/files/Auditor-General_Report_2020-21_20.pdf



CLOUD RELUCTANCE CREATES DATA RISKS FOR GOVERNMENT

Jacqui Nelson and Alex Lyons

Government agencies are facing increasing risks from cyber attacks, but a reluctance to adopt cloud solutions could be driving their vulnerability to human error, state-based actors and sophisticated threats.

The Australian Government is now one of the top five industry sectors for data breach notifications, according to the latest Notifiable Data Breaches (NDB) report from the Office of the Australian Information Commissioner.

Government agencies reported 33 notifications in the six months to December 2020 and this follows an Australian Securities and Investments Commission breach through a vulnerability in a legacy software application.

Government agencies typically prefer to ring-fence their data with legacy solutions that are verified, stable and have stood the test of time. While this may be necessary to ensure data sovereignty, the risks of using locally managed software over cloud software can no longer be ignored.

Legacy software was developed before modern cyber threats existed and relies on complex security tools that focus on defending rather than enabling. As the threat landscape continues to evolve, these legacy systems become more vulnerable, paving the way for more data breaches. A network of disparate systems is unguarded to attacks that can exploit the gaps. Using a firewall may protect the infrastructure, but if data is not secured, it can still be compromised.

End-to-end encryption (E2EE) is the only way to withstand cyber attacks of any magnitude. E2EE protects sensitive data by keeping the key to the data with its owners, not within its own system. Attempts to breach systems will continue, but combining E2EE with modern tools that grant more visibility and control results in true data protection, control and ownership, even in the cloud. These 'true' solutions prevent massive leaks by rendering encrypted data useless to attackers.

The latest NDB report also reveals human error as the public sector's biggest cyber issue, which hasn't been helped by the uptake in remote work. This trend drove an 18% proportional increase in human error across all industries and is likely to continue with the surging shift to telework.

State-based actors are also responsible for cyber attacks on government agencies and have enormous resources to discover and exploit vulnerabilities in software. These same actors use social engineering and bribery of corrupt employees as other attack vectors, putting huge pressure on public sector employees, who have only been armed with education and training to combat these threats.

Bad actors and the threats they pose continue to get smarter, and education and training will only go so far in protecting sovereign data. Relying on staff to recognise sophisticated attacks through social engineering and trying to reinforce legacy systems are not viable solutions.

Rather than put the onus of cyber awareness on staff, government agencies should be making it an inherent part of their organisational security with safe-by-design concepts. Attacks by state-based actors can't be prevented, but what the right provider can do is stop them from accessing data, if and when they infiltrate the network.

Government agencies face a large-scale change management project to mitigate the long-term risks of locally managed software and the impact of human error in highly protected environments. It starts with accepting the need to shift to the cloud and having a provider that understands how to properly protect data with end-to-end encryption.

Jacqui Nelson and Alex Lyons are CEO and Solutions Engineer of DekkoSecure, an Australian-owned and -operated cybersecurity company that provides end-to-end encryption.

Embracing e-invoicing in the public sector

Australian public sector agencies are under significant pressure to manage the current COVID-19 crisis while maintaining services, containing costs and driving the nation's economic recovery. Additionally, growing demand for integrated government policies and services, rapid technological change and increasing cybersecurity risks have required greater levels of integration between Australian government agencies, as well as more collaboration across public, private, non-profit and community sectors.

To help address these challenges, federal, state and local governments are adopting a whole-of-government approach whereby public sector agencies work formally and informally across portfolio boundaries and all levels of government to achieve a shared goal and a consistent response to issues. This is being further driven by the Australian Taxation Office's mandate to have all federal public sector agencies adopt e-invoicing as a consistent approach to the management of supplier invoices by 1 July 2022.

Considering more than 1.2 billion invoices are exchanged annually in Australia, which involves a significant level of public sector resources, e-invoicing is anticipated to save the national economy $28 billion over the next decade while also supporting the whole-of-government approach and resolving many current public sector issues.[1]

Public sector issues that e-invoicing resolves

E-invoicing in Australia is based on the successful International PEPPOL (Pan European Public Procurement On-Line) platform. It will help Australian government agencies across all levels of government to more seamlessly resolve issues around maintaining services, containing costs, and driving the nation's economic recovery through benefits such as:

- improving administrative efficiencies and reducing costs through automating manual processes and streamlining workflows within and across agencies. E-invoices cost less than $10 to process compared to around $30 for a paper-based or PDF invoice due to the extensive time saved on manual processing
- returning cashflow to suppliers faster by helping to reduce public sector payment cycles down to as little as five days. This gets cashflow back to businesses and back to communities much faster to help drive the nation's economic recovery
- delivering real-time data insights that help public sector agencies more efficiently monitor and manage services and expenditure
- providing scalability that makes government agencies more adaptable to change, while complying with governance and legislative requirements
- enhanced security that significantly reduces the risk of duplicate and fraudulent invoices, while also reducing the risk of a security breach in public sector financial processes.

Three essential elements of a public sector e-invoicing solution

There are three essential things that public sector agencies need for an e-invoicing solution:

1. A trusted software partner with Australian public sector compliance experience

Using a trusted supplier that has extensive knowledge of the Australian public sector, and government compliance, helps speed the time to e-invoicing implementation while reducing cost and risk. This gives Australian public sector agencies peace of mind when it comes to ensuring compliance with ATO e-invoicing requirements. A supplier with Australian public sector experience can also help to optimise the e-invoicing solution to meet public sector agency needs.

