

gov tech review



SMART SOURCING

THE NEW AGE OF I.T.

UNDER ATTACK
CRITICAL INFRASTRUCTURE
TARGETED

DIGITAL INNOVATION
TRANSFORMING HEALTH CARE

Rittal – The System.

Faster – better – everywhere.

Discover more:

www.rittal.com/rimatrix-ng

RiMatrix Next Generation

Modular is the way forward

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


Monitoring



Rack


Cooling



Power



Security

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP



FEATURES

6 | Smart sourcing

Leading the public sector
into a new age of I.T.



18 | New era of ransomware puts public sector on alert

What can we learn from
recent attacks?



10 | QIC implements public safety solution

Making safety surveillance
smart



22 | Addressing new critical infrastructure reporting requirements

Understanding
managed detection and
response



14 | eHealth NSW transforms

Creating a sustainable
health system



24 | Technology transforms patient outcomes

Gippsland Health
Alliance overhauls
electronic medical
records system



27 | 5G IoT connections to grow 1100% in three years

28 | Cyber attacks on health care are here to stay

30 | How Western Health tackled digital innovation at speed

32 | Mitigating attacks on critical infrastructure



Cover image: iStock.com/ipopba

Insider



Welcome to the first issue of *GovTech Review* for 2023. The summer break may now be a distant memory, but there is plenty going on in the world of technology and government already this year with security, in particular, remaining a predictably hot topic.

Major international incidents like foreign 'spy' balloons being shot out of US and Canadian airspace — and subsequent sightings of similar objects over China — are fuelling the fire when it comes to security, surveillance and intrusion prevention. Critical infrastructure globally is seen as an increasingly significant target for cybercriminals and nation-state threat actors seeking maximum impact, while hybrid and remote work models look set to stay for a while at least, effectively expanding the attack surface and allowing for exploitation of new vulnerabilities.

We'll no doubt look back at 2023 and recognise it as a turning point, where the acceleration of digital transformation exposed organisations and government agencies to heightened risk of attack and opened new avenues for intrusion, while machine learning, AI and automation were deployed to varying success on both sides of the field. All this, while still deep in the midst of an ongoing tech skills shortage coupled with a worsening threat of economic downturn. Once again, organisations across both the public and private sectors are being asked to derive more from less.

Well, out of adversity comes opportunity, as the saying goes. Technology is being employed in myriad ways, empowering government to address skills shortages, improve customer service delivery and to develop the levels of agility, security and resilience required to effectively meet the needs of its citizens in a continually shifting threat landscape. For every problem or business challenge, multiple solutions arise and, in some cases, those solutions can even solve a seemingly infinite number of problems — ChatGPT comes to mind.

We may live in challenging times, but that also delivers some of the most exciting technology developments and milestones. While that often comes with a degree of discomfort caused by change and disruption, it also leads to smarter, faster and more efficient ways of doing things — and who could argue with that?

I hope you enjoy this issue of the magazine.

Dannielle Furness, Editor
editor@govtechreview.com.au

wfmedia
connecting industry

A.B.N. 22 152 305 336
www.wfmedia.com.au

Head Office:
Locked Bag 2226
North Ryde BC NSW 1670
Ph +61 2 9487 2700

EDITOR
Dannielle Furness

gtr@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Linda Klobusiak, Marija Tutkovska

CIRCULATION
Dianna Alberry
circulation@wfmedia.com.au

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

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

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

VR offers exciting possibility in disability support

A study led by Western Sydney University (WSU) and published in the journal *Scientific Reports* has found that immersive VR technology may offer exciting potential for the disability sector.

Researchers conducted a five-month study involving 31 adults with varying neurodevelopmental disabilities including autism and intellectual disability, and concluded that use of the new immersive Evenness VR Sensory Space technology offered improvement in sensory processing in addition to alleviation of anxiety and depression.

Co-lead researcher Dr Caroline Mills, from WSU's School of Health Sciences and Translational Health Research Institute, said the promising application of immersive VR in the disability sector has exciting potential to inform new practices for organisations who support people with a neurodevelopmental disability.

"Our findings have shown that VR technology may offer a promising avenue for the provision of sensory interventions and an effective calming tool, with the most prominent benefit reported by users being a reduction in anxiety," Mills said.

Co-lead author Professor Danielle Tracey, from WSU's School of Education and Translational Health Research Institute, said the Evenness VR Sensory Space could have effective application as a clinical intervention.

"Given the preliminary nature of this study, we are pursuing more robust future study designs to better understand the benefits and ensure the program can be used in real-life environments to support the people that need it," Tracey said.

The study was conducted in collaboration with researchers from the University of Wollongong, in partnership with The Disability Trust and tech company Devika.

Ken Kencevski, Managing Director of Devika, said the findings significantly support the evolution of the program.

"Dr Mills and the team have allowed us to improve and validate Evenness Sensory Space as we look to increase its positive impact to individuals, centres and communities around Australia," he said.

For more information on the technology, visit the webpage [here](#). The full research report titled 'Exploring the benefits of the Evenness Virtual Reality Sensory Room' is also available on the same site.

iStock.com/Just_Super



iStock.com/Black_Kira

183,000 licences reissued after Optus breach

Queensland's Department of Transport and Main Roads has reissued almost 200,000 replacement driver licences after the Optus data breach late last year.

Transport and Main Roads Minister Mark Bailey said those impacted by the data breach still had two weeks to get a free replacement.

"Over 183,000 cards have been replaced by my department, which is a huge milestone, and in the last month, there has been a significant drop in the number of impacted Optus customers visiting our customer service centres to have driver licences replaced," he said.

"As we've seen a decrease in card replacement requests, free replacement of driver licences will be discontinued from 1 March. Impacted Optus customers who request a new driver licence in person on or before 28 February will still be eligible for a free card replacement.

"I'd like to say a huge thank you to our Transport and Main Roads staff, in particular our IT staff working behind the scenes, and those in our customer service centres who have been working around the clock to deal with a huge number of new licence requests.

"To give you an idea of what they achieved, we generally process around 10 licence replacements per day, but on some days during the last few months our team did almost 15,000 in one day — it's a massive achievement and I'd like to say thank you on behalf of all Queenslanders impacted," Bailey said.

Additional security measures were added last year to minimise the likelihood of repeat incidents and to guide the way organisations verify identity.

"Last year, we added extra security measures to safeguard Queenslanders' identity and changed how organisations such as banks and telcos verified someone's identity," Bailey said.

