

gov tech review



CRISIS CONTROL

ICT'S ROLE IN
BUSHFIRE RECOVERY
AND THE COVID-19
RESPONSE

SECURITY
THROUGH SLEIGHT OF HAND

GOVERNMENT I.T.
IN THE CROSSHAIRS

SETTING STANDARDS
FOR SECURING DATA



ExtremeCloud IQ

Unlock the potential
of AI and ML

Manage your wired and
wireless network in the cloud
with ExtremeCloud IQ

Simple, Efficient, Secure
Cloud-Driven Networking



**EFFORTLESS
NETWORKING**



**DEPLOYMENT
FLEXIBILITY**



**ACTIONABLE
INSIGHTS**

**ExtremeCloud IQ is a
subscription based
service offering:**

- Automated network operations: end-to-end, edge-to-DC
- Artificial Intelligence and Machine Learning to unlock new data insights
- Containerised microservices - new features appear at cloud-speed
- Access to Unlimited Data for the lifetime of your subscription
- Flexible public and private cloud offerings to reduce capital and operational expenditure

Contact Extreme Networks Australia for your free demonstration today

Ph: +61 (2) 9060 6438 | www.au.extremenetworks.com/contact-sales/

FEATURES

6 | State of emergency



Oracle helped the Victorian Government assist bushfire victims by deploying a SaaS customer relationship system in just three days.

22 | Working from home: lessons learned



Here are the tech, policy and budgetary ideas you need to know about the COVID-19 'working from home' phenomenon.

14 | Standards set the scene for securing data



Standards Australia is working with experts to discuss the adoption of an international privacy standard for information and data management.

27 | Dealing with COVID-19's tech impact



Governments will struggle to complete tech optimisation or modernising plans if they're not directly relevant to supporting COVID-19 responses.

20 | AusPost helps digitise agency mailrooms



A mailroom digitisation solution has been deployed to help state agencies cope with the COVID-19 lockdown.

32 | Security through sleight of hand



Deception technology is proving to be an innovative and successful approach for defending local governments against cybersecurity threats.

21 | AI is the future for data in government and education

30 | Five principles to guide I.T. cost reduction

33 | Conference calendar

33 | Featured product

34 | Government I.T. in the crosshairs



Insider



Tech's role in a world in upheaval

Australia has had a lot to deal with over the past nine months or so. First there were the awful bushfires that ravaged much of eastern and southern Australia, devastating lives, livelihoods, property and the natural environment. And then came the COVID-19 pandemic, with its health, social and economic costs, each of which will be with us for quite some time to come.

In each of those crises, technology has had a role to play in responding to events, conveying information and helping decision-makers make the right choices. And all of this has operated at a personal level as well as within the business, not-for-profit and government sectors. Without the range of information and communication technologies available in 2020, it's probably fair to say that our society would not have coped as well as it has.

As this issue's lead story about Victoria's bushfire response demonstrates, information technology — particularly that which is cloud based — can swing into action very quickly, enabling governments to respond rapidly and deploy services in a matter of days (instead of weeks or months as previously). And the flexible nature of cloud and as-a-service technologies means that systems can be swiftly adapted and improved as the need arises.

This flexibility became very apparent once the COVID-19 restrictions hit, and thousands of businesses and millions of employees suddenly had to change the way they work. Virtual meetings, webinars, home deliveries and online transactions (to name just a few) quickly became the norm, with some saying that many of these changes will remain even after the pandemic panic has abated.

But can you imagine how we would have coped had the pandemic hit us, say, 30 or 40 years ago? No internet, no laptops, no mobile phones, no cloud — barely any tech at all. Millions would not have been able to work remotely, and either almost the entire economy would have had to be shuttered, or else it would have had to have been business-as-usual but with an invisible virus rampaging through the workforce. Perhaps that's one silver lining we can take from this whole experience — that, while our preparations and responses may have not been perfect, nevertheless we had many of the tools we needed to tackle it head on, and we've made good use of them.

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



**PUBLIC
SECTOR
NETWORK**

OFFICIAL EVENT PARTNER
publicsectornetwork.co/events

FREE SUBSCRIPTION

for government tech professionals

Visit www.GovTechReview.com.au/subscribe

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

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

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



WELCOME TO THE EMPOWERED CLOUD

**Better together: We're accelerating the
power of AI for everyone.**

SAS and Microsoft are joining forces to define the future of analytics in the cloud for our customers. This strategic partnership integrates SAS[®] analytics and AI with Microsoft cloud solutions: Azure, Microsoft 365, Dynamics 365 and Power Platform. Our shared vision enables customers to easily run their analytic workloads in the cloud to meet business goals faster and drive innovation cost-efficiently. Now our customers can unlock even more critical data insights on the path to digital transformation.

It's time to reimagine analytics in the cloud.

sas.com/microsoft

STATE OF EMERGENCY

Heather Boerner

ORACLE HELPED THE VICTORIAN GOVERNMENT
ASSIST BUSHFIRE VICTIMS BY DEPLOYING A
SaaS CUSTOMER RELATIONSHIP SYSTEM IN JUST
THREE DAYS.



©stock.adobe.com/au/Leah-Anne Thompson

Australia, and indeed the whole world, has been through a lot of trauma lately, and it doesn't look like easing up anytime soon. The devastating summer bushfires were awful enough as they were happening, but now comes the long struggle to help those affected get access to the services they need as they work to rebuild their lives. It will be a multi-year effort.

In times of crisis, it is easy for the populace to become overwhelmed and for public services to be stretched to the limit, which is why it is more important than ever that governments are able to respond quickly and flexibly to rapidly changing needs, particularly when it comes to digital interactions with departments and agencies.

"When we're doing true disaster response, we need to find a really good balance between the speed of the response that makes the solution actually useful and a solution that has enough functionality and is good enough to provide immediate service," said Peter Still, Senior Principal Product Strategy Manager for Public Sector CX Applications at Oracle.

"It is possible to be really agile, to identify the most important requirements in an emergency."

According to Still, there are three phases to crisis management that government IT needs to get right:

1. **Digital response.** This is immediate help for people in need when a crisis hits, whether it's a bushfire or any other disaster. Solutions should be capable of being implemented within days (or a small number of weeks).

2. **Government service continuity.**

This is about keeping government running and finding new ways to interact with citizens, even when inquiry volumes are very high and traditional office services are disrupted.

3. **Agile recovery.** This is about implementing systems to support the environmental, economic, health and social rebuilding.

"The most immediate request is for immediate updates about what is happening with the crisis, eg, Where is the fire? Do I need to shelter in place? Am I allowed to go to work?" Still said.

"That's followed closely by the need for immediate information about assistance and for personalised advice — working out automatically what people are eligible for and helping them register for assistance."

Such information is vital for getting through a crisis and rebuilding on the other side of a crisis.

Putting all of these steps into action by enlisting the aid of Oracle's cloud services was essential for the success one Australian government had when coping with the aftermath of a terrifying calamity.

FACING THE FIRE

At 3.00 am on the morning of 7 February 2009, the barometer showed 4% humidity and a whipping wind buffeted Rita Harris's sheep farm in the Victorian town of Taggerty. By 11.00 am, it was so hot that the hairs on the back of her legs singed in the stifling heat. It was obvious that this was going to be an extreme day.

That would prove to be an understatement.

>>

Crisis response

By midnight, the power and phone were out and Harris was choking on the thick orange smoke and swirling ash coming from fires raging in the bush. She'd taken to watering down her house every few minutes to hedge against catastrophe. Flames nearly 70 metres high were towering over the 15-metre-high trees in her yard. Nearby petrol tanks were exploding at regular intervals. She describes the sound of the fire as deafening, like a thunderclap that goes on for hours.

"We thought there was a nuclear bomb," she said. "It was literally like that. We stood there basically waiting to die."

The fires started on what is now known as Black Saturday, scorching hundreds of thousands of acres and killing 173 people. At the time it was the most devastating natural disaster in Australia's history.

Harris, however, was one of the lucky ones. Her house still stood. But she was shaky and disorientated when she arrived at a relief centre in Yea, some 80 kilometres from her property. Then the horrifying reality began to set in: Had her friends and family survived? Could she

continue to earn a living? What would happen next?

CRISIS INTERVENTION

As the fires raged in Taggerty, another crisis was heading towards the then Victorian Department of Human Services (DHS, now the Department of Health and Human Services, DHHS). Thousands of people were displaced from their homes or injured, or their businesses were destroyed. That meant a wave of displaced and traumatised people looking to the government for assistance.