2. Software that integrates with existing systems to reduce operational cost and security risks.

E-invoicing should improve and support internal processes and streamline workflows, while also supporting optimum levels of accountability and governance. As a result, the solution should save public sector agencies money by improving internal efficiencies and reducing staff time spent on manual tasks. This is achieved through technology-agnostic e-invoicing software that seamlessly integrates with existing public sector systems.

3. An ability to work across public sector suppliers that have e-invoicing capabilities and those that don't.

It may take some time for all businesses, especially small businesses, to adopt e-invoicing, so it's essential for public sector agencies to deliver data security and fast invoice payment benefits to all suppliers, whether a supplier uses e-invoicing software or not.

For more information about e-invoicing download the *A guide to e-invoicing and PEPPOL in Australia and New Zealand* ebook, or visit SAP Concur's e-invoicing for public sector website.

Reference

[1] https://www.ato.gov.au/Business/E-invoicing/E-invoicing-for-government/

SAP Concur

SAP Concur Technologies (Australia) Pty Ltd
www.concur.com.au

PERSONALISATION IN GOVERNMENT SERVICES

A STUDY BY ADOBE AND DELOITTE HAS FOUND THAT 76% OF AUSTRALIANS ARE MORE LIKELY TO USE GOVERNMENT WEBSITES IF THEY ARE PERSONALISED.

The majority of Australians have a preference for digital engagement with government, and for that engagement to be tailored to them. Since the beginning of the COVID-19 pandemic, websites across government have had 1.7 billion visits, with a report from Adobe and Deloitte revealing that 76% of Australians are more or equally likely to use government websites if they are personalised and tailored to their digital profile.

Research shows that almost nine in every 10 Australians looked for government services online in 2020, with Australians aged 15 and over transacting with government on average more than once a week. However, Australians reported a range of frustrations when seeking information from government sources including websites, call centres and in person.

Approximately 75% cited long hold times, 59% said they were unclear when they would get the requested information, and 53% said there are too many passwords to remember. When asked about preferred communication channels, 56% of Australians said their preferred access to government information is online, despite 50% still encountering inconsistent information across departments and agencies, and 22% having to check multiple sources when searching for government information.

Suzanne Steele, Vice President of Adobe Australia and New Zealand, said the report highlights the importance of enabling personalisation, and the current absence of a 'digital front door' to government services and information.

"Australians are needing to invest too much time researching for important information published across disparate departmental websites. The data states three in four Australians today want a personalised digital experience from government. By reading the signals that citizens elect to share online, government can personalise an individual's digital experience based on their needs and digital profile, while honouring user choices " said Steele.

This deficit in the digital experience could explain why so many Australians are turning to non-government sources like search engines, businesses or media articles for government-issued public information.

The report found that 41% of people relied on search engines when looking for government-issued public information, while only 27% said they went to government websites first. In 2020, 70% of Australians looked for public health updates, yet only 24% said they accessed that information directly from government sources.

Australians also ranked 'trust' as the most important factor when seeking public information, with 60% of people surveyed ranking it number one in their top three important considerations when trying to access public information. The next two considerations were 'easy to understand' (54%) and 'most up to date' (53%). Since the pandemic began, citizen trust in Australian governments and agencies has been reported as being on an upward trajectory.

Steele said the report disputes the notion that citizens are reticent to share information with governments, with 81% of Australians saying that they are more or equally likely to use a government service if it remembered previous interactions on all government websites. Additionally, 77% of Australians said they are more or equally likely to use a government service if it used their location to provide information specific to their needs.

"Government must move from a one-size-fits-all approach to deliver the right information at the right time to individual citizens. Beyond driving efficiencies for both parties, this shift to personalisation has the potential to strengthen public service outcomes and continue to build on already increasing levels of trust in government," said Steele.

Deloitte Australia CEO Richard Deutsch said the report reveals that digital has become the medium of choice for Australians seeking government services and information. Deutsch added that the current focus on the digital economy presents an opportunity for government to better meet the needs of its citizens.

Deutsch said the report conclusively reveals that digital has become the medium of choice for Australians seeking government services and information.

"The current focus on the digital economy presents a timely opportunity for government to better meet the needs of its citizens. The next step in the government's digital transformation is to provide each citizen with a more personalised digital experience, directing them to the information they need based on who they are by reading the signals that citizens choose to share online," said Deutsch.

The importance of connected culture in the public sector

Unified communications is critical to the success of digital transformation initiatives and the adoption of flexible working practices.

The Australian public sector should look for every opportunity to integrate and unify their communications, their applications and their systems, because internal communications and collaboration capabilities need to keep pace with the rapid change taking place. Unified communications is critical both to the success of the digital transformation initiatives currently underway, and also to the adoption of flexible working practices, particularly at a local government and state government level.

Supporting digital transformation

Digital transformation initiatives at all levels of government are driving better, faster and more cost-effective service delivery, with improved overall outcomes to the community. However, this means that the services that had traditionally been provided face-to-face or person-to-person are now increasingly being delivered either online or through automation.

That has the potential to exacerbate the siloes that might exist already within the organisation, especially when citizens move out of a self-service or online channel and into a more traditional voice or in-person interaction. Unless video, voice, email, text, chat and customer data are integrated, it's very hard for public services to provide a seamless customer experience and a co-ordinated response. This is also becoming the expectation of citizens, who are now used to engaging with their telcos, banks and other service providers via their channel of choice.

Enabling flexible work

It's clear that unified communications' impact is as much on the employee experience (EX) as it is about the customer experience (CX) — with a direct correlation to the organisation's ability to deliver services to the community.

That EX is being challenged by the acceleration in the adoption of flexible working practices as a result of COVID-19. Public service colleagues who had been sitting alongside each other in the office are now just as likely to be working remotely.