"One of the benefits of this change is Queenslanders can now replace their card online if their driver licence details are compromised. With the added security measure in place, Optus customers don't need to replace their driver licence because card numbers were not compromised during the breach. After paying the standard replacement fee of \$82.10, Queenslanders can easily order a new card without visiting a customer service centre.

"Being able to order a replacement driver licence online means Queenslanders can take action immediately and receive their card faster. Organisations who put Queenslanders' important information at risk should take more responsibility," he said.

SMART SOURCING LEADING THE PUBLIC SECTOR INTO A NEW AGE OF I.T.

Martin Dube, Vice President of Cloud, Asia Pacific & Japan, Rackspace Technology

AMIDST RAPID CHANGE AND UNCERTAINTY WITHIN THE SOCIAL AND ECONOMIC LANDSCAPE, THE AUSTRALIAN PUBLIC SECTOR HAS FACED SIGNIFICANT PRESSURE TO OPERATE EFFECTIVELY IN OFTEN UNPRECEDENTED DEMAND.

This challenge has been exacerbated by legacy technologies, which have remained difficult to transition alongside flexible working models. However, many organisations have risen to the challenge, stretching budgets, skills and capacity.

For many in the public sector, their digital innovation journey has started with the adoption of cloud architectures to deliver on the heightened expectation of speed, quality and security. In doing so, many have realised they need and want to govern their technologies differently so that they consume services in the right way at the right time.

The public sector during the full impact of the pandemic has been caught short with the limited abilities to fully operate digitally and support Australian citizens' business day-to-day needs. The areas where the needs have

been around are digitising end-to-end processes across the platform to provide a seamless experience and digital services for their citizens, digitising documents, systems-to-systems connectivity, the ability to provide ongoing services with value by leveraging cloud and AI/ML across industries.

This has seen the emergence of a new trend in how organisations approach the management of their IT estates, known as 'smart sourcing'. With this approach, organisations can regain control and leverage a more flexible approach to IT delivery by finding a middle ground between fully outsourced and in-house delivery of IT services.

So, as a by-product of the pandemic and recent economic headwinds, what exactly is smart sourcing, and what are the steps public sector organisations need to take to implement it?

THE CURRENT LANDSCAPE

Outsourcing has been a popular solution across an array of Australian industries, owing to its perceived flexibility and cost-effectiveness. To keep up with Australia's changing economic landscape and the rising boom of new digital services, many see outsourcing as their only option.

However, what many organisations have learnt is that while outsourcing enables access to the services and needs they require in the short term, retaining long-term knowledge within the organisation is near impossible. Organisations are finding themselves stuck in a consistent cycle of reducing their capabilities, in favour of third-party providers.

Public sector organisations are growing increasingly aware of this phenomenon and have taken action, shifting instead to an approach of insourcing and smart sourcing. Control over technology and the rebuilding of in-house skills are being prioritised more than ever.

At the same time, cloud technology has spearheaded much of the private and public sector's digital innovation strategy. Despite this, the public sector has been slow in its transition, delayed by time, budget and regulatory





considerations. Not only this, but many lack the expertise needed to understand and deliver the status quo and the desired destination in terms of services and technology.

With the Australian cloud market set to hit \$20bn by 2025, digital leaders in the Australian public sector are recognising the intrinsic role cloud plays in their plans. As a result, interrogating whether an organisation possesses the correct knowledge and understanding of an organisation's cloud journey will mean many will look to evaluate the best way to source its technology requirements.

Retaining long-term knowledge within the organisation is near impossible.

Digital leaders in the Australian public sector are recognising the intrinsic role cloud plays in their plans.

GETTING SMARTER WITH IT

The accelerated adoption of cloud, along with a growing acknowledgement of the need to bolster in-house IT expertise, has seen many turning to smart sourcing as an agile approach to procuring 'best of breed' solutions.

By leveraging the benefits of both fully outsourced and in-house

IT services, smart sourcing provides an optimal middle ground between these two worlds to create a dynamic and futureproofed technology environment. Beyond this, it allows organisations to explore and nail down the right blend of cloud platforms and hybrid and on-premise systems to form a multi-cloud approach that addresses



each organisation's unique demands. Investment in external and internal skills can also be more easily balanced – paying for the former only when there is real value in doing so and improving the latter so that they retain control in the long term.

However, with the rapid innovation and changes that now make up the digital landscape, leaders need to recognise smart sourcing is a continuous process, rather than a one-off action. It is a thoughtful and strategic shift in business processes to empower IT leaders to consistently identify the right combination of technology services and suppliers that organisations need to evolve. It will need smart thinking to get the most from the array of cloud options available and to find the right fit for its organisation.

KICKSTARTING THE JOURNEY TO SMART SOURCING

A key step in beginning the journey to smart sourcing is to take a holistic view and map out an organisation's current services and technology architecture, including any existing outsourcing contract. This will enable IT teams to track

overall performance, its impact on users and citizens and from there, how it can be better managed to improve results.

With this, IT teams will need to possess a thorough understanding of several key elements of the existing infrastructure. Knowledge of information architecture will be paramount, and organisations will need to consistently assess the critical or commodity nature of each element on an ongoing basis. Inevitably, change in elements will impact other aspects of the whole — knowing precisely which components fit and where is critical to a successful introduction of smart sourcing.

Secondly, public sector organisations must ensure their efforts to improve skills and knowledge are retained and not neglected. IT and organisation leaders must continue to invest in training and education and instil a culture of ongoing learning and development amongst internal teams — particularly as retaining a core internal team offers a degree of agility.

In summary, smart sourcing is focusing on tasking rather than outsourcing so that knowledge is rarely impacted.

TAKE A CONSIDERED APPROACH WHEN IMPLEMENTING SMART SOURCING

While large changes and innovations in technology and business management can enable new opportunities and room for improvement, rushing to implement cutting-edge technologies can be ineffective or, at worst, detrimental. There is no single approach that is the optimal solution for all public sector organisations. With this, many are now coming to realise smart sourcing is a key solution that goes beyond the benefits of either in-house or third-party skills.

Cloud and emerging technology can enhance government operations and support IT teams in what is a highly demanding industry. However, knowledge is ultimately the lifeblood of most organisations today. Through utilising the flexibility of smart sourcing, public sector organisations can better manage the performance of high-traffic and demanding digital platforms and direct talent towards innovative and impactful action.



Using a paper-based Asset Management system is like asking a toddler about their day. The accuracy is debatable.

Discover a simpler solution for Asset Management.