In short order, government officials realised they would have to hire hundreds of new case managers to assist government agencies in targeting services to priority areas. This required a case management computer system that could track the survivors and connect them to the services they needed — and be nimble and scalable enough to evolve as the crisis changed.

"The enormity of the event and how quickly it occurred really put a lot of pressure on us to make decisions and get things in place very quickly," said Grahame

Coles, the then chief information officer at the DHS, whose team was tasked with creating the system that would support the relief effort. "We knew on Wednesday that we had to get a system in place by the following Monday."

Although DHS had had a PeopleSoft case management system from Oracle in place, it was configured for existing processes and could not be quickly modified to meet the demands of the still-developing emergency. So Coles and his team searched for a new solution. Just 24 hours after the Victorian premier's announcement that each survivor would have an assigned caseworker, Coles had selected an Oracle cloud solution platform for DHS case management.

Oracle staff set to work, configuring the solution to meet the needs of Victorian bushfire managers as they were deployed in the wake of the fires — a system that was both nimble and secure. It had to be simple enough for new case managers with no computer experience to navigate intuitively. It needed to display all the necessary case data on a single page, to simplify data input and

>>



©stock.adobe.com/au/jamperary

Secure remote
cellular
connectivity
for commercial
applications.

Remote asset monitoring and control
for real-time polling and response.

Cybertec produces innovative, reliable and high performing commercial and industrial communication devices, built for the Australian environment.

- ✓ Designed and made in Australia for our conditions
- ✓ Compact rugged metal design
- ✓ Industry leading security and VPN options
- ✓ Each modem is burn tested to ensure years of reliable operation
- ✓ Wide operating temperature
- ✓ 5 year industry leading warranty



CYBERTEC

A Madison Company



madison
Technologies

Connect with confidence.

Madison Technologies has been the distributor for Cybertec for over 12 years, providing a range of hardware solutions locally across our national supply chain, and a team of experienced sales and technical support engineers specialising in Cybertec products.

Sales Enquiries 1800 72 79 79 www.madison.tech

well connected

In only three days, the system was built and launched, tracking and assisting the 400 new case managers and the help they offered clients. “I have seen a very creative and pragmatic approach to crisis response from the government organisations I have been privileged to work with.” — Peter Still, Oracle

allow for a case file to be printed with a single click.

Case managers also needed to track survivors as they moved from one temporary home to another. The system also had to be accessible through a secure internet connection for case managers on the road. And it had to be flexible and scalable enough to handle an influx of hundreds of new users and thousands of new cases.

“The case managers were being inducted and basically had 30 minutes’ training on how to use the system,” Coles said. “So when we had a look at the options, that was one of the main criteria: Can the system be basically self-taught? Can we get it out there with 30 minutes’ training?”

In only three days, the system was built and launched, tracking and assisting the 400 new case managers and the help they offered clients. It also managed the disbursement of more than \$350 million in private donations to families in need and the distribution of 26,000 pallets of material goods offered by fellow citizens. This donation management system received an award for innovation in public sector policy.

SILVER LINING

The Oracle cloud solution was a software-as-a-service (SaaS) solution using remote web hosting and secure web connections to link caseworkers with officials in Melbourne. This was especially important because in the far-flung rural areas of Victoria, where the fires devastated whole towns, there was little electricity, there

were few government offices and there was almost no time to compile notes gathered from weary fire survivors.

By deploying a SaaS solution, DHS ensured that the system would be accessible by wireless devices as case managers moved from one devastated community to another. The SaaS solution also allowed officials at the headquarters in Melbourne to monitor what was happening in the field so they could provide the help survivors needed.

All the case managers had to do was enter their username and password, and they gained access to the files for all their clients: permanent addresses, temporary addresses and any information already gathered about loss of property, loss of family members, business losses and the services available and appropriate for them.

However, the technical expertise of the case managers was quite varied: indeed, some had never owned a mobile phone, let alone worked with a cloud-based case management system. But Cindy Tarczon, a contract case manager who worked with Harris in the aftermath of the fire, said that the straightforward, single-page design of the system made it easy for case managers to learn and navigate. “It was very user friendly and we were able to get up and running without any need for formalised training,” Tarczon said.

In the first four weeks, 4000 cases were added to the system. By the end of the year, 5500 people were in the system. And because officials in Melbourne were able to capture and collate the information coming in from case managers, they were



able to quickly create social programs or mobilise services specific to the problems in a given region.

Tarczon believes the government’s response was quicker and more precise with Oracle’s cloud solution because the case files gave government workers a real-time snapshot of what was going on in the fire zone. “We were able to quickly gather accurate information from our clients about what was needed, what the thoughts were on the ground for those people in the community and what welfare agencies and other support agencies really needed to be doing to be effective in this disaster,” she said.

PICKING UP THE PIECES

Another aspect of addressing the needs of those displaced by fires was delivering government aid once they were out of harm’s way. As the recovery effort kicked into high gear, the information that



© iStockphoto.com/Ash-Anne Thompson

case managers in the field needed was changing too.

Because the Oracle cloud system was simple to use and easy to control, officials were able to upload new versions of forms, policies and other pertinent data, preventing case managers from operating on inaccurate information that might delay help to their clients.

“We put up the guidelines, the policies, the consent forms. All of the documents they would need on a day-to-day basis, we were able to post on there. They could all easily access it and it allowed us to manage version control,” said Colleen Clark, the then assistant director of the Victorian Bushfire Case Management Service.

After the fires, Harris formed a close bond with her case manager Tarczon, who arranged financial assistance and access to services. At a time when Harris was still struggling with the losses she

and her community had endured — and when she was still waking every morning to a landscape that looked more like the burnt crust of another planet than the Taggerty she knew — support from the DHS was something she couldn’t have done without.

“I’m glad somebody’s thinking of the big picture,” Harris remembers thinking. “It meant that we went home thinking that the next couple of months were organised. You just have no idea of the impact of having five and a half weeks of not knowing if you’re going to lose your home or not and gradually discovering that friends of yours have died.”

TAKING IT ONLINE

Technology has changed a fair bit since 2009, and citizens’ level of comfort with dealing with governments through technological channels has greatly increased. Indeed for many, especially the

younger generations, digital engagement is the expected norm.

“That 2009 case study is the best example I’ve seen of something that was deployed incredibly rapidly. It was deployed in a really disciplined way to start helping people almost immediately,” Still said.

“But what has changed a little bit since then is [that] there’s more focus on self-service and using modern digital channels to provide assistance.

“The model in Victoria in 2009 was that we were assisting people to register for the emergency benefit programs that were available. But it was done largely using case workers,” he added.

“We still absolutely support that today, but I think... most people when they can would prefer online self-service, whether it’s through a chatbot or through the web.”

OTHER SUCCESS STORIES

As a disaster unfolds, governments need help to automate and manage services that people rely on, but which are disrupted in a disaster. This is partly about moving transactions that people might otherwise conduct in person, to online. And it’s partly about providing a CX platform to empower employees, who are used to working in an office but now need a way to route work between them rather than talking across the cubicles in an office.

Over the longer term, social services programs, unemployment assistance and other initiatives need to adapt quickly, and ensure excellent service; there needs to be a low rate of fraud, waste and abuse; and there must be the ability to keep adapting to meet government outcomes.

“Security is always important in government, too, so we cannot compromise on that... and it has come up often in discussions I have with customers,” Still added.

“Usability is important to drive adoption as well, eg, to ensure that employees can work in a new environment or to encourage citizens to try self-service even if they transacted with government in other ways before,” he said.

>>

Crisis response

Oracle's SaaS solutions have helped governments around the globe achieve some remarkable results. Take France, for example. One of its agencies used Oracle's CX solutions to transform its citizen social benefit experience to 100% digital via omni-channel for 30 million of the country's people. Deployed within five months, it supported 10 million transactions in the first four weeks with a peak volume of two million transactions per hour.

Then there was the major US government agency that used Oracle CX to launch an interactive tax assistant, enabling 24/7 self-service customer access to tax information and FAQs. The same technology enabled it to rapidly deploy a rebate calculator in the wake of the 2008 financial crisis. And it also powered the agency's 20,000-plus customer service representatives spread across 256 call centres and 54 service centres.

CREATIVE SOLUTIONS

So what has driven this agility and the ability to respond quickly to fast-moving events?