In a NSW Public Service Commission study, while individual, team and customer outcomes were either maintained or improved in flexible working pilots, the major threat to achieving these outcomes was identified as technology, particularly the communications tools available to remote workers. Our own research on remote work has backed this up — providing employees with access to resources and collaborative technologies fosters a 'connected culture' which translates into greater productivity.

Improving both CX and EX can largely be achieved by deploying a single, integrated contact centre and unified communications platform. Casey Cardinia Libraries (CCL) did this just before the lockdown last year. While CCL introduced new technology for its users, RingCentral's ability to integrate with multiple applications, including Microsoft Teams, ensured that staff continued to use the same familiar interface and didn't have to learn another new system. This allowed CCL to quickly transition to a remote working operation, a centralised 1800 number and online ordering system. That meant the local public library could continue delivering exceptional services to the community throughout 2020 and into 2021.

With weather extremes, bushfires and COVID-19, our communities and our public services have endured some of the most difficult conditions we have ever faced. However, we have shown during the last 18 months our resilience and adaptability in the face of these disruptive changes. Ongoing digital transformation projects and the adoption of technology remains key to maintaining this resilience.

RingCentral®

RingCentral Australia
www.ringcentral.com.au

AUDITS FIND SOME SA COUNCILS HAVE LAX SECURITY

Dylan Bushell-Embling

Audits of three South Australian councils conducted by the state's Auditor General has found significant deficiencies in the councils' ICT security standards.

The audits of the Port Adelaide Enfield, Prospect and Port Augusta city councils all uncovered evidence of lax security standards causing unnecessary cyber risk.

In the case of all three councils "important internal control elements to mitigate cyber security and technology risks were not operating effectively," the auditor general's department said in its summaries of the audits.

The audits found that most of the main ICT systems of the Port Augusta and Port Adelaide Enfield councils are internally hosted but supported by external contractors. The former has just four staff on its ICT team while the latter has 16.

Meanwhile, the Prospect council outsources its help desk and local infrastructure support and has service agreements in place for its ERM, database admin and other services. The company has two staff on its IT team.

The Prospect and Augusta councils were found in the audits to have gaps in cybersecurity policies, procedures and standards, while Port Adelaide Enfield had insufficient coverage with these policies, procedures and standards.

All three councils also had weaknesses in password controls and change management controls, and were running unsupported software, the audits found.

Other common security gaps between the three councils include insufficient management of risks and contracts over third-party service providers, a lack of a standard ICT risk register and reporting, and insufficient user access management.

Each council's web application was also found to be using vulnerable software libraries with exposed administrative portals, and some documents within the applications had inadequate security applied.

The Port Augusta City Council was meanwhile found not to even have a backup policy and procedure or disaster recovery plan, or to have established any information security incident response plans. The council was also found to be still using unsupported legacy servers.

The three audits outline a series of recommendations tailored to each council, requiring improvements in areas including security governance, system security, change management, backup and recovery, and vulnerability assessments.

Each council has been urged to formalise an information security user awareness program, establish or formalise an ICT risk register, and implement changes to their password settings and policies.

The audits also recommend councils establish and follow a formal patch management policy, and to implement procedures to evaluate and track all system changes and patches released by vendors using a separate test environment.

In their respective responses to the audits, the three councils generally accepted the findings and said steps are already underway to address the deficiencies uncovered during the investigations.

But the Prospect and Augusta councils also highlighted the challenges involved with the current lack of an agreed ICT control framework in local government, and noted that a standard compliance framework should take into account the size of the council, the available resources and level of risk involved.

One step at a time:
Why local councils don't need transformative digital overhauls

Brett Barningham

Taking a digital improvement approach doesn't mean everything needs to be done at once — an incremental approach can help to discern what really matters.

© StockAdobe.com/au/Studio ProX

Local councils are constantly striving to improve the digital experiences of citizens, although the difficulty of attaining budgets for large-scale transformations can be a hefty challenge to overcome.

When budgets get denied or financial needs aren't fully met, it's a lose-lose for everyone involved. While local government bodies strive to offer up innovative digital services for citizens and employees, the reality is that adequate funding can be just as hard to come by.

However, digital investment doesn't just have to come in the 'transformational' variety. This was proven throughout the COVID-19 pandemic, which — for many councils — shifted digital investment away from big projects with long lead times to rapid deployments of platforms and services based on needs.

As we come out of the pandemic, it might be useful to maintain this 'change is the new normal' ethos. In some cases, the best option for cash-strapped local councils is to integrate technology enabled solutions through 'digital improvement' rather than 'digital transformation'.

Take Moorabool Shire Council near Melbourne, who had their whole asset management process modernised through the implementation of a single application. Grappling with challenges borne from manual paper-based processes, the council employed Civica's Reflect application to automate the management and inspection of footpaths, roads and other assets.

The results were inspiring, as it transformed the day-to-day work of field teams without a full-scale digital transformation. In providing a data-driven asset tracking capability, the solution eliminated guess work and made the whole process — from managing teams to issuing vital repairs — far more efficient.

Driving cost savings

Moorabool Shire's investment in 'digital improvement' also has the potential to drive big cost savings. Asset management is a core activity for local councils and improving this process with a digital capability means less time and money is wasted. As a result, budgets for other digital transformation projects can be made available.

Although it doesn't have to be just about asset management. Councils should think about how they can improve their interactions with their specific communities. Are there any simple foundational elements or manual processes that could easily be improved with a digital capability? Could various bespoke systems and data sets be pulled together to create a 'single-source-of-truth'? Could more data be made available to citizens? These are the things councils should consider.