Asset Management can be complicated for any organisation. But when you're working within old Asset management systems, it can lead to constant inefficiency, errors and data duplication. Enterprise Asset Management from TechnologyOne offers one interconnected solution that connects from data input to long-term project management to strategic planning. Delivering you more accurate visibility across the cost and performance of every asset.

technologyonecorp.com/eam

technologyone



QIC IMPLEMENTS PUBLIC SAFETY SOLUTION

Axis Communications

Queensland Investment Corporation (QIC) was established by the state's government to manage its long-term investment responsibilities. It delivers asset solutions across infrastructure, private debt, private capital and real estate, including management of 24 shopping centres totalling close to 1.3 million square metres in gross lettable area throughout Australia.

As the manager of many large shopping centres across the country, QIC invests substantial time

and resources into creating safe environments for its retail tenants, workers, customers and visitors. This focus on safety came to the fore following the onset of COVID-19, during which time Australian shopping centres began to witness a significant increase in self-harm incidents.

In response to this serious industry and social issue, and a specific self-harm incident that occurred at one of its centres in 2021, QIC spearheaded a new safety program called Project Safe-Guard. Involving a bespoke solution for a highly targeted use case,

Project Safe-Guard is designed to significantly reduce the likelihood of self-harm and security breach incidents at QIC's shopping centres.

The project utilises surveillance technology to detect unusual activity by individuals who may be in danger of self-harming or gaining unauthorised access in high-risk areas, such as internal and external high voids, car park ramps and service tunnels. This detection capability enables greater opportunities to reduce and prevent such incidents from occurring, while helping QIC to protect its assets.



istock.com/ben-bryant

Since its implementation, the alert system has successfully helped to reduce self-harm incidents.

MAKING SAFETY SURVEILLANCE SMART

Already claiming fleets of Axis Communications network cameras in its shopping centres, QIC turned to a local Axis partner, PMT Security Systems, to help implement the technology needed, starting with a pilot site at Robina Town Centre, a shopping centre complex on the Gold Coast in Queensland.

“This was an opportunity to look at and assess a shopping centre for different types of risk, and I included other things beyond self-harm,” said Deb

Palmer, National Programs Manager and Project Safe-Guard Project Lead, QIC.

“We looked at misuse of places like car parks, and people entering high-risk areas, and vulnerable areas. At some centres, there are open mall style entrances that are unable to be closed after trade.”

Being a large centre comprising five multi-level car parks and more than 350 stores, Robina Town Centre has large areas that require monitoring by network cameras and the 24/7 security control room at the site, with additional support by security guard foot and vehicle patrols.

PMT Security, Axis Communications and video management system provider Milestone Systems collaborated to develop a solution designed to identify high-risk areas within the shopping centre, guided by historical incident reports and a self-harm audit tool designed in partnership with Lifeline.

For the solution to deliver on anticipated outcomes, it required surveillance technology that could cover wide areas and provide detailed, accurate data. By employing Axis products such as the D2110-VE Security Radar, which has a 60-metre range with a 180-degree field of view, and the Axis Q6135-LE PTZ Network Camera for visual identification of incidents, QIC was able to minimise the technology footprint requirement while realising operational goals.

Other Axis solutions that were utilised in the solution included Axis network cameras with deep learning capabilities, which were employed in multiple locations around the centre in areas where a specific field of view was required.

RULING OUT RISK

Employing the existing Milestone video management system that was already installed at Robina Town Centre, QIC, Axis and PMT Security worked together to establish business rules for the new camera and detection device footprint to alert security team members in the control room of unusual activities at certain times and in certain locations.

“We already had existing, fairly new Axis PTZ cameras with pan, tilt and zoom capabilities for wide-area coverage in Robina Town Centre’s car parks. With this solution, we continued using those PTZ cameras, but added some Axis Security Radars to the mix to deliver more of the full benefits from the existing camera fleet,” Palmer said.

“Many cameras stayed put or moved position for better analytics outcomes. However, if a camera was out of date or couldn’t handle the analytics we needed from it, it was replaced and repurposed.

“We are only using the analytics technology in areas of high risk. The rest of the cameras are still being used in the same ways they were previously,” she said. >



The capacity for the analytics software to work with specific business rules was important to ensure minimal false positive alerts, as this could help to avoid undue workload and fatigue for security personnel.

Thanks to the capabilities of the Axis camera and sensor fleet, such as virtual tripwires, highly prescriptive business rules could be programmed into the Milestone system to ensure most alerts were triggered by genuine incidents.

RECLAIMING CONTROL

Since the implementation of the Axis camera and sensor system at the pilot Project Safe-Guard centre, security personnel have been alerted to, and have been able to prevent, at least two potentially fatal self-harm incidents.

More broadly, the pilot centre has seen a significant reduction in various incidents going undetected, with security teams now able to respond proactively to security breaches in high-risk areas as they happen, helping to prevent the occurrence of facility misuse, including illegal access, loitering and bad behaviour.

Additionally, the new technology has helped Robina Town Centre secure the open-air mall area that was previously difficult to secure after hours. Thanks to the highly accurate virtual tripwire

capability of the Axis network camera fleet providing coverage of the mall, security personnel now have a greater ability to actively monitor the area and prevent its potential misuse by unauthorised visitors after trading hours.

Most importantly, the increased visibility provided by the Axis network camera and radar fleet means security controllers are now able to see things that they previously couldn't see happening. This factor has supported QIC's high-level goal of making sure its shopping centres are safe places for people in the community, even out of hours.

For security personnel, the Axis camera and radar fleet has helped to alleviate the potential emotional stress that can sometimes arise from being in a workplace at which a self-harm incident or fatality may occur. Since its implementation, the Project Safe-Guard alert system has successfully helped to reduce self-harm incidents. This has led to greater confidence among security staff that they can prevent such incidents from occurring.

"I have gone into a control room after recent alerts have stopped a potential self-harm incident, and the positive response from the security team is incredible. They can't believe it has worked, and it's worked several times.

The emotional stress of having to deal with something post-incident can be big," Palmer said.

Moreover, the control with which business rules can be applied to the Axis network cameras via the Milestone system has reduced the potential for false positive alerts. This helps to minimise the risk of alert fatigue among controllers, meaning they are more likely to respond in a timely manner to alerts when they come through because they are likely to be genuine incidents.

THE START OF SOMETHING BIG

With Robina Town Centre being the pilot site for Project Safe-Guard, similar systems have now been rolled out in other QIC shopping centres, including Grand Central in Toowoomba, Queensland, and Canberra Centre, with another five across Australia in progress.