"I think two things have changed," Still said. "The first is that governments are

changing. I have seen a very creative and pragmatic approach to crisis response from the government organisations I have been privileged to work with."

Still says that while government IT has a reputation for being slow and deliberate, he has seen governments make creative use of solutions they already own and also focus on very quick implementations and smart solutions for immediate problems.

"We have seen a number of governments set out to implement new solutions in less than a week, which is very unusual for enterprise citizen experience solutions — but it may be the start of a culture change that will stay with us," he said.

"The second thing that has changed are the solutions that vendors like Oracle can provide," he added. "We can deploy software very quickly in the cloud, without customers needing to worry about procuring hardware, figuring out how to install the software etc.

"In addition, even though every government organisation is a little different, and has somewhat different requirements, our SaaS products have a strong foundation of functionality and best practices built in, which helps governments get started very quickly.

"That could be with advice wizards and knowledge searching on a portal, management of service requests, running a contact centre or even managing complex cases for citizens who have been badly impacted," he said.

SMOOTHING THE WAY

One of the main advantages of online, self-service solutions is that they are available 24 hours per day and don't lead to the problem of huge activity spikes (eg, on the phone) during business hours, as seen recently with people calling Centrelink for assistance during and in the aftermath of the bushfires.

"Part of the global solution we have today is called the Oracle Intelligent Advisor. This was actually invented in Canberra and is still built and maintained in our Canberra office. It lets you take very complex government policies and turn them around so that it generates automated advice," Still said.

Helping people help themselves by smoothing the way to finding relevant information, linking to the correct online forms to fill out or guiding them through the maze of red tape is often far more effective than the traditional methods, Still said.

"If you talk about chatbots, or a website, or a chat session with a human operator, or a phone call... the direction we're taking is [that] all of these things should be joined up, and it shouldn't matter how someone makes that contact," he said.

"At the end of the day an interaction is an interaction, so you should apply the same logic to work out whether someone's eligible for fire assistance, what their payment would be.

"From the point of view of a government, you can be much more agile and deploy much faster if you can define how an interaction works — what the rules are — one time, and then they'll always be consistent; you only have to build it once."





ABB Wireless

Broadband wireless mesh technology

ABB's broadband wireless mesh technology is specifically designed to meet the demands of IP-based applications for industrial operations in the utility, oil & gas, mining and smart city markets.

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





STANDARDS SET THE SCENE FOR SECURING DATA

Daniel Chidgey*

STANDARDS AUSTRALIA IS WORKING WITH EXPERTS TO DISCUSS THE ADOPTION OF AN INTERNATIONAL PRIVACY STANDARD FOR INFORMATION AND DATA MANAGEMENT.

Our daily lives can be accounted for in infinite patterns of 0s and 1s. These represent the data collected from

the actions we take, from buying a stick of gum with a credit card to uploading our passport to confirm our identity. All this data is fragile and important. This is no more apparent than with the current conversation surrounding the federal government's COVIDSafe app. When announced, Australians were quickly assured this vital tool would keep data safe and secure. So it's no surprise data and cybersecurity are on everyone's mind.

From smart cities to international cybersecurity, Standards Australia works across numerous sectors in an attempt to support and protect essential data. Whether it's privacy, storage or ethical considerations, Standards

Australia continues to assist consumers, governments and industry in order to support consistency, security and safety for all Australians.

MANAGING PRIVATE INFORMATION

Whatever business you're in, data privacy is an increasing priority. Anyone who comes into contact with personal data and information must take care in handling it. It is important organisations are supported in managing people's private information, specifically in relation to privacy concerns and stricter requirements.

Standards Australia is working closely with international experts to discuss the adoption of the international standard ISO/IEC 27701, *Privacy standard information and data management*. The committee involved intends to modify the standard for Australian use while aligning our privacy requirements with international functions.

The standard provides guidance for establishing, implementing and maintaining a Privacy Information Management System (PIMS) in order to best manage information and data in any capacity and support the privacy of such. The standard is aimed at being applicable for organisations of all types and sizes.

These standards will help professionals and industry manage their data in a way that supports the safety of Australians in their communities and internationally. Standards Australia will continue to work with our international partners to give Australia a voice and stay at the forefront of data management.

STANDARDS SHAPING SMART CITIES

So far this year, Australia has adopted several international standards to help shape smart city development. Standards Australia has worked with international bodies to modify and adopt standards which will aid the effective development and implementation of technologies essential to functioning and successful smart cities.

>>



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



The foundation of smart cities is data collection, and the use of this data in order to provide solutions which aid efficiency, sustainability and progression for communities. For example, a smart city can use the information collected by cameras to help reduce traffic congestion and improve flow.

While these improvements and initiatives are designed to produce better living conditions and communities, the entire project is founded on data. The protection and ethical use of this data is essential to the success of smart cities and through working with professionals from across the world and industries, the expertise involved in developing standards provides a unique opportunity for standards to support the correct storage and precautions for data collection and use.

The foundation of smart cities is data collection, and the use of this data in order to provide solutions which aid efficiency, sustainability and progression for communities.

Internationally, there is a range of standards focused on smart cities that have already been developed by the International Organisation for Standardization (ISO) to support future smart city initiatives across the globe.

The adopted standards aim to assist governments at every level to understand and measure improvements that can be made as communities and cities begin to expand.

ISO 37120 *Sustainable cities and communities — Indicators for city services and quality of life*. ISO 37120 has become an international reference point for sustainable city indicators; it outlines indicators that measure the performance of city services and quality of life. Indicators are an important tool that help cities establish a baseline to measure and evaluate performance.

The standard aims to provide a uniform approach to what is measured and how measurement is to be undertaken and can be utilised by cities regardless of size or location.

ISO 37123 *Sustainable cities and communities — Indicators for resilient cities*. This standard intends to set out requirements for cities to measure their responsiveness in recovering from either natural or man-made disasters. As Australia is often subject to extreme weather conditions, this standard has the potential to assist cities, regional hubs and other communities understand and improve recovery processes.

ISO 37101 *Sustainable development in communities — Management system for sustainable development — Requirements with guidance for*

use. Sustainability is an integral part of the management and development of smart cities and ISO 37101 aims to provide cities with the tools to become more sustainable. The standard targets environmental, social and economic issues, including improved community services and socioeconomic benefits, as well as supporting clear purposes for sustainable development in communities and encouraging sound planning systems to achieve them.

INTERNATIONAL DIGITAL ECONOMY SECURITY

A recent report estimated Australia's rapidly growing digital economy will contribute \$139 billion to the GDP by the end of 2020. One of the biggest challenges to this growth is cybersecurity concerns.

In February of this year, Standards Australia released a report focused on cybersecurity in the Pacific region. The Pacific Islands Cyber Security Standards Cooperation Agenda outlines recommendations to strengthen cybersecurity in the Pacific Islands through the use of standards. (In the context of this report, the Pacific Islands involved include Fiji, Papua New Guinea, Solomon Islands, Tonga and Vanuatu.)

The report sets out recommendations around greater access to funding, resourcing and technical assistance including the development and adoptions of cybersecurity standards from international partners. Proposed standards in this space are hoped to provide essential support and framework to protect business data, to in turn help build confidence in clients, customers and partners in Pacific nations.

Working with international partners is a key pillar to the successful development of standards, and Standards Australia plays a pivotal role in these relationships. While standards are an important tool in supporting legislation and policy, it is the act of working together across international borders to provide shared knowledge and information that supports these possible outcomes, such as this report.

SUPPORTING DIGITAL EVOLUTION

The digital world is constantly evolving, and Standards Australia is committed to proactively working to support and provide a foundation for these ongoing developments. Standards Australia welcomes and encourages feedback from our stakeholders and Australian communities.

If you're looking for more information or would like to give feedback or discuss opportunities in this sector, please reach out to our Stakeholder Engagement Team at SEM@standards.org.au.

**Daniel Chidgey is Head of Stakeholder Engagement for Standards Australia.*



© Stock.AdoBe.com/au/Anek

The COVID-19 pandemic has significantly impacted all levels of Australian government departments. It has reinforced the

urgency to upgrade existing infrastructure and technologies to transfer and secure data efficiently. Modern technologies are no longer an operational desire; they have become a necessity.

A better-connected workforce ensures communications with team members are more efficient. Government workers and MPs can benefit with from communications tools to remain connected in the office, at home and on the go.