Another useful tool that has risen as an imperative in the wake of the pandemic is self-service tools for citizens. Again, these can be more simple implementations that allow people to pay rates online or check on the status of a repair.

Taking a digital improvement approach means everything doesn't need to be done at once. Rather, councils can take an incremental approach to discern what really matters for their communities and start there.

It also eases the burden on change management, which is an aspect of digital transformation that local governments often underestimate. The cost of change outside of the project is often multiple times higher than the cost of the technology itself and this isn't always adequately accounted for in budgets. Change is difficult. People need to learn new skills, belief systems and reinterpret the way they view and value their jobs, often against their explicit wishes. Depending on the specific workforce, many can resist change, and this creates an additional financial burden on transformation projects.

By taking an incremental approach, this change can be easier to manage as staff have more time to learn new processes and IT has increased capacity to help them through this.

Moving forward, councils can ease their overall financial burdens by delivering shorter, sharper projects that solve one problem at a time. Using an incremental approach based on needs, IT can more efficiently deliver projects that drive meaningful cost savings, freeing up budget over the long term to allow focus on additional digital innovation.

An update to our previous research with UTS Centre for Local Government into improving citizen engagement titled "Community as a Service" is due out in April. This update captures the thoughts of councils from around Australia on what has changed in their approach to citizen engagement during the pandemic. To read the new report when it is released and also the existing report please go to https://www.civica.com/en-au/.

CIVICA

Civica Asia Pacific
www.civica.com

HARNESSING DATA AND ANALYTICS FOR CITIZEN HEALTH AND WELLBEING

Sonia Sharp

THE HUMAN SERVICES SECTOR HAS RICH DATASETS THAT CAN HELP CASEWORKERS APPRECIATE THE FULL PICTURE OF CONCERN. NOW IT NEEDS TO EMBRACE SAFE DATA SHARING.

Given the human services' progress and the will to collect, share and use data more effectively, the sector is set on a good course to realise its ambition to holistically meet the needs of our most vulnerable citizens by working collaboratively across the ecosystem.

During COVID-19, Australia's human services agencies have been pushed to rapidly adopt digital technology, with 59% of respondents of a survey of Australia's human services professionals saying their agency's use of digital technologies and data solutions has increased.

Even before the pandemic, government agencies and providers recognised that reliable, cross-agency data is critical to help make better decisions and design more informed policy options. COVID-19 magnified that need, catalysing great efforts to make easy-to-visualise data accessible to decision-makers at all levels.

Importantly, citizens' trust in government increased this year, when they saw their elected representatives harness real-time data and step in swiftly to create a safety net for those affected by the health and economic shocks of COVID-19.

DIGITAL AND DATA SOLUTIONS ARE NOT TEMPORARY

That said, EY global research into human services agencies found 46% of Australian respondents saying that "introducing digital technologies and data solutions was a temporary measure to help our organisation get through the pandemic period".

It's a confounding finding when respondents were largely positive about the way agencies invested rapidly in technology upgrades to support virtual contact with vulnerable individuals and families. Around two-thirds of Australian respondents said the use of digital

© Stock.Adobe.com/au/peshkova

technologies and data solutions had improved access to care, delivered better outcomes for customers and made staff more productive since the outbreak of COVID-19.

One of the biggest issues faced during 2020 was the risk that many vulnerable citizens became invisible due to COVID-19 restrictions. A major concern for human services agencies throughout the pandemic was how to reach customers who were previously engaged through face-to-face contact, such as home or office appointments, or reporting through school or hospital referrals. In particular, the pandemic brought a whole new cohort of customers into the risk of vulnerability due to loss of jobs, homes or loved ones, and agencies weren't able to detect them in their usual way.

There remains great concern that the most vulnerable and disadvantaged, including those without stable internet access, will 'fall through the cracks' if services become increasingly digital. A myth is emerging that the act of turning a paper file into binary code is somehow disadvantageous to the work of human services.

Nothing could be further from the truth.

Of course, human services agencies will need to continue face-to-face contact for the most at-risk cohorts. For some individuals, families and communities, face-to-face will remain the best medium for engagement. No-one is suggesting home and office visits should cease.

But customers now expect to access help online and by phone, and indeed, some prefer this. Some agencies are finding they can improve input to caseworker assessments and decision-making through increased use of digitising, analysing and sharing data — building a richer picture of need and customer preference as they protect and help vulnerable citizens.

STILL IN THE DEVELOPMENT STAGES

Currently, despite all the progress being made across government, many human services caseworkers do not have access to all the key data held by their own agency or adjacent agencies within the same government tier.

At the extreme, we have examples of agency collaboration where colleagues from different agencies (like child protection, health, police and justice) sit in co-located offices logged into different, unconnected systems. Their usual means of sharing data is talking to the cross-agency colleagues sitting next to them.

Most human services agencies do share data electronically, but there are some still reliant on phone or fax. As a result, frustrated customers still have to repeat their story to different agencies — and caseworkers frequently visit people without knowing what happened with another agency the week before.

Every public sector agent who intersects with the same citizen should have access to all the appropriate data relevant to that citizen in real time.

Leading the way, New Zealand has a shared dataset across its entire population that is used by all government agencies to shape policy and frontline services. As just one example, Oranga Tamariki (the NZ child protection agency) uses the data to:

- understand vulnerable families and children
- design its service offer to target services at the most vulnerable
- intervene as early as possible in those families' lives before crisis occurs.

CITIZENS ARE NOT SUPPORTED

Perhaps even more concerning, until we crack data sharing, we cannot use the most advanced digital tools to support human services goals.