Not only was Grand Central's system deployed in just three months, it has quickly led to a reduction in self-harm incidents and security breaches at the shopping centre. The Grand Central deployment also made use of the Axis C1310-E Horn Speaker, providing security team members located in the control room with the ability to communicate with, or deliver audible warnings to, individuals in other areas of the centre. This is used in security breaches only.

Between Robina Town Centre and Grand Central, at least four potential self-harm incidents have been prevented since the Axis network cameras were deployed to support Project Safe-Guard.

"At Robina, we have built a town centre for the community to come to for more than just shopping, and in doing that we want it to be a safe place. This is all about safety, even out of hours," Palmer said.

"At Grand Central, we've already stopped two potential self-harm incidents, along with multiple security breaches and misuse."

The modern way of working in the public sector



The modern way of working survey 2023

After years of disruption, employees have new needs and new expectations about their working lives and many employers are exploring how they can empower their people to work in more flexible ways and get the most out of their working days.

In partnership with Censuswide, Nuance surveyed professionals within the public sector — to find out what modern working means to them, and identify the new challenges they're facing in their working environments.

The survey also explored how technologies such as speech recognition can fit into professionals' modern working lives and support them in their roles.

A closer look at modern working lives

It wasn't surprising to see so many respondents reporting they've embraced hybrid working — for many professionals, it's been a chance to improve the balance between their personal and working lives. The results indicate hybrid working is popular, with just under half of respondents (43%) ranging from entry-level roles right through to senior management, saying that hybrid working best describes their current working situation.

But despite the many benefits of hybrid working, it does bring some additional

challenges. Respondents struggle with not being able to speak to their teams in person (48%), more interruptions at home (40%), and limited access to tools they'd have access to in the office (36%).

The administration burden

Administration tasks are a crucial part of almost every public sector role, helping ensure services run smoothly, teams work efficiently, and public needs are met. Administrative work remains a burden, with public sector professionals spending on average more than half the working day typing.

How technology can help

The high percentages of time spent typing, means public sector organisations need to be looking to technology to help relieve the burden on their employees, whether they are in the office or hybrid or working remotely.

Public expectations are also driving the need for technology. According to an independent review of the APS (Australian Public Service), 'as the rate of technological change continues to accelerate, and public expectations of the Government increase accordingly, the APS needs to use data and digital technologies to better meet the needs and expectations of the Australian people, businesses and communities'.

31% of respondents to the Censuswide The Public Sector Modern Working Survey, thought that an organisation that uses the latest technology appears to strive for the best experience for their clients and 38% thought they listened to the needs of their employees.

Speech recognition technology

Only 20% of respondents are already using speech recognition technology in their work today to deliver multiple benefits to their organisations, but 67% are predicting their organisation will use this technology in the future.

In The Public Sector Modern Working Survey, we explore the top benefits and challenges of hybrid working, why public sector professionals would rather talk than type, what speech recognition is delivering for public sector professionals and how organisations can embrace modern working with speech recognition.



Scan for your copy of the report.



Nuance Communications
australia.nuance.com

eHealth NSW TRANSFORMS PUBLIC HEALTH SYSTEM

Amazon Web Services Australia



istockphoto.com/matchmeena29

New South Wales (NSW) Health's vision is to create a sustainable health system that delivers outcomes that matter to patients, is personalised, invests in wellness and is digitally enabled. In line with this vision, it is currently on a digital transformation journey to build an even stronger, more flexible, patient-centred health system for its citizens.

eHealth NSW plans, implements and supports information and communication technology (ICT) and digital capabilities across NSW Health by designing and implementing technology solutions to innovate and transform how health care is delivered to patients. With their passion for collaborating with clinicians to build industry-leading healthcare solutions, eHealth NSW is the digital centre of excellence for NSW Health.

From 2021 to 2022, eHealth NSW migrated 10 clinical applications, including mission-critical workloads from its on-premises infrastructure onto the AWS Cloud. With AWS and its managed services, eHealth NSW has reduced manual operational activities, shortened the time to create new environments and achieved performance improvements for its applications. During the pandemic, eHealth NSW was also able to swiftly scale its videoconferencing solution to support staff working remotely, clinicians and patient consultations.

MODERNISING EHEALTH NSW'S INFRASTRUCTURE TO SAVE TIME AND IMPROVE PERFORMANCE

As an ICT service provider for the state's public health system, eHealth NSW handles highly sensitive and personal data. Being on the AWS Cloud,

eHealth NSW can take advantage of cloud-based security services that provide enhanced visibility, and auditing capabilities and controls. This is projected to save NSW Health hundreds of hours per year on manual and reactive operational activities. eHealth NSW uses AWS Security Hub and Amazon GuardDuty to automate security checks, implement continuous monitoring and conduct early threat detection to minimise security risks.

Clinicians and researchers are also seeing improvements to NSW Health's various clinical applications since the move to the AWS Cloud. For example, the Enterprise Patient Records application has realised a 10-fold improvement in performance and a 70% reduction in critical incidents, resulting in faster access to clinical data for frontline clinicians. Additionally, eHealth NSW can implement

enhancements to applications up to 50% faster, as they can now launch new environments in under four hours to conduct testing. In the past, this would have taken them six to eight weeks. NSW Health has already recognised US\$16 million-worth of benefits due to avoided costs, reduction in capital and expenditure and improvements in productivity. Up to 144,000 collective hours of productivity have also been saved for frontline clinicians.

To support growing data needs, eHealth NSW also deployed Amazon FSx for NetApp ONTAP for its Enterprise Image Repository (EIR). The EIR, which is a centralised medical imaging store, currently holds over 1.6 petabytes of diagnostic images and reports, and its data is growing at a rate of 25% per annum. EIR also uses Amazon Relational Database Service (Amazon RDS) for high availability and encryption, and to automate time-consuming database administration tasks, such as software patching and backups.

"We worked closely with the AWS Professional Services team to modernise our infrastructure, allowing us to redirect our resources toward improving the clinical application features and delivering greater value to the state healthcare system," said Farhoud Salimi, Executive Director, Service Delivery at eHealth NSW.

"Additionally, the AWS team has been very helpful in equipping our team with the resources and training we need to manage our new infrastructure."

ADAPTING TO NEW COMMUNICATION NEEDS DURING THE PANDEMIC

eHealth NSW's migration to the cloud also proved to be very timely during the COVID-19 pandemic, when the use of videoconferencing increased by 18 times due to a surge in remote workers and telehealth. With the AWS Cloud, eHealth NSW was able to ensure ample network, server and storage capacity to maintain performance at scale.