Businesses must take extra steps to make sure their employees are not only connected to the Internet but also use the right equipment. It is essential that devices can prevent cyber security threats and integrate with enterprise systems that would otherwise stay within office walls.

Powertec has over 90,000 installations in Australia and New Zealand, including large companies, government departments, small to medium-sized businesses, farms, aged-care facilities, hospitals and individual consumers. Below is a case study by Powertec which

details the capabilities of their cellular signal booster, Cel-Fi GO.

Case Study: Cel-Fi GO in a Government Building

Business Profile & Needs

A purpose-built, two-storey Government building located in Wacol, Queensland reported that they were receiving virtually no reception on the lower floor and sporadic connection on the upper level. The custom construction of this building includes acoustic products, incorporated into the fabric of the walls of several rooms which prevents the penetration of mobile phone signal.

It is essential for management and employees from this building to receive 3G/4G mobile signal throughout the entire building, including crucial departments. To ensure adequate signal levels are dispersed throughout the building, Powertec Telecommunications were engaged to develop a mobile signal coverage solution.

Product/s Used

- 6 x Cel-Fi GO Stationary Units
- 3 x Blackhawk LPDA Antennas
- 2 x Blackhawk Collared Roof Mast 2 M
- 11 x Pulse Larsen DAS Antennas Ultra-thin

Legal and approved, Cel-Fi GO is a one-box indoor coverage solution capable of boosting both 3G and 4G mobile signal. It is designed to dramatically boost voice quality and increase data speeds for several applications.


Operating on all 3G and 4G frequencies in Australia and abroad, Blackhawk antennas can be used in a range of residential, commercial, and industrial mobile broadband applications on any mobile network. This is the ideal external antenna for Cel-Fi repeater systems.

Business Benefits

The Cel-Fi GO installation has provided this government building with a strong and reliable 3G/4G mobile signal in all areas of the building. Powertec Telecommunications offer a large variety of products and solutions for cellular signal, Wi-Fi, IoT and more! Contact the Powertec team today on (07) 5577 0500 or visit their website www.powertec.com.au to view the product range.



**Powertec Telecommunications
Pty Ltd**
www.powertec.com.au



COVID-19 Crisis Management: If Public Cloud isn't the answer, then what is?

C OVID-19 is on everyone's minds. It's undeniable. But we've seen amazing resilience in Australia and New Zealand. It's been far from business as usual, but companies, people and our government have continued working because products and services still had to be delivered and work had to be done. Access to data, information and applications had to keep up. IT teams have been striving to quickly get everything out of their technology infrastructure that they can, to support a sudden increase in the need for remote work, access and

digital service capabilities. People expect the tools they need to "just work" and that's quite a challenge.

When it comes to "agility", "digital transformation" and "scalability", COVID-19 has forced many organisations and agencies into overdrive. As restrictions ease and we can see "getting back to normal" on the horizon, IT departments are going to have to support a new normal. One that will need the agility, flexibility and digital capability to scale, provision and prepare for fluctuations in service and remote work requirements that may still be faced.

"Despite the urgency of the COVID-19 situation and the rapid pace at which

organisations and government agencies have had to ramp up capabilities, it's possible to make decisions that set you up properly for the longer term," says Adrian Johnson, VP and Managing Director, Hitachi Vantara ANZ.

"As a technology provider, we've developed or adapted solutions to help organisations meet the challenges of the moment, like delivering desktop and application experience to a suddenly larger remote workforce. But those solutions wouldn't be much good if they were only designed to help for now. They have to be foundational, giving companies infrastructure that can be built upon. That's what infrastructure is supposed to be," says Johnson.



© Stock Adobe.com/au/Seventyfour

Use Case: Public Sector Business Continuity Challenges during COVID-19

Public Cloud is not for Everyone and Everything. Thanks to the cloud and modern collaboration tools, the technology exists for an organisation or government agency's staff to work from wherever, using whatever device they prefer. But not all workloads, applications or data sets are suitable for the public cloud. Government agencies have regulations in place that mandate the security of on premise solutions. Many organisations have elements of their business best managed on premise. The current Federal government policy, and

that of many organisations, is "cloud first". A modernised policy of "Hybrid Cloud first" would be a better approach for now and for whatever comes next.

Dealing with Business as Un-usual

Faced with this unprecedented pandemic situation, a number of Federal agencies worked with Hitachi Vantara and VMware to rapidly establish and scale virtual desktop services with a hyperconverged, bundled solution platform offering public cloud-like capabilities, in adherence with on-prem requirements.

"Because Hitachi Vantara has been a very strong partner of VMware for many years now, we've been able to partner at an engineering level and come up with creative solutions in response to the COVID-19 crisis," says Simon Caruso, VMware Chief Technologist and Solution Engineering Manager, Federal Government.

"Crucially, we've been able to help our public sector customers quickly ramp up and offer private cloud-based capabilities to support a workforce forced to work from home. That solved the immediate challenge in a way that met their governance and regulatory requirements," says Caruso, "but it's not just a short term solution."

The platform enables a private cloud to be built in an agency or department's datacentre, or someone else's, that involves the same technologies and operational stack required to burst to cloud with the likes of AWS or Azure. It's designed and ready to support apps on-premises, in the cloud, or in a hybrid or multi-cloud configuration, managed in a single platform.

Ticking all the Boxes

Building on existing infrastructure. This was no time for rip and replace, but for a solution that is simple, quick to implement and requires no new training. They needed to maximise performance and efficiency, and get the most out of existing infrastructure to realise the ROI on legacy systems.

That's the beauty of augmenting your existing environment with a software defined infrastructure, which is designed for buying in small increments and you can pay as you grow. **Integrated** | With speed of the essence, no

one wanted multiple user interfaces. This solution platform manages other solutions in the environment and works with core VMware solutions. The VMware admin becomes a generalist across all workloads.

Agile. Faced with a rapid increase in the number of employees accessing apps, files and systems remotely, agencies needed their virtual desktop infrastructures established and/or scaled very quickly.

Flexible. The solution needed to manage both on-premise systems and necessary bursts to the cloud, to avoid business disruptions and to ensure interoperability. The platform acts as an extension of the current environment.

Simple & Secure. It needed to be governed, secure and easy to manage, operate and consume.

Disaster Proofed. We had to support modernised disaster recovery plans in case personnel could not access datacentre facilities.

Future Proofed. Dealing with the critical technology needs of the moment were the priority, but the foundation will remain consistent as we move out of the crisis into a new normal. It will support future workloads such as Kubernetes, containers and next generation digital, business critical applications.

Strong Ecosystem

One thing technology vendors can do in a crisis is band together to support organisations and government agencies working hard to keep everything going.

When the COVID-19 crisis really hit, Hitachi Vantara and VMware built on a decade of partnership to very quickly re-architecture and implement an integrated platform and hyperconverged bundle to help federal agencies meet this new challenge.

Integration is great, but when best-in-breed technology vendors align roadmaps and co-engineer solutions to help IT departments in crisis with future-proofed infrastructure, that's even better.

HITACHI
Inspire the Next

Hitachi Vantara
www.hitachivantara.com

AUSPOST HELPS DIGITISE AGENCY MAILROOMS

Dylan Bushell-Embling

A MAILROOM DIGITISATION SOLUTION HAS BEEN DEPLOYED TO HELP STATE AGENCIES COPE WITH THE COVID-19 LOCKDOWN.

Australia Post has helped digitise the mailrooms of 40 state government agencies and other large customers to support their operations during the COVID-19 pandemic.

The company's inbound information management operation subsidiary Decipha has onboarded 40 new customers with a scaled-down version of its mail digitisation solution since the COVID-19 lockdown commenced in mid-March.

These include key government departments in Victoria, Queensland and New South Wales, as well as a number of financial institutions and insurance companies.

According to Decipha Head of Product and Solutions Damian Naylor, the scaled-down solution it is providing is able to be deployed within days instead of months.

He said key considerations during the design of the temporary service were simplicity and the capability for rapid deployment.

"What our customers need right now is an interim solution that digitises mail and disperses it to their nominated digital delivery points. They don't need

all the bells and whistles. That sort of robust solution can come at a later stage," he said.

"This basic version is step one — creating a digital version of the contents of an envelope. We've also been able to offer basic mail classification where we're able to sort mail based on high-level business rules."

But he said there remains a manual element in this digital process that involves sorting general or unstructured mail like contracts, purchase orders and HR-related documents.

"We don't yet have a detailed enough understanding of our customers' specific business rules to know who or where a general document should be sent," Naylor said.