If consumers can find and book accommodation on Airbnb in under a minute, why are our caseworkers spending hours calling around to find placements for at-risk children? If a smart

crop system can predict when a farmer needs to order more nitrogen, why can't we actively monitor key indicators like school absenteeism or hospital visits to predict when children are likely to become at risk?

The technology exists to do all of this — and so much more. And we don't even need to gather more information.

Agencies can and do integrate existing datasets to understand cohorts and interactions across agencies and communities, and design better programs, services and responses. By combining multiple datasets from across systems and reviewing against historic patterns, new tools can uncover early markers that signal a child or family is at risk.

In the UK, by running predictive analytics over publicly available data, one London borough can now identify six to eight weeks in advance that a family may become homeless — and nine months ahead of time that a child may need to be taken into care.

In Brazil, vulnerable families are identified before they become homeless by analysing welfare payments and changes in food bank usage patterns.

Wherever data sharing is prevalent, agencies are able to respond to early warning signals and offer support before families reach crisis point. Such interventions not only improve citizen wellbeing — and sometimes save lives — they are also substantially more cost-effective than waiting until a crisis occurs.

Automated data collecting, sharing and visualisation tools could save caseworkers 30 to 50% of their administrative time in some instances, freeing them up to spend more time with at-risk children and families.

In New Zealand, the Family Harm app has replaced a 13-page paper form that used to take police officers 40 minutes to complete. Information that used to take days to reach police records is now uploaded instantly — often during an interaction. The app also gives frontline officers useful information such as historical episodes at the same location.

If consumers can find and book accommodation on Airbnb in under a minute, why are our caseworkers spending hours calling around to find placements for at-risk children?

Police describe having this additional context as an "eyes wide open" approach that is paying huge dividends.

CASEWORKERS NEED MORE ROBUST DATA

Many government agencies have formed cross-agency intelligence functions and integrated datasets to enable real-time analysis of risk and forecasting of need — both to inform policy and service system design and also enable rapid decision-making during operational service delivery.

At the same time, the Commonwealth has continued to invest in building data capability across the Australian Public Service through initiatives such as the Multi-Agency Data Integration Project and the data professional stream strategy.

But nowhere is this more important than in human services, which relies heavily on its caseworkers exercising judgement. Their job is to make the best decision they can in any given situation. And, despite decades of experience, enormous dedication and immensely good intentions, caseworkers are only human. For a multitude of reasons, some decisions are made without the benefit of all the key information relevant to the case.

These indispensable frontline staff do an amazing job, often burdened by heavy workloads. They don't always have a lot of time to triage a new reported risk of harm or make a decision on a family in their caseload. Also, because at-risk families are seen by many agencies, even when caseworkers see risk markers they may assume someone else is already dealing with the issue — a variation of the well-documented 'bystander effect'.

FIVE MYTHS HOLDING BACK DATA SHARING

In both our formal research interviewing frontline workers and end users, and our work with clients, we continually hear people speak of a desire to move to holistic, integrated service delivery. And the pandemic has demonstrated that people can react quickly to new technologies, with 58% of Australia's human services respondents thinking their agency staff quickly adapted to the use of new digital technology and data solutions.

We believe if people had time to stand back and think about what's possible and understand the reality of data sharing, resistance would fade away.

To this point, let us dispel once and for all the myths and concerns around data sharing. Anecdotal evidence suggests some human services frontline workers are reluctant to share data because they believe:

1. **Privacy issues have not been solved.**
   Most states have already passed legislation that enables information sharing. In contrast to historical precedent, privacy commissioners are now encouraging data sharing with the user's consent and where it makes sense. Caseworkers should also be aware that a lot of the data shared is anonymised. Datasets can be linked in a central way that protects the identity of individuals but brings together critical data from different systems across agencies. This can then be presented back to case workers in automated case notes, putting together all the touchpoints an individual or household has with human services agencies.

© Stock.Adobe.com/au/peshkova

SURVEY METHODOLOGY

The survey was conducted using an online interview administered to members of the YouGov Plc UK panel of 800,000+ individuals. Fieldwork was undertaken between 3 and 29 September 2020 with 2313 health and human services managers spread across Australia, India, Italy, New Zealand, UAE, US and the US. In Australia, the cohort included 69 human services managers.

2. **People can't be reduced to numbers.** This is true, but data sharing isn't just about the numbers. Written case notes can be digitised and searched, giving caseworkers a summary of decades of notes in seconds.
3. **They need to see for themselves.** Some caseworkers have learned from experience not to trust anything they haven't seen with their own eyes. Without downplaying the importance of direct involvement in assessment, any additional information is an important resource, even if it comes with a question mark. Over time, as cross-agency collaboration and data sharing become more widespread, trust will build and caseworkers will become more confident about the information the system delivers to their phone before they walk into a home.
4. **Digital is less secure than paper.** Many people who are resisting digitising and sharing data have no qualms about handing over a paper file or faxing information to another agency. Arguably, properly protected digital records are at least as or even more secure than their paper equivalents.
5. **Data and automation will replace the human touch.** People fear that automation is the precursor to removing human judgment from human services. Yet the likelihood is that the opposite is true. In the mining industry, the introduction of automation has actually created jobs. The future of human services will continue to rely on human judgement and the need for a human touch. The technology being proposed will simply make it easier for people do their jobs well and give them rapid access to useful information that will make them even more effective.