NSW Health Pathology used Amazon Connect via the eHealth NSW cloud platform to build a new MVP COVID testing call centre within two weeks. At its peak, the call centre scaled to manage 40,000 tickets per week. To further ease public anxiety, NSW Health Pathology also set up an SMS bot using Amazon Pinpoint. This initially allowed patients with negative results to receive a notification within hours, instead of waiting up to 10 days, and was enhanced throughout the pandemic to include positive results and most recently results for Influenza A, B and RSV.

FACILITATING UPSKILLING OF STAFF AND BETTER PUBLIC HEALTHCARE DELIVERY

Moving to the cloud triggered operational changes and drove the need for new approaches to building, operating and managing applications. eHealth NSW recognised the need to upskill its employees to ensure success of its digital transformation and maximise the value of the cloud.

eHealth NSW worked with the AWS Training and Certification team to establish a multi-cloud stream within its Digital Academy (DA) in 2020.

With nine pillars, the DA is designed to accelerate the digital health workforce of the future by bringing eHealth NSW staff together to learn new skills, put learning into practice, collaborate and share ideas. The DA pillars include Agile, Analytics, Cloud, Cybersecurity, Human-Centered Design, Integration and Interoperability, Safety and Quality, Service Management, and 'Start with the Customer in Mind'. Each pillar seeks to uplift skills, processes and practices internally, and build a resilient workforce.

The multi-technology cloud stream was added to the DA in 2020 and has evolved in the past two years to include a series of pathways for staff to develop the necessary cloud skills. These

eHealth NSW can implement enhancements to applications up to 50% faster.

pathways are targeted towards enterprise architects, cloud engineers, human factors specialists, project managers, data analysts, coders, engineers, technicians, clinicians, business support and experts in many other disciplines.

As of October 2022, the DA has delivered training on AWS to over 1500 technical and non-technical employees. This included a variety of foundational and in-depth courses, self-paced digital training resources, as well as experiential learning events like Lunch and Learns, AWS Immersion Days and Game Days held virtually and in person.

eHealth NSW aims to train a majority of its 2000 staff by 2023, thus equipping its employees with the right skills and confidence to build and manage applications on AWS. The DA has increased the speed at which people learn new skills and opens new cloud career opportunities for diverse learners.

"This mass reskilling pathway is not only providing new skills to ensure staff have long-term viability in the tech industry, but it is also empowering women to be more confident in tech," shared Heather Cardin, Head of Training at eHealth NSW. "It has created a community of shared learning and enablement and improved employee satisfaction."

Looking ahead, eHealth NSW will use the agility and scalability that the cloud offers to advance its capabilities in analytics, artificial intelligence and machine learning to deliver predictive and personalised healthcare services to the citizens of NSW.



iStock.com/freder

Get the Most Out of Your Microsoft Security Investment with an E3 to E5 Uplift

You've invested in Microsoft security services, but are you actually getting full value from your licences? **Learn how moving from E3 to E5 drives a security uplift.**

A few years ago, most governmental organisations were signed up to Microsoft E3 licences as a standard practice. Generally speaking, this made sense — not only was doing so cheaper, but E5 licences didn't have the strength of features they offer today. Today, however, security is something organisations can't afford to ignore due to the evolving threat landscape. If you're

already in the Microsoft ecosystem, it makes sense to explore opportunities to take full advantage of its benefits. In particular, here's how uplifting your licensing benefits your organisation and its security.

How E5 licences uplift your security posture

At a high level, you can think of the integrated, unified security stack of Microsoft 365 (M365) E5 products as an end-to-end

security solution that secures both the whole Microsoft environment, as well as multi cloud and hybrid environments. Upgrading your licensing grants you access to this breadth of security capabilities, as well as new security-centric features — including many that were previously only available as standalone products.

Features gained moving from M365 E3 to M365 E5:

- Azure Active Directory Premium P2 (vs P1)
- Microsoft 365 Defender
- Microsoft 365 Defender for Endpoint P2
- Microsoft 365 Defender for Office 365
- Microsoft 365 Defender for Identity

- Azure Information Protection P2 (vs P1)
- Microsoft Defender for Cloud Apps

Additional compliance benefits gained from the transition:

- Rules-based automatic retention policies, machine learning-based retention, records management
- Advanced eDiscovery, advanced audit
- Insider Risk Management, communication compliance, information barriers, customer Lockbox, privileged access management
- Built-in third-party connections

Features gained moving from M365 EMS E3 to M365 EMS E5:

- Risk-based conditional access
- Privileged identity management
- Intelligent data classification and labeling
- Microsoft Cloud App Security
- Microsoft Defender for Identity

In gaining access to these features, your organisation benefits from: Stronger identity and access management without compromising productivity; stronger threat protection that's streamlined across multiple apps and systems; better protection of your sensitive information; stronger compliance, resulting in easier audit preparation and; the ability to refine who gets access to what on a more granular level.

It's important to note that some of these components may be available for purchase separately. For example, if you aren't ready to sign up for E5, you may be able to add the E5 Security Suite to an existing E3 licence.

Additional benefits of upgrading from E3 to E5

Beyond the new capabilities listed above, uplifting your licensing offers a number of other advantages, including cost-saving benefits. Some organisations may have third party virus or mail scanning software, for example, and these can be replaced through the uplift, with the addition of Identity Protection and the Risk and Compliance Suite as well.

As these third-party tools are taken out of the rotation, two additional advantages are conferred; 1) there is potential for a security uplift as vulnerabilities with third party software are removed and; 2) you reduce the ongoing complexity associated with managing multiple vendors and SaaS products. This influences staffing decisions and helps navigate labour shortages. Standardising across the Microsoft security stack makes it easier to find talent with the right skill sets.

What holds organisations back?

Despite these clear advantages, there are a number of factors that keep organisations from taking the next step forward. One is the sheer size of some governmental organisations, which can involve thousands of users, spread across multiple agencies. Some of these have thousands of legacy on-prem servers in place — the thought of auditing them and making licensing changes is daunting. Configuration is another challenge. It may be easy to turn features on, but they need to be set up and configured properly. But perhaps the most pervasive mindset is thinking that 'we're not worth attacking'. The growing sophistication of modern phishing, spear phishing, and social engineering attacks immediately disproves this. If a hacker can breach a lower agency and pretend to be someone within it, the potential for risk and exposure is incalculable.

How to upgrade from E3 to E5 licensing

Fortunately, overcoming these challenges is not only possible, but it's proven, given the number of organisations that have done so successfully. Once you've committed to making the change, the next step is actually purchasing upgraded licensing — and the good news is that this process is fairly straightforward.