He said digitised mailroom solutions are expected to become more important in the post-lockdown economy given that remote working is expected to remain popular.

"Organisations will have to address this elephant in the room. They're possibly going to have more staff working remotely and more flexible work arrangements. Many of our customers are already considering this and mail digitisation supports this new model of work," he said.

Decipha is already engaged with a number of customers who have not yet signed up to digitise their mail but are considering it as part of their futureproof planning.

These customers typically decided they weren't at a sufficient state of shutdown to warrant digitising mail and were reluctant to sign up for an interim solution that still required manual handling, Naylor said.

"But they're telling us that they never want to be caught off guard again so they're talking to us now about a mail digitisation solution that involves automation, high-level business rules, classification and some form of workflow," he added.

"They want technology that enables information to be distributed throughout the enterprise and is delivered to the right person, team or business function."

Feedback from these discussions could be used to shape the design of future Decipha services that will reflect this increased demand.

Decipha has been offering process outsourcing services including screening, categorising and sorting incoming information into data streams for the past 20 years.

AI IS THE FUTURE FOR DATA IN GOVERNMENT AND EDUCATION

Matt Goss, SAP Concur

FROM AUTOMATING EXPENSE POLICIES AND PROJECTING BUDGETS TO ANALYSING LARGE-SCALE DATASETS, AI AND MACHINE LEARNING ARE GAINING MOMENTUM.

esstock.adobe.com/patlow_denis

Artificial intelligence and its subset machine learning (ML) are often met with some workforce resistance, particularly in the public and higher education sectors. This is fuelled by the fear that the technology may present data security risks and could replace jobs.

Task automation is indeed a key benefit, with more than 30% of tasks able to be automated in 60% of jobs.

But less than 5% of jobs are predicted to be fully replaced. Instead, automation will replace the mundane, repetitive tasks, giving employees more capacity to focus on value-adding and creative tasks.

Monotonous jobs lack stimulation and often result in inaccuracies as the educated, creative employees responsible for these tasks become tired or disinterested, leading to shortcuts or mistakes being made, which can also lead to data security issues.

AI and ML are designed to automate these aspects of the job to reduce errors and cost, while also improving job satisfaction. While the automation

technology continues to run constantly without requiring any breaks, workers can focus on tasks that require their creativity and attention.

This lets them add more value via strategic tasks while the organisation achieves productivity gains when it comes to the automated tasks.

This is especially valuable when it comes to big data. Public sector and tertiary organisations potentially have access to more data than at any time in history, and this data can be used to deliver significant value to business operations.

However, without the right systems to acquire, organise and apply big data, that value can go unrealised.

By using AI, public and private institutions can more efficiently make sense of the huge datasets that contain structured and unstructured data. The sheer volume and complexity of this data means it simply can't be processed by humans. Automating this process via AI provides the ability to make the raw data meaningful and can help data analysts exploit the available datasets to find value.

Public sector organisations are a prime example. They generate and store large volumes of data, such as census data, that can yield significant value by offering insights into what specific groups value, by looking at where, when and how cash is being spent, for example.

AI can capture streaming data, determine valuable attributes and provide real-time analytics that can inform efficient and effective decisions.

AI can also assist in cost containment for public sector and higher education institutions by increasing employee efficiency and providing better spend visibility and analysis.

Additionally, by leveraging ML capabilities such as automating departmental expense policies, organisations can ensure employees and transactions are compliant in real time, reducing the risk of fraudulent activities, regardless of intention.

In the current global climate, public sector and higher education organisations need to cut costs while simultaneously pivoting to meet rapid market changes. Real-time data insights let these organisations more easily adapt as needed.

Using AI and ML algorithms to evaluate data, public sector and higher education organisations can better model and address real-time scenarios while also forecasting probable data patterns that impact business operations.

This visibility lets teams make more informed, strategic decisions and align the business response to keep one step ahead of market developments.

From automating expense policies and projecting budgets to analysing large-scale research datasets, AI and ML are gaining momentum in helping the public and higher education sectors make strategic decisions to pivot and scale their operations while improving employee satisfaction.

Matt Goss is Managing Director, ANZ, for SAP Concur.

WORKING FROM HOME: LESSONS LEARNED

Joseph Sweeney, IBRS
In April 2020, Intelligent Business Research Services (IBRS) conducted a virtual roundtable with senior ICT executives, supplemented by interviews, to identify the key lessons learned during the unprecedented mass migration of staff to remote working during the COVID-19 crisis.

The key outcome from the roundtable was the need to keep an active journal of the reasons behind decisions taken and the lessons learned while enacting business continuity plans (BCPs) during this emergency. All the participants were interested in learning from the past, which is why they had elected to attend the roundtable. However, only one organisation had a running journal of 'decisions and actions in the moment' that could be referenced in the future to look for valuable insights, lessons learned and better practices.

OPPORTUNITY TO SPEARHEAD TECH UPGRADES

Astute ICT executives recognised that board-level demands to get people working from home quickly and effective was accompanied by a need for reliability.

The need for reliability was then used as a rationale to replace or upgrade overdue ICT solutions. For example, one organisation had previously been unable to make a sound business case to replace laptops that had known battery issues. The pandemic changed the equation — with people needing to be productive away from direct tech support, it was decided that the problematic laptops should be replaced immediately, rather than attempting to 'sweat the assets'.

Lessons:

- Business cases — especially those relating to upgrades or modernisation of existing end-user computing or productivity solutions — can be revisited in light of the need to increase reliability. This can include business cases to modernise end-user computing architecture, such as moving away from traditional SOEs (and System Centre Configuration Manager) to the 'self-service' models, such as Microsoft Autopilot.

COLLABORATION AT SCALE AND PRODUCT SELECTION

Staff have quickly discovered that ad hoc communication tools used in the office were not designed to cater for widely

distributed teams or whole-of-company meetings. This requires a rapid round of trial and error in choosing which collaboration tool was most appropriate for which type of meeting. This was accompanied by vendors rushing to modify product UIs to cope with the different use cases demanded by people working from home. The result has been a rapid maturing in understanding about how to select specific tools for specific collaborative tasks.

Lessons:

- Categorise the types of meetings needed by the organisation in terms of scale, level and type of interactions required. Socialise these observations.
- Capture feedback from team leaders to understand which tools are most effective for which types of meetings. Recognise that one communication tool is unlikely to fit all needs and share better practices on which tool to use and when.

SERVICE DESK RESOURCING

A few organisations with outsourced service desk partners reported frustrations with the service supplier's flexibility, and modifying or setting aside contract terms in order to support at-



©stock.adobe.com/au/ana_kolesnikova

home staff. However, more organisations reported that after an initial spike in activity, service desk volumes have returned to a semblance of normality.

One interesting approach mentioned during the roundtable was to immediately put a hold on all 'change projects' in order to reduce ICT management complexity during the pandemic and focus on 'the new business essential of the service desk'. This organisation reallocated ICT staff from frozen projects to bolster support of staff working from home.

Lessons:

- Outsourced support desk contracts need provision for rapid change when BCP plans are enacted, with clear lines of communications, roles and processes defined.
- Consider documenting a process for reallocating ICT staff to bolster staff support during BCP.
- Review support desk logs from the move to working from home, and see where operational improvements can be made or automation applied.

CAPACITY OF SOFTWARE TO HANDLE REAL WORKLOADS

Despite specifications claiming otherwise, some software products

struggled to support the number of concurrent remote workers. Vendor estimates of performance assume relatively low individual worker usage patterns. These estimates have proven inaccurate for real working-from-home scenarios.

For example, Microsoft's Direct Access, VDI infrastructure and some VPNs were unable to handle the volume of activity with the resources recommended in the products' documentation. In most of these situations, organisations were able to quickly scale up the products by adding additional capability, albeit at additional cost.

Lessons:

- Take vendors' capacity claims with a grain of salt.
- Where available, review recent usage patterns (logs, traffic, etc) for critical infrastructure software and test a future vendor's products (and product updates) against these more realistic metrics.
- Define processes to call upon 'elastic scale' for critical infrastructure software in your BCP plan.
- Some vendors waived additional licensing or contract terms related to scale during the lock-down period. Take advantage of such terms if applicable.