HOW TO KEEP DIGITAL MOMENTUM GOING

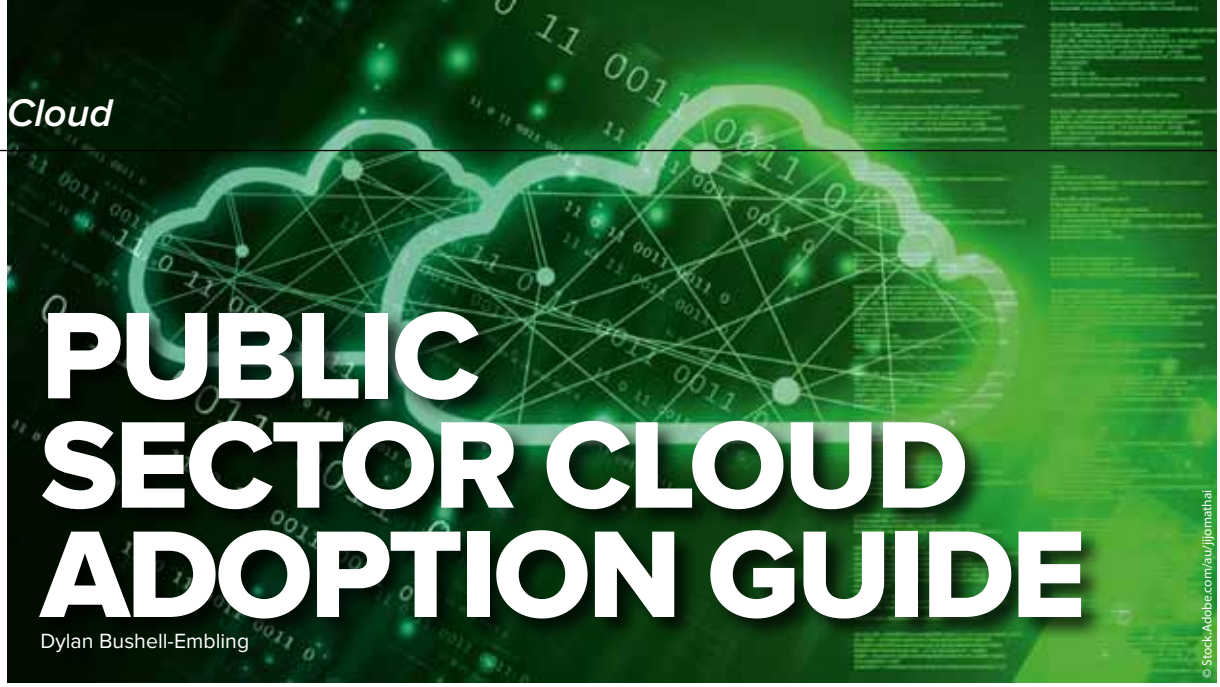
Holistic, integrated service delivery enabled by data sharing is the key to unlocking the potential in what the human services sector already has in place. To embrace the power of data to protect our most vulnerable citizens, agencies and departments should:

- set the vision from the top and embed process and practice signals that encourage data sharing
- open up the system to more flexible funding arrangements and new models of accountability to remove blockers between agencies and providers
- agree on new, shared measurements of success against which every agency and provider is held accountable
- create a culture that rewards individuals when they make a choice to try something new and think beyond traditional ways of planning and executing programs
- make investment in digital literacy as important as that in other professional development.

Ultimately, all these changes need to be driven by a desire to focus outcomes on an end user's real needs and wellbeing. It will then be that individual who determines what those outcomes should be. As one end user said, wouldn't it be fantastic if all organisations could "get on the same page and work for us". That will not happen until human services embraces data sharing at every level.

Let's not wait for the next crisis to drive change forward. Human services has everything it needs to build on the digital 'muscle' it has built over the last nine months and start to understand and make brilliant use of the rich data it holds.

EY Partner Dr Sonia Sharp holds a Ph.D. in educational psychology and has worked in senior government positions in Australia and the UK.



PUBLIC SECTOR CLOUD ADOPTION GUIDE

Dylan Bushell-Embling

A NEW REPORT OUTLINES THE KEY FACTORS BEHIND THE SOMETIMES-SLOW ADOPTION OF CLOUD SERVICES IN THE PUBLIC SECTOR.

Public sector IT association Socitm has published a new practical guide for public sector CIOs into the challenges and opportunities presented by cloud computing.

According to the report, while the relatively slow adoption of cloud computing in the public sector is often attributed to public servants being adverse to change, this only paints a partial picture.

Other factors include cloud sellers overselling the benefits and misunderstanding the risks, costs and challenges of cloud adoption in a public sector context, as well as a lack of strong governance and unclear cloud adoption policies at the leadership level.

A key factor behind a successful cloud adoption strategy is understanding the various types of services available, the report states. Procurement concerns will differ depending on the service.

For example, hosted cloud platforms offer basic cloud infrastructure as a service, the report states. Procurers can assume the recognised brands are safe, secure and resilient, but must take care in managing how sensitive data is tracked and shared, and where data is located and processed.

Cloud-native applications meanwhile can be deployed and fixed faster, but CIOs will need to ensure that their team has mature methods for development and optimisation. Homegrown solutions can help address particular challenges better than even specialist solutions from the private sector, but care needs to be taken to optimise performance and security and avoid creating future legacy overheads.

Realising the benefits of cloud investments also involves careful planning and often requires advice on how to best capitalise on the investments.

These benefits include improved resilience, enhanced security, potential cost savings, sustainability improvements, greater flexibility and superior innovation.

Public sector CIOs also need to resist the temptation to attempt to do everything at once, Socitm said, warning that too many concurrent cloud implementation and transformation projects can be confusing and challenging in terms of governance, supplier management and change management.

In addition, adopting cloud computing can introduce some unique risks. But while many CIOs expect the main risks of cloud computing to be in maintaining resilience and control of the technology environment, security and data management, these fears can be misplaced, the report states.