Government in Australia typically has enterprise-wide or government-wide Enterprise Agreements in place with existing pricing, though this varies by state or

jurisdiction. If you don't have an existing agreement, the next step may be purchasing more licensing from a distributor or signing a new agreement. Microsoft is eager to support licensing upgrades and will make the process as easy as possible.

Once licensing is in place, the next question you'll need to address is how to roll out your upgrades. Many of the organisations find the benefits of E5 licensing compelling, but also want a lot of features upgraded and they're wary of doing everything at once. We often recommend incremental upgrades or staged rollouts, planned and executed according to an appropriate roadmap. Dedication to the overall process is ultimately more important than whether you go all-in or do a staged rollout.

Moving forward to optimise your Microsoft investment

If all of this sounds overwhelming, don't worry. Having the right partner on your side makes it possible to minimise complexity while streamlining new implementations in order to get the most out of your Microsoft investment. Not only does Canon Business Services have experience assessing the application architectures of large organisations and guiding them through the uplift process, but we've also written a substantial volume of documentation and IP around automating deployments, removing existing products, and onboarding devices onto new environments in a way that's compliant with government standards.

To learn more about our process for uplifting Microsoft licensing from E3 to E5, contact us to speak with one of our governmental security experts or to inquire about our exclusive Security Uplift offer.

Canon

CANON BUSINESS
SERVICES **ANZ**
business.canon.com.au

NEW ERA OF RANSOMWARE PUTS PUBLIC SECTOR ON ALERT

Ashwin Ram, Cyber Security Evangelist at Check Point

Costa Rica has recently suffered a months-long cyber attack. Organised by the same group that impacted Australian institutions at the end of last year, this attack ushered in a new era of ransomware.

For months, the Central American nation has been on the frontlines of unprecedented ransomware attacks that have impacted just about every aspect of life. Essential services have been crippled, teachers have been unable to collect their pay cheques, doctors have been prevented from tracking the spread of COVID-19, all while international trade has ground to a halt.

It's tempting to think this is trouble in a faraway land. But the chaos is not an isolated incident. Instead, it is the culmination of a recent rise in ransomware attacks across the globe. Not too long ago, in Nov–Dec 2021, there were multiple instances of Australian organisations impacted by attacks from the same cybercriminals, Conti. According to the Australian Cyber Security Centre (ACSC), in addition to ransom requests and data encryption with subsequent impact on organisations' ability to operate, victims also had Personally Identifiable Information (PII) data stolen and published by the threat actors.

And this is just an example. The ACSC observed continued ransomware

attacks targeting Australian critical infrastructure entities, including in the healthcare and medical, financial services and markets, higher education and research, and energy sectors. Since 2019, there has been a significant increase in cybercrimes against Australian institutions that have provided vital services to our population. These happened across multiple government spheres, including, to name a few: the Australian Parliament House Data Breach (February 2019), Service NSW Data Breach (April 2020), Tasmanian Ambulance Data Breach (January 2021), Northern Territory Government Data Breach (February 2021), Western Australian Parliament Data Breach



(March 2021) and Melbourne Heart Group (February 2019).

The simple truth is that cyber attacks can and do happen; no organisation is exempt. The most recent Check Point Research report shows the second quarter of 2022 saw an all-time peak in global cyber attacks. Closer to home, Australian organisations experienced 941 attacks each in Q2 2022, representing an extraordinary 97% increase compared to the previous year.

While the country is rolling out enhanced regulations related to cybersecurity levels via the Critical Infrastructure Act for essential services, it's important to remain vigilant. Still, with threat levels increasing, what can

the government and private sector learn from these attacks, and how can they avoid ending up in cybercriminals' crosshairs themselves?

BEWARE OF VULNERABILITY WINDOWS

Ransomware attacks are rarely the acts of individuals sitting at their computers and randomly deciding when to strike. Instead, threat actors such as cybercriminals, extortionists, nation-state actors, hacktivists etc, plan them meticulously. They can spend weeks, if not months, planning and carrying out reconnaissance to understand their targets and monetise their malicious activities as much as possible.

As a result, ransomware attacks are often executed during times of instability or uncertainty. We've experienced that with the handover of power from one government to another or coinciding with world events such as the start of the war in Ukraine and the onset of COVID-19. These major events act as distractions that make it easier for threat actors to mask their attacks against systems and embed themselves deep into the victims' environment.

These distractions don't even need to be massive geopolitical events like wars or pandemics. For government organisations and businesses operating in critical infrastructure sectors, crippling

essential services can grind whole economies to a halt.

Change in any form brings with it risk. Indeed, in previous years, we've seen ransomware attacks targeted to coincide with national holidays, Christmas and even long weekends. The attackers aim to catch their targets off guard when people's attention might be elsewhere.

We call these "vulnerability windows", and to effectively protect themselves, organisations, whether they're governments or businesses, need to monitor their risk proactively and deploy resources accordingly.

PRACTICE GOOD CYBER HYGIENE

People might view ransomware attacks and think that they result from a massive security breach or organisations not having stringent enough controls. Still, this kind of event is more often than not simply due to poor cyber hygiene.

The concept works exactly the same way as personal hygiene, in that people who maintain their health by taking preventative measures are less likely to get sick, while those who don't, put themselves at a greater risk.

When it comes to organisations, poor cyber hygiene creates chinks in security architecture that attackers can exploit. That's why practising good cyber hygiene is crucial. Simple steps like using strong passwords, multi-factor authentication, updating software regularly, securing backups and cybersecurity awareness training all go a long way to keeping your organisation safe from cyber attacks.

WATCH OUT FOR INSIDER THREAT

Recently we've seen a growing number of attempts by groups like Lapsus and Conti to actively recruit individuals from within governments and businesses to sell remote access credentials. There

are advertisements all over the internet with groups overtly asking for this kind of access and offering good money.

It's not just money that can motivate insider threats; sometimes, the intent can be malicious. Perhaps an individual doesn't agree with the politics and policies of the organisation they work for. Or they're leaving, so they take access with them or leave back doors open for attackers to get in after they're gone.

Whatever their motivation may be, a Zero Trust approach and monitoring are vitally important to reducing the risk of insider threats. Fortunately, the behavioural analytical heuristics that are now set within security programs are specifically designed to spot unusual activity. Used in conjunction with good cyber hygiene, organisations can help to protect themselves from attacks wherever they originate from.

HOW CAN GOVERNMENTS COMBAT THE RISE OF RANSOMWARE?