DIGITAL MATURITY

There was an overall agreement among participants that the challenges of working from home were dominated by behavioural issues rather than technological. In particular, staff were (and still are) engaging in activities that increase stress for themselves and colleagues. These behaviours included:

- Staff are filling 'dead time' with work activities. As a result, they are negatively impacting their work-life balance.
- Related to the above, staff are not setting defined hours for being 'at work'. Many staff are extending their work hours, or expecting others to be available after traditional hours (especially into the evening).

- Worries about lack of casual feedback on work, social visibility and recognition.
- Isolation from friends/colleagues at work.

Lessons:

- Training programs and policies are needed to ensure people understand that 'off-time' is just as important as 'at work time'. Explicit 'better practices' for work-life and workplace mental health need to be considered. Ideally, this should be accompanied by approaches to share time availability and coordinate team member presence.
- Consider hosting a wellbeing week activity to launch or re-enforce the above program(s). Introduce experts to discuss physical and mental health and better work practices, both for remote working and to prepare people for a return to the office.
- Establish regular water cooler team meet-ups. These may be weekly or even daily, depending upon the nature of the work and team.
- Managers need to engage with teams and give public feedback, as well as one-on-one feedback. It should be recognised that this places additional workload on managers.

PERFORMANCE VISIBILITY

Working from home has shifted team leaders' — and indeed all team members' — attention to output, as opposed to presence. The result is that working from home has increased the visibility of:

- High performers — those team members who produce a lot of work, versus
- Background performers — those whose input may not be as tangible or who are genuinely adding less value to a project than others. In short, working from home exposes performance issues.

IBRS has some concerns over this issue. While many managers believe they are measuring staff performance by output, the reality is that most staff performance appraisals are heavily influenced by presence and time.

The danger with working from home is that presence and time are disrupted, exposing only output. However, a better metric for the digital workforce is outcome.

Lessons:

- Organisations need to rethink/relearn how staff are appraised, given that managers' perceptions on staff performance are likely now forever transformed.
- Managers need to be clear on what expectations they are setting for staff: presence (time), output (deliverable) or outcomes (solutions and quality).
- With regards to performance measurement, organisations must consider the role of children and parenting in remote working, beyond the simply banning staff from working from home if children are in the house.
- Consider Scrum or Agile team meetings both to keep projects on track, but also to build social cohesion and performance visibility, along with the peer appraisal of outcomes that results.

ACT BY PRINCIPLE, NOT PROCESS

The mass migration to working from home has exposed the fragility of many organisational policies and processes.

Remote working policies were particularly troublesome for some organisations, with some clauses being

unworkable (for example, children-at-home clauses). However, the majority of the participants at the roundtable had overcome bottlenecks in policy or process by simply recognising that such policies were written before the pandemic and did not apply.

One respondent commented that their organisation focuses on principles, not process, when making decisions on how to deploy end-user computing rapidly to staff homes.

In all cases, senior executives (COOs, CFOs) gave ICT permission to change or bypass processes in order to get staff working quickly at home. Procurement and asset management processes in particular were modified or ignored.

Lessons:

- Policies and processes need to be updated to deal with a potential second wave of pandemic lockdowns. Pre-COVID-19 policy conditions or processes that negatively impact remote working need to be removed or amended.
- Mid-level managers should not be able to reinterpret company-wide principles. For example, line or business managers demanding staff come in to work for meetings; HR managers insisting that anyone with school children be categorised as 'essential workers' and demanding they attend the office; asset managers refusing to allow staff to take home keyboards, mice or screens and other operational items.

THE NEW NORM?

Roundtable participants' views on what the new normal would look like varies greatly. Some participants believe that after the lockdown, most of their workforce will return to the office and work in ways not dissimilar to pre-COVID-19 environments. Others believe that a portion (20%+) will work from home at least two days per week, and that collaboration/video communications tools will become a standard work platform. Still others argued that as executives now see that the workforce can be managed

remotely, there will be a greater use of gig workers.

What can be said is that the experience of mass working from home has opened eyes to what is possible in the workforce. It has also exposed weaknesses in workforce management practices.

The result is that most organisations have seen a leap forward in digital workforce maturity.

Lessons:

- Consider conducting scenario planning workshops to identify possible futures for the workforce (eg, taking into account global economic trends, local social factors, additional waves of the pandemic, etc). Use the scenarios to inform workforce strategies.
- Leverage the information and insights captured in the organisation-wide BCP journal and create a future state vision (three-year) for the workforce. Whiteboard sessions with key executive stakeholders — in particular, CFO, HR Director, CTO, CIO — may be a quick method to develop this future state vision.

FINAL NOTE

Determining what the workforce of the future should look like is a challenge. The impact of COVID-19 is far-reaching and far from clear. Budgets will also be under extreme pressure.

The good news is, there are formal models and better practices than can be implemented to enable you to make the best decisions possible within the scope of an uncertain future, and the flexibility to respond to the majority of situations.

No organisation will return to a pre-COVID-19 workforce. However, exactly what the new workforce will look like and how and where work gets done is largely dependent on the decisions that you and your executive make in the coming months.

Dr Joseph Sweeney is an IBRS advisor specialising in workforce transformation and end-user computing.



EKA CyberLock securing roads and traffic control boxes

Recently I noticed a traffic control box in a Sydney motorway tunnel and with cars in front of me and behind me travelling at 80 kilometres per hour. This box is as isolated as a lock on a mountaintop in outback Australia, even though it is in a tunnel directly under central Sydney. I thought to myself, “Who would need to access this box?” Answer: the tunnel owners, contractors, Transport for NSW (formerly RMS) and, I would assume, many others such as Telstra (as I had a perfect mobile signal down there). Then I thought of the value of the equipment inside. These traffic control boxes house the vital components that not only keep us safe but also help deliver the smooth operations of our major roads, such as security and CCTV equipment, speed and red-light cameras, and traffic light controllers. So, we have various groups of people, all requiring access to a geographically spread set of boxes that contain sensitive and expensive equipment that is vital to the smooth operation of our road network. This is a security nightmare, normally solved by running a cable

to every door as you would in conventional access control.

The solution is a system that delivers all the benefits of access control but requires no cables or wiring. EKA CyberLock is such a solution.

EKA CyberLock is an electromechanical, key centric access control system. Key centric means the smarts of the systems are in the key, which makes it a portable access control solution and, with the CyberLink App, extremely easy to administer. This administration flexibility is why EKA CyberLock is the solution for securing remote sites, especially when network of sites are spread over a large geographical area such as the abovementioned traffic control boxes or even remote mobile phone towers in outback Australia.

- EKA CyberLock makes a variety of electronic cylinders and padlocks that can be used to secure traffic control cabinets. They are designed to replace the existing mechanical lock cylinders.
- Access is managed on a centralised database called CyberAudit Web management software.

- Users are issued with a 100% electronic CyberKey that is loaded with their specific access profile and customised to their exact needs, thereby making various levels of access for different stakeholders simple to design and administer.
- The battery in the CyberKey also powers the cylinders, meaning the cylinders are truly 100% cable free and require no battery replacement.
- Lost keys can be managed out of the system, meaning you will never need to rekey again because of a lost key.
- Every opening, attempted opening or system change is recorded in the audit trail.
- Users can update their CyberKeys access profile with the CyberLink App on their smartphone.

To find out more about this application go to www.ekacyberlock.com.au or contact us on sales@ekacyberlock.com.au or 1300 722 311.



EKA Cyberlock
www.ekacyberlock.com.au



Public Sector Network connects government organisations across the globe

Our mission is to give public sector professionals a single place to come together, share ideas, and get free, unlimited access to the latest information about critical topics that are transforming the government landscape.

Our government-only community networks help members to find relevant international content and case studies that are critical to your work and can help you save time, and money.

COMMUNITIES WE SERVE



Corporate &
Shared Services



Cyber Security &
Risk Management



Data Management
& Analytics



Defence, Security
& Justice



Digital Government
& CX



Health &
Human Services



HR &
Future of Work



Innovation & ICT



Local Government
& Municipalities



Smart & Sustainable
Communities

For more information:

✉ info@publicsectornetwork.co

Visit www.publicsectornetwork.co

☎ +61 (2) 9057 9070



Neville Cannon*

**GOVERNMENTS
WILL STRUGGLE TO
COMPLETE TECH
OPTIMISATION OR
MODERNISING PLANS
IF THEY'RE NOT
DIRECTLY RELEVANT
TO SUPPORTING
COVID-19 RESPONSES.**

Given the impact of COVID-19, it's untenable that Australian government IT departments or shared services organisations can assume normal levels of activity. Mandated restrictions have caused significant workforce disruptions and a shift to maintaining frontline services. This means that long-term projects associated with optimisation and modernisation have been pushed to the side.