Instead, cloud technologies commonly cause risks in areas including increased use of shadow IT, a growing dependency on internet connectivity and capacity, the lack of clear data ownership for apps, and the lack of understanding or tracking of data use — which can have regulatory implications.

The report adds that a move to a predominantly cloud model of IT requires even more careful consideration by CIOs, who can expect to face challenges in areas ranging from security to avoiding vendor lock-in, the provision of technical support, data governance issues and increased requirements for IT resources.

Another area that needs careful thought is choosing a cloud service provider partner. Socitm recommends that CIOs conduct extensive due diligence checks in tendering and selecting a cloud service.

These checks should involve an evaluation of both the vendor and its solutions — with credential checks and standards and accreditation evaluations — as well as the terms of the proposed contract, including the support for transition and migration that the vendor will provide.


image credit: iProov

ATO invests in face verification technology from iProov

iProov has been selected by the ATO to provide face verification services for myGovID. It's the latest in a series of examples of governments turning to Genuine Presence Assurance for online identity verification.

Genuine Presence Assurance enables governments, banks and other organisations to verify that a person accessing services remotely is genuinely whom they claim to be. It combines the highest levels of security with an effortless experience for the user — essential to delivering inclusivity to citizens who may be unfamiliar with technology.

A remote user wanting to complete a secure process using their mobile device, for example opening a bank account, onboarding to a digital identity program or applying for a driver's license, is asked to verify their identity with a brief face scan. This process, which lasts a few seconds, uses a sequence of colours to establish that the user is:

- The right person — does this person match the identity in the trusted source
- A real person — is this person a human being and not a photo, a mask or other presentation attack
- Authenticating right now — is this person authenticating themselves right now and is not a digitally injected attack using a video, deepfake or other synthetic media

The user does not need to move or follow instructions. They simply position their face into an oval on the screen and the scan takes place.

By enabling governments to prevent online fraud in this way, iProov technology means that processes once requiring an in-person appointment with an identity check done by an official can now be done digitally.

iProov's Genuine Presence Assurance is being used by governments globally to support a wide range of services, from digital identity programs to immigration and health. The UK Home Office is using iProov, provided by WorldReach, to enable millions of EU citizens living in the UK to apply to the EU Settlement Scheme.

iProov is also being used by the National Health Service (NHS) in the UK to onboard citizens to their NHS login, which provides access to health records and repeat prescription facilities.

In Singapore, the Government Technology Agency (GovTech) is using iProov, supplied by Toppan Ecquaria, to provide face verification services for their national digital identity program, enabling Singapore residents to access 500 digital services via the SingPass app.

In the US, iProov is helping to facilitate cross-border travel for the US Department of Homeland Security. iProov's solution enables travellers to use their personal devices to report their entry and exit to US Customs and Border Protection without requiring the direct engagement of a CBP Officer in person or online.

Genuine Presence Assurance also maximises user privacy. Face verification is very different to face recognition, where faces are matched to a database without user consent. A user knows that face verification is taking place, they collaborate with it, they see a direct benefit from it and their privacy is protected, using the privacy firewall.

Establishing the genuine presence of an online user has never been more important. Fraudsters can view banks and governments as honeypots, worthy of a concerted effort for impersonation or fake identity creation. In America, for example, benefit programs and stimulus packages have been targeted by fraudsters online, leading to losses of $36bn USD.

With Genuine Presence Assurance, governments have the ability to verify user identity securely and protect against fraud, while offering convenience, inclusivity and privacy to the citizen.

iProov Ltd
www.iproov.com

Secure IT disposal

Reuse-Recycle IT is a provider of certified secure technology disposal for government and industry throughout Australia. Its experienced team manages the complete disposal process, ensuring the secure handling, storage and destruction of all IT equipment, including classified equipment. Its processes are ISO, PSPF and ISM compliant and include end-to-end reporting and auditing as well as certification of sanitisation/destruction. Where necessary, Reuse-Recycle IT can also work together with external service providers.

Reuse-Recycle IT is also ISO 14001-2015 Environmental accredited and can guarantee that all equipment is processed appropriately, to the highest environmental standards, creating zero landfill.

The company only engages with buyers who provide assurance that they will comply with international laws and standards, such as child labour laws, export controls and adherence to UN labour laws and worker rights.

On the customer's behalf, Reuse-Recycle IT pursues financial return from electronic waste (such as the $5+ million returned to the ACT Government) while also providing a managed, secure service with timely and accurate reporting.

Reuse-Recycle IT's team can discuss users' IT disposal requirements and explain how its services can assist to 'empty your basement' and provide financial return in doing so.

Reuse-Recycle IT

https://reuse-recycleit.com.au

Calendar

Comms Connect New Zealand 2021
Wellington: 12–13 May
Panels, case studies, tech insights and training for critical comms users.
comms-connect.com.au/event/comms-connect-nz/

Australian Cybersecurity Congress
Online: 25 May
The 'premier' virtual conference for cybersecurity professionals in Australia.
terrapinn.com/congress/australian-cyber-security/

Techweek2021
Online: 25–30 May
A tech festival with a mix of live, virtual and hybrid events.
nztech.org.nz/event/techweek2021/

Tech in Gov
10–11 August
Bringing together public and private sector experts to learn and network.
terrapinn.com/conference/technology-in-government/

EduTECH International Congress & Expo
Melbourne: 17–18 August
Bringing members of the education tech scene together under one roof.
terrapinn.com/exhibition/edutech-australia/

ITU Digital World 2021
Hanoi: 1–30 September
A global platform for accelerating ICT innovations.
digital-world.itu.int