The problem is that we're not doing enough to ensure that private or public sector organisations are protected from the rise of ransomware. Indeed, while governments have worked to implement stringent measures in areas like data privacy, the same can't be said for ransomware and destructive malware such as wipers.

Many Australian companies, especially those operating with essential services, have completed the Cyber Incident Reporting component required as part of the Critical Infrastructure Act. This is great news for the Australian population. However, even organisations with

the most effective risk and incident response programs should conduct a threat scenario-based risk assessment and reaffirm the business approach to openness, access, protection and compliance.

So, where there should be strong compliance or mandates in place to ensure that organisations are adequately protected, there are instead guidelines and best practices that businesses can choose to follow. It's a crazy situation. After all, in other areas of life, like driving a car, for example, you need to reach a certain level of qualification or capability before you're given a licence. But you don't need any specific qualification or certification to be given the task of securing a business. And until ransomware is treated as seriously as other areas, organisations across the world will be at risk.

DON'T GET COMPLACENT

Cybersecurity can't just be another tick box exercise, and governments must act to set standards and enforce compliance to ensure that organisations are adequately protected.

It's time we started to adopt a risk management framework that ensures organisations are as protected from ransomware as they are from other threats facing their operations. We've got to become more proactive, conducting regular exercises, threat assessments and gap analysis to ensure that we are more resilient to cyber attacks. Because the biggest lesson we can take away from the plight of Costa Rica is that ransomware attacks can and do happen to anyone.



Consider Private Cellular to Enable Industry 4.0

Nathan McGregor, SVP Asia Pacific, Cradlepoint

The Australian Government's National Reconstruction Fund (NRF) provides an opportunity for Australian enterprises to leverage Australia's 5G competitive advantage to lead in the application of 5G-based digital solutions in priority areas. The NRF has the potential to support projects that seed the market to drive 5G-enabled enterprise digitalisation, from advanced manufacturing to mining operations, retail shopping and distribution centres, transport, ports, and logistics. It can also lower barriers to adoption to promote accelerated evaluation and production adoption of digitalisation initiatives enabled by 5G and help drive Industry 4.0 in Australia. While these use cases can choose between a number of traditional wireless connectivity approaches — Wi-Fi or public mobile networks (4G or 5G) — performance, coverage and control requirements of Industry 4.0 often require more. This is where private cellular has become an enabler for early Industry 4.0 adopters globally and should be considered a go-to-platform for Australia too.

Private cellular in practice

Private cellular networks are similar to public cellular networks in that they utilise the same base 4G or 5G technologies, but differ in that they are owned by enterprise, dedicated to a specific site, and designed and operated to an enterprise's specific Industry 4.0 needs. The equipment solutions behind these networks are right-sized for industry, simpler to deploy and simpler to operate than their much larger public network alternatives. A major feature of private cellular networks is that data does not leave the site and always remains behind the secure cyber and physical

perimeter of the enterprise. Data is also protected by strong multi-layered, end-to-end security measures, and these networks are not shared with other users. Licensed radio spectrum is required for private cellular and provides a level of operational security versus Wi-Fi: no other operator is allowed to use the same spectrum in the same area. This restricts private cellular use to areas where enterprises can cost effectively license spectrum, which is currently in remote and some regional parts of Australia, however this is expected to change dramatically over the next 1–2 years as Australia follows other countries and introduces industry spectrum options in all metro, regional and remote markets.

Where to use private cellular vs. Wi-Fi

Private cellular is mainly associated with select verticals today where there are complex networking challenges and low-latency, high reliability needs, such as ports of entry, oil refineries and off-shore platforms, manufacturing plants, and mines: often with hundreds of users and devices spread across a localised or campus area. Wi-Fi is not effective in these circumstances and better suited for more compact areas and IT needs, where connection density, concurrency of use, bandwidth allocation, and security requirements are less demanding.

Cost comparison

Private cellular can offer a lower total cost of ownership than deploying widespread Wi-Fi. The volume of access points and backhaul cabling it takes for Wi-Fi to work well in large facilities makes it a costly investment, with a much longer lead time to deploy. Private

cellular (4G and 5G) reach much farther and support more concurrent connections than Wi-Fi access points. In a large area, this means significant hardware savings for cellular broadband.

Performance and reliability

Wi-Fi also struggles to deliver consistent performance required by high-bandwidth and low latency applications, such as autonomous guided vehicles (AGVs), robot control systems, XR-enabled connected workers and AI and ML-supported video as a sensor. Private cellular enables granular control over device performance, and the ability to enforce end-to-end policies that govern quality of service, throughput, latency, and loss targets.

Migrating across different wireless technologies

There is a growing benefit from adopting a heterogeneous approach to wireless connectivity in enterprises, particularly those moving into Industry 4.0. With the right Wireless WAN solutions provider, organisations can invest in edge devices today that can evolve with their wireless strategy from Wi-Fi to cellular, or allow their operations to utilise all three approaches in a single strategy. Devices that connect via Wi-Fi, private cellular or public 5G networks, managed via a single operating platform, enable Industry 4.0, and protect investments over the long-term.



PART OF ERICSSON

Cradlepoint Australia Pty Ltd
www.cradlepoint.com/au

ADDRESSING NEW CRITICAL INFRASTRUCTURE REPORTING REQUIREMENTS

Jason Whyte, General Manager (Pacific), Trustwave



istockphoto.com/LeoWolfer

As government organisations continue to digitise, the need to safeguard their systems against increasingly sophisticated and ever-present cyber threats is more pressing than ever. The public sector collects and holds a significant amount of personal data, making it an irresistible target for malicious cyber actors. An attack against the industry could potentially

affect thousands of organisations and hundreds of thousands of public sector employees and citizens. Since some government organisations are considered critical infrastructure (CI) operators, they face new requirements for protecting their systems and data.

The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (SLACIP Act) introduced new regulations for entities and organisations operating in the CI

sector, including some government organisations. The new requirements include mandatory reporting obligations for serious cybersecurity incidents under strict timeframes, placing the onus on businesses and operators to raise the alarm should they fall victim to a cyber incident. And for organisations operating in New South Wales specifically, the Privacy and Personal Information Protection Amendment Bill 2022 calls for public sector agencies,

state-owned corporations, local councils and some universities to report breaches “likely to result in serious harm” to both affected individuals and the Privacy Commissioner.

Cyberthreats are getting more sophisticated as cybercriminals continuously expand their capabilities, while organisations’ cybersecurity measures remain one step behind. To combat more frequent, targeted and complex attacks, organisations are turning to managed detection and response (MDR) to improve their security posture and become more cyber resilient.