As the short-term immediate response requirements fade, government organisations will seek to strengthen what has been initially provisioned, making sure what is in place is more robust and secure.

In the longer term, recovery will require a critical examination of the risks and mitigations that can be put in place to better meet any similar future challenge. Such an examination will have to consider the requirement for legacy

systems to be able to withstand further stress tests at times of critical need.

Modernisation is no longer an IT desire but an operational necessity. However, any such assessment will be undertaken at the exact same time that governments are facing enormous pressure to focus on the economic recovery phase. Given the depth of measures taken to date, this could last for many years to come.

COVID-19 is forcing governments to undertake previously unacceptable actions. Policy, legislation and responses are now be determined on a daily basis, creating a situation where decisions made at one point in time may prove to be wrong or inadequate later.

The level of disruption and upheaval makes it unlikely that governments will focus on optimising existing processes or modernising systems that aren't directly and immediately supporting emergency operations.

>>

Modernisation programs

ADAPTIVE PLANNING

In the short-term, the continuing spread of COVID-19 will require departments to address numerous challenges, including health care, transporting goods and people, caring for the vulnerable and elderly, seeing businesses close and unemployment.

CIOs should expect unspent project funds to be reallocated, at least in the near term, and staff to be dynamically reallocated as necessary.

In the long term, governments will focus on restoring public confidence and trust in institutions and processes, as well as economic recovery and prosperity. In addition, there will be increased attention on what can be done to better manage and prepare for any such future event.

Future process optimisation is likely to look very different as radically new processes and delivery mechanisms will emerge.

RAPIDLY CHANGING POLICYMAKING AND PRIORITISATION

Normal decision-making has been affected by the strain of rapidly changing policymaking and prioritisation. Governance that may normally have taken place over days and weeks may need to occur in hours.

“It’s likely that new applications to support collaboration and communication will be demanded and existing applications deprioritised.”

Prepare for continuous change by establishing daily staff meetings, adapting governance processes to accommodate shifting requirements and changed priorities, and assessing available resources. Also, capture costs and issues associated with COVID-19 emergency responses and request financial support.

SUPPORTING COLLABORATION AND COMMUNICATION

It’s uncertain what the duration and final outcome of COVID-19 will be. Optimisation or modernisation of existing applications and new processes could prove fruitless if found to have failed the pandemic test. It’s likely that new applications to support collaboration and communication will be demanded and existing applications deprioritised.

Critically review optimisation projects that are halted and determine whether they’re candidates for replacement after the pandemic crisis.

Step up agile teams to create minimal viable products (MVPs) that deliver value and keep pace with continual changes. Also, mothball projects that aren’t vital and release resources for frontline duties.

CHANGES TO PROJECT PRIORITISATION AND FINANCIAL BUDGETING

Post-pandemic reviews will take into account the lessons learned, including what must be built in for future resilience and what must revert or be stopped to deliver savings. Project prioritisation and financial budgeting will be radically altered to accommodate new operational processes.

Capture lessons during the pandemic to build and protect targeted investment business cases in agile and flexible digital solutions, while expecting cuts to operational budgets. Review technologies and solutions to increase organisational resilience by strategically migrating to ‘packaged business capabilities’ that support a ‘composable’ enterprise.

PROMOTING DIGITAL AS THE WAY FORWARD

While facing the immediate pressures of managing the growing and continually shifting challenges COVID-19 delivers, pay attention to lessons learned along the way.

As the crisis continues, capture tactical and strategic lessons to best support arguments for investment in digital capabilities when the time is right.

**Neville Cannon is a Senior Director Analyst at Gartner, focused on the public sector and government.*





TRUST Frontier Software with your payroll processing

Accurate, secure and reliable



1300 376 684
sales@frontiersoftware.com
www.frontiersoftware.com



Frontier
software

Human Capital Management
& Payroll Software/Services

OFFICES IN AUSTRALIA, INDIA, MALAYSIA, NEW ZEALAND, PHILIPPINES, SINGAPORE AND UNITED KINGDOM

FIVE PRINCIPLES TO GUIDE I.T. COST REDUCTION

Marcus D'Castro, ASG Group

SOFTWARE ASSET MANAGEMENT CAN SAVE GOVERNMENT AGENCIES MILLIONS OF DOLLARS AND DRAMATICALLY DECREASE RISK.

With the National Cabinet announcing its three-step plan to gradually remove baseline restrictions and make Australia COVID-19 safe, our nation has begun its careful journey towards recovery.

Yet at a government business level, the sprint that saw agencies rapidly respond to COVID-19 issues and public health requirements by adding new capability and IT capacity to cope with immediate demands has now become a marathon — the finish line is not yet in sight.

The focus for many government agencies and departments has moved beyond implementing measures for business continuity and on to the next stage... dealing with the flow-on effects, such as increased risk and substantially increased IT costs.

Those agencies and departments have a few new challenges to navigate.

For example, there could be increased risk from the use of non-compliant software that was implemented to respond to immediate critical needs, as well as software vendors ramping up client audit activities as an alternative means to achieve their revenue targets.

There are also uncertainties and potential changes regarding budgets due to government spend on COVID-19 issues, with the added unknown of the federal budget delays for FY21.

The impact of this on planned ICT projects is likely to be the cancellation of major programs of work, which creates a shifting landscape for software requirements and usage.

The solution is to find sustainable and innovative ways to cut costs whilst still delivering for citizens.

FIVE PRINCIPLES FOR REDUCING COSTS

Effective cost reduction services look at ways to maximise value from existing investments, without losing focus on customer and growth opportunities. Here are five principles we recommend that government departments and agencies should follow:

1. Make cost reduction a core competency by focusing on continuous, long-term improvement rather than viewing it as a once-off initiative.
2. Tie cost reduction to citizen centricity by focusing on how to reduce costs in a way that uplifts the quality and relevance of services provided to citizens.
3. Find ways to collaborate and communicate. Resilience and cost optimisation can become a lot stronger if they are approached from a community perspective. For example, open dialogue with citizens, your supply chain and other government agencies can reveal new methods of collaboration that leave all participants better off.
4. Establishing a culture of trust is a key enabler to being able to establish a culture of continuous cost reduction.
5. Change the mindset. The traditional approach to reducing costs has





©stock.adobe.com/au/doucefleu

often centred on reducing staff and eliminating projects. On their own these approaches can actually harm efforts to establish a continuous improvement culture and they also close channels from which great ideas often originate. A better approach is to question everything in a holistic manner and constantly use alignment with citizen-centric strategic goals as an evaluation filter for any decision being contemplated.

Group 10 Consulting — a capability arm of ASG — has seen an uplift

in requests for software asset management (SAM) assistance. SAM is a business practice that involves managing and optimising the purchase, deployment, maintenance, utilisation and disposal of software applications.

During periods of major change, effective SAM activities are more difficult to carry out than in normal circumstances. This is mostly due to widely varied software vendor licensing methods — which often are designed to create confusion — and difficulties in determining what is being used within highly complex IT systems.

Successful SAM programs often achieve substantial return on investment results and dramatically decrease risk. For instance, via a SAM managed service program one agency was able to achieve \$33 million savings on budget over a three-year period, and almost \$20 million in cost avoidance. Overall, we have seen government clients save more than \$500 million via SAM initiatives.

Marcus D'Castro is Executive General Manager for Capability and Consulting at ASG Group.



SECURITY THROUGH SLEIGHT OF HAND

Jim Cook, ANZ Regional Director, Attivo Networks

DECEPTION TECHNOLOGY IS PROVING TO BE AN INNOVATIVE AND SUCCESSFUL APPROACH FOR DEFENDING LOCAL GOVERNMENTS AGAINST CYBERSECURITY THREATS.

Tuning into the news, one might easily get the impression that local councils are disproportionately impacted by cybersecurity incidents compared to many other industry sectors.

Certainly in the US, municipal governments have proven easy targets for ransomware. Research shows 44% of them experience daily attack attempts, and a further 30% are unsure how many times their systems are being probed.

A perennial issue is that local governments are comparatively under-resourced compared to other levels of government, let alone compared to the private sector. While the federal government is steadily improving its defences, funding for cybersecurity drops off steeply at state and local levels.

Small agencies with small budgets often find themselves short on both tools and talent, and vital hardware and software updates can often go untended for months or even years. This provides fertile ground for cybercriminals looking to take advantage of an easy target.