Comms Connect Melbourne 2021
Melbourne: 19–21 October
Showcasing the latest technologies and solutions in communications.
comms-connect.com.au

Australian Cyber Conference 2021
Melbourne: 15–17 November
Providing leaders with cybersecurity insights and best practices skills.
cyberconference.com.au

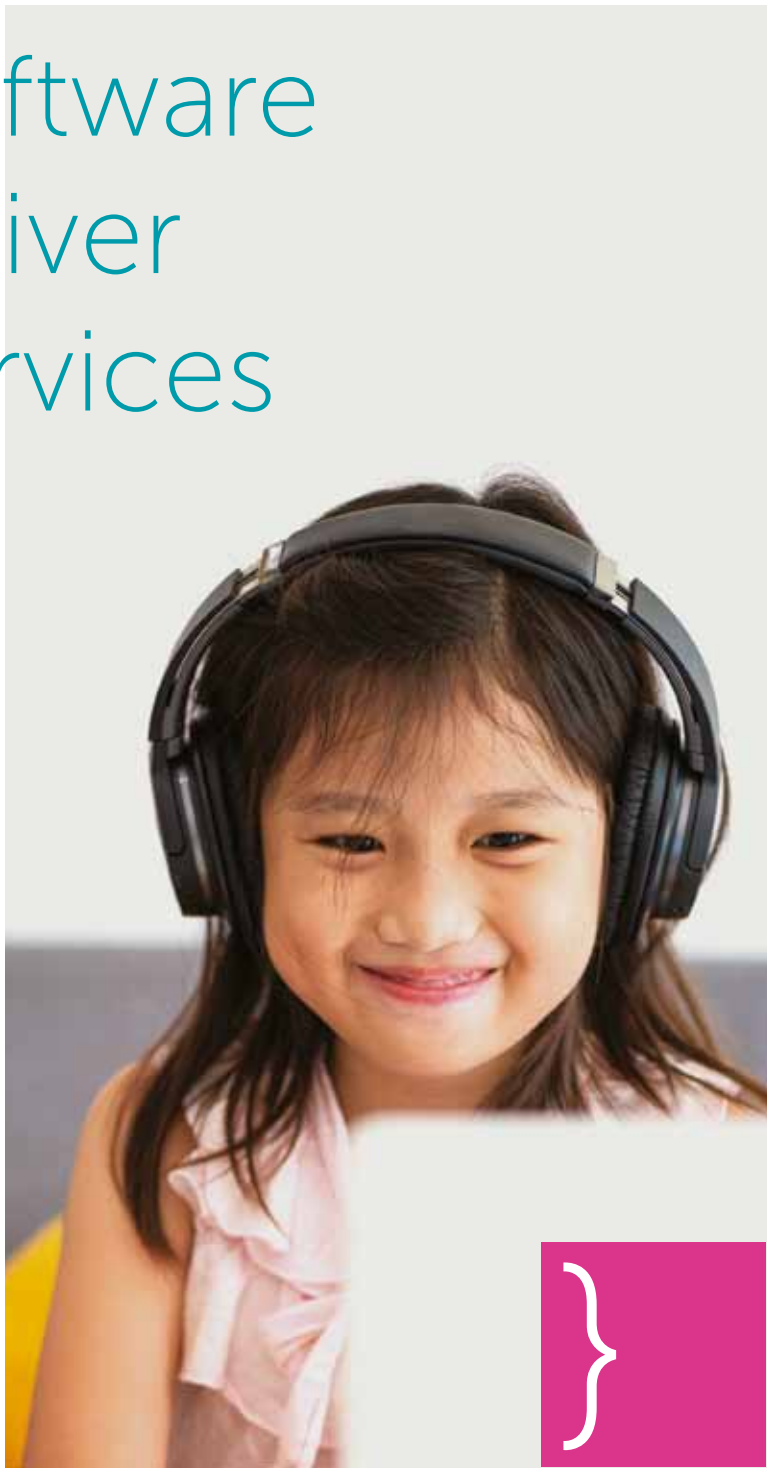
civica

{ Our smart software is helping deliver the public services of the future.

Across the public sector and regulated markets, we support local and regional government, health and social care, social housing and education, combining our global reach with local understanding.

Our sector experience sets us apart.

With a customer focus and track record of delivery, we provide the smart software and services which help public service providers around the world to achieve better outcomes for people and communities.



civica.com | #communityasaservice

SECURE YOUR DATA & EQUIPMENT

A data enclosure is your last line of defence, so it needs to be strong enough to stop unauthorised access.

The MFB range of Class B and Class C enclosures are purpose built frames fitted with key locks and boltwork approved by the Australian Government Security Construction and Equipment Committee (SCEC)

All enclosures are fitted with tamper evident cable entry systems, high impact clear polycarbonate panels on doors, secure venting systems and certified combination locks.

An alternative product, the MFB range of High Security enclosures provides a lower level of security and is not SCEC approved. Effectively construction methods mirror the Class B and Class C series, however the doors are fitted with a cheaper bilock keying system. Also additional flexibility with the design regarding cable entry encourages effective quick installation and high volume data cable installations.

With over 50 years in the business, and backed by the SCEC approval for manufacture, these Australian built 19"rack mount enclosures provide peace of mind in relation to the security your data needs.

SCEC
APPROVED | PRODUCT

MFB®

DESIGNERS & MANUFACTURERS OF 19" RACK SYSTEMS

50 YEARS

PROUDLY MANUFACTURING IN AUSTRALIA

AUSTRALIAN MADE **MAKES AUSTRALIA**

ISO 9001 Quality Management | ISO 14001 Environmental Management

19" Rack Cabinets Licence No. 84594

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