For the government sector, this type of protection has become necessary for effective detection and response to help safeguard CI. The more highly sensitive information government agencies house, the more likely they will be targeted not only by ordinary cybercriminals but also malicious nation-state actors with a ‘licence to hack’. A major data breach would be detrimental from both a financial and reputation standpoint and emphasises the importance for government to take data security seriously.

It’s no longer enough for government organisations to be cyber ready. They must take proactive measures to enhance resilience by being hyper-aware, vigilant and capable of keeping their organisation safe, which is why MDR is becoming an essential service. As the threat landscape rapidly evolves and requires constant monitoring, the Australian Government is increasing fines for serious breaches amid a spate of high-profile cyber incidents that compromised customer data.

However, establishing and maintaining 24/7 monitoring, response and threat-hunting capabilities is a relatively expensive activity, particularly for state and local governments that are typically less funded than federal government institutions. Moreover, the complexities of deploying and properly

configuring specialist technologies, such as extended detection and response (XDR) and security information and event management (SIEM) platforms, across multiple sources including networks, clouds and endpoints, can take months to implement.

Partnering with an experienced MDR provider can ensure that government organisations maintain their security posture instead of going it alone with their in-house cybersecurity team. MDR services augment in-house government security teams by providing 24/7 monitoring, enhanced intelligence, access to experienced analysts and proactive threat hunting and vulnerability assessments.

Before partnering with an MDR provider, it’s important to understand the value that MDR services can deliver to ensure they align with the business. Government organisations should consider:

- 1. Technology:** As government organisations continue to digitise their services, there is a corresponding increase in risks and vulnerabilities. Choose an MDR that has deep experience with XDR and SIEM technologies for comprehensive threat detection and response capabilities.
- 2. Detection:** All MDR providers detect threats; however, it’s important to look at how they detect them. Is it human-led, hypothesis-driven or is it done through automated searching? A quality MDR partner should combine human and technological knowledge to execute threat hunting with 24/7 monitoring and real-time analysis and investigations.
- 3. Response:** Government organisations should partner with an MDR provider that is proactive and focuses on responding to threats by containing them and keeping them from spreading further. The MDR services should be able to remotely act on endpoints, within the network


or other applications, to isolate systems and stop threats before they cause damage.

- 4. Research capabilities:** Threat intelligence helps government organisations better understand their attackers, respond faster to incidents and proactively map out the attackers’ next move. Look for an MDR provider with an active research arm that can incorporate other cyber threat intelligence to benefit from the latest information on emerging threats worldwide.

- 5. Field-testing experience:** Ensure an MDR partner has field-tested experience with incident response. Hurried responses can result in negative consequences, like unnecessarily shutting down systems or business processes and causing financial and operational disruptions.

- 6. Culture:** It’s important to determine whether an MDR provider can offer a long-term partnership that aligns with the department’s objectives, needs and culture. Government organisations should consider their potential provider’s operating model, industry reputation and how they will integrate with the in-house security team before engaging with an MDR partner.

Many IT and security teams face a ‘do more with less’ challenge as a result of smaller budgets and scarce resources, and largely rely on third parties and contractors to carry out their core functions and responsibilities. As cyber threats increase, government organisations should use MDR to protect their CI assets. Failing to do so can leave the public sector, as well as the Australian people’s security and privacy, exposed to malicious threat actors. Working with a trusted and experienced MDR provider can help government organisations establish a mature cybersecurity posture and better protect their CI assets from unauthorised access.

The background image shows a person's hands typing on a laptop keyboard. A semi-transparent blue overlay covers the upper half of the image. Within this overlay, there are several glowing blue icons: a heart, a person with a plus sign, a laptop with a bar chart, a DNA helix, a clipboard with a checklist, and a large icon of a doctor with a stethoscope and a plus sign.

TECHNOLOGY TRANSFORMS PATIENT OUTCOMES

Microsoft

Gippsland Health Alliance (GHA) comprises 11 hospitals and six bush nursing centres across 50 sites in the Gippsland region of Victoria, which covers 41,500 square kilometres and is home to around 300,000 people. GHA was established in 1998 as part of the Victorian Government's Rural Health Alliance strategy.

The organisation's main objective is to enhance patient care and better use resources by providing timely information to health professionals and administrators, wherever they are located. Central to achieving this objective is its electronic medical record (EMR) system, which houses digital versions of key patient information.

GHA wanted to improve the accessibility of its existing EMR system for clinicians so they could make more informed decisions. It also wanted to reduce the system's risk of being affected by cyber attacks, increase its resilience and achieve significant cost benefits.

Following a rigorous tender process, in 2017 GHA chose Microsoft partner Altera Digital Health to deploy its Sunrise EMR clinical suite, a cloud-based solution built in Microsoft Azure.

Adrian Shearer, Chief Technology Officer and Interim Chief Information Officer at GHA, said the option of a fully managed service was one of the key reasons why the alliance selected Altera Digital Health and its Sunrise solution on Azure.

"We were looking for an organisation that could deliver all of the infrastructure, design and security as part of the solution," he said.

HEALTHY GROWTH

Thanks to the flexibility of the cloud-based EMR system, GHA has been able to scale up the solution as needed.

The solution was originally deployed to accommodate approximately 300 registered users, but the alliance has since expanded its accessibility to around 800 users. GHA can also respond quickly and efficiently to the need for external clinicians and physicians by adding them as temporary users.

"The incremental uplift as we go has been seamless," Shearer said.

"So from 300 concurrent users to 800, there's been no impact on my team operationally to deliver that. They've just turned up the heat and expanded."

The first site in the alliance to deploy the Altera Digital Health Sunrise EMR clinical suite was Latrobe Regional Hospital (LRH), a purpose-built teaching hospital with more than 2100 staff members who provide care to a population of more than 260,000 people.

The EMR solution was implemented in LRH's 30-bed emergency department in April 2019. Today, it is being used by all of the hospital's inpatient services and community mental health services across the Gippsland region.

GHA has implemented Altera Digital Health's Sunrise Emergency Care solution, which is part of its EMR platform, at the emergency departments of Central Gippsland Health Service, Bairnsdale Regional Health Service, West Gippsland Healthcare Group and Bass Coast Health. The EMR platform is expected to be rolled out across the inpatient services at all four hospitals by November 2022.

Shearer said the EMR solution has improved GHA's ability to recruit health information managers.

"We no longer require people with that skillset to come and live here and look at paper records," he said.

ENHANCING PATIENT VISIBILITY

GHA's cloud-based EMR system provides users with a complete view of all patient episodes across the

Gippsland region from wherever they are located. This has