A recent audit report in NSW found 80% of councils do not have a cybersecurity policy or framework. Compare this to the private sector, where only 25% of organisations report they are not using a framework (according to a global survey of 1200 security professionals). The NSW audit also found 78% of councils in the state had no central register of cyber incidents, and 76% had not trained all staff in cybersecurity.

“Poor management of cybersecurity can expose councils to a broad range of risks, including financial loss, reputational damage and data breaches,” NSW Auditor-General Margaret Crawford found.

Local Government Professionals Australia, the peak body for local government officers, sought federal assistance at the end of last year to help councils address cybersecurity shortfalls.

Most local government senior executives “are acutely aware of the risks and vulnerabilities in the cybersecurity space but there is a resource gap in defending against them”, according

to Local Government Professionals Australia CEO Clare Sullivan.

“Local government budgets are under increasing pressure here, with reduced revenue-raising capacity coupled with ageing infrastructure, increasing community expectations and cost shifting from other levels of government,” the organisation’s President, Mark Crawley, added.

SINGLE-PERSON (AND SMALL) SECURITY TEAMS

Many local councils have invested heavily in end-point and network perimeter solutions — but once an attacker is through them, things can become very dark, very fast. Some also are restrained by having only a small security team with which to protect themselves, largely due to the cost of assembling and maintaining such a resource.

To prevent such small teams from becoming overwhelmed, and to supplement their skills, many are turning to new types of defensive systems such as ‘deception technology’.

Deception technology uses traps and lures — resembling genuine files, systems and credentials — that are placed within the network to fool attackers into engaging. Even the lightest engagement with these decoys triggers an alert that enables security to quickly respond to the incident and record the attackers’ behaviour.

The overwhelming feedback from those who have adopted this approach is that it solves a lot of use cases at the same time, the most common being detecting and stopping an attack once it has breached perimeter defences. Others include detecting ransomware attacks early, detecting credential theft, stopping lateral movement, and obtaining visibility of internal networks and cloud environments.

Deception technology is already widely adopted around the world and in the last year has begun to see traction with, and positive impact in, securing

Australian businesses. For small security teams, cyber deception has proven to be an accurate and efficient way to find threats that have bypassed prevention defences.

Modern deception will also include trickery that will deceive an attacker into believing that they have received the information they are seeking — whereas in reality, they are given fake data or credentials that will only lead them into a decoy environment and raise the alert of about an attempted object or data theft.

This sleight of hand creates a situation where the attacker can no longer trust what they see or the tools they use. This can be a powerful deterrent when used with traps and lures that keep attackers occupied and away from genuine systems.

The increased complexity for the attacker can be quite effective in slowing the attack, and will often lead them to abandon their efforts and look for a softer target.

Deception technology is proving to be the augmentation and assistance that many single-person and small security teams need to tip the scales back in their favour. By using machine learning, the solution can be easily deployed and maintained without requiring additional staffing. Responders can also react quickly since every alert is engagement-based and comes with the attack details needed to quickly respond to the threat. This is critical for small teams so that they can prioritise their efforts on real incidents and not go chasing false positives or nuisance alerts.

PREVENTION VS PROACTIVITY

Traditionally, cybersecurity efforts have tended to focus on preventative techniques. However, when you consider the growing numbers of breaches that continue to occur each year, this approach alone is no longer sufficient.

Instead organisations should add proactive techniques, to detect early and control the actions of their attacker, into their security mix. They will then be in a better position to detect and derail threats much earlier so that criminals cannot establish a foothold or complete their planned attack.

Taking the time now to examine cyber deception options, and make them a part of a security architecture, will reduce risk and better prepare an organisation for threats as they arise.

Calendar

2nd AUSEC 2020

Melbourne: 9–11 September
Intelligence into new hacking techniques and exploits.
claridenglobal.com/conference/ausec-cyber-security/

AusCERT Cyber Security Conference

Gold Coast: 15–18 September
Speakers, tutorials, workshops and networking opportunities.
conference.ausec.org.au

IoT Festival 2020

Melbourne: 9 October
Explore trends, challenges, opportunities and applications of the IoT.
www.iothub.com.au/iotfestival

Australian Cyber Conference 2020

Melbourne: 27–29 October
Providing leaders with cybersecurity insights and best practices skills.
cyberconference.com.au

Comms Connect New Zealand 2020

Sydney: 28–29 October
Panels, case studies, tech insights and training for critical comms users.
sydney.comms-connect.com.au

Tech in Gov 2020

Canberra: 3–4 November
Two days of learning and networking for government ICT leaders.
www.terrapinn.com/conference/technology-in-government/

Featured product

Conference room devices

Poly (formerly Plantronics and Polycom) has introduced a series of Poly Microsoft Teams Rooms — the Poly G10-T, G40-T and G80-T. These room solutions include audio and video innovations that are specially designed for Microsoft Teams and provide IT managers with a solution for any size of room, from a huddle room to a large meeting room. Easy to manage and with enterprise support, they join the previously announced Poly Studio X family, which will also offer a native Teams collaboration experience.

Poly

www.poly.com/au/en



GOVERNMENT IN THE CROSSHAIRS

Dylan Bushell-Embling

Australia's government sector overtook finance as the second most targeted sector by cyber attackers in 2019, according to NTT's latest 2020 Global Threat Intelligence Report.

Attacks on the government sector accounted for 26% of all attacks on industry during the year, placing the sector behind technology (35%) but well ahead of finance (13%), education (11%) and professional services (8%).

While government was also the second most targeted sector globally, it accounted for just 16% of attacks.

The most common attack types targeting Australian industries include application-specific attacks (40%), web application attacks (20%) and DoS or DDoS attacks (19%).

DDoS attacks on Australian organisations were more common in other regions, the report also finds. Meanwhile, application and web application attacks accounted for nearly 60% of all attacks combined, above the global average of 55%.

The report also finds that the majority (59%) of malware attacks use one of the top five most common malware families in Australia — conficker, zmeu (loTroop), chinachpper, jsp and knife.

But despite the significant hostile cyber-activity targeting in Australia in

2019, NTT's report finds that Australia has a "generally mature cybersecurity profile" — particularly in the finance and manufacturing industries.

The report also includes an analysis of the ways the COVID-19 pandemic is shaping the threat landscape. It finds that phishing attacks leveraging COVID-19 started as early as mid-January, and that attack volumes are escalating daily.

New malicious websites posing as official information sources for COVID-19 data are being created at a rate which sometimes exceeds 2000 per day.

Campaigns leveraging the crisis are also being used to spread a range of malware variants, including Emotet, Trickbot, Lokibot, Kpot and the new ransomware variant CoronaVirus.

The crisis has also caused an increase in cyber attacks on healthcare and support organisations involved in COVID-19 response work.

NTT has also observed the use of an open redirect which pushes information-stealing malware to infected systems, and prompts the user to download a 'COVID-19 Inform App' purportedly from the World Health Organisation.

The report states that the crisis has shown the need for organisations to implement technologies and processes capable of anticipating and preventing attacks and other disruptions before

they can impact regular operations.

NTT is also urging organisations to ensure they're addressing challenges associated with the threat landscape evolving with COVID-19, such as the related surge in remote working.

This requires clearly and effectively communicating changing business and security requirements, policies and procedures to employees, while ensuring employees flag roadblocks to effective collaboration and workflow.

"The current global crisis has shown us that cybercriminals will always take advantage of any situation and organisations must be ready for anything," commented Matthew Gyde, President and CEO of NTT's Security division.

"We are already seeing an increased number of ransomware attacks on healthcare organisations and we expect this to get worse before it gets better. Now more than ever, it's critical to pay attention to the security that enables your business; making sure you are cyber-resilient and maximising the effectiveness of secure-by-design initiatives."

NTT's annual Threat Intelligence Report is based on data from log, event, attack, incident and vulnerability data from clients, as well as analysis from the company's Global Threat Intelligence Platform.

FREE

for government and industry professionals



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



www.WFMedia.com.au/subscribe

AUSTRALIAN MADE



DESIGNERS & MANUFACTURERS
OF 19" RACK SYSTEMS



PROUDLY
MANUFACTURING
IN AUSTRALIA

mfb.com.au

VIC (03) 9801 1044 / sales@mfb.com.au



19" Rack Cabinets
Licence No. 84394

NSW (02) 9749 1922 / sydney@mfb.com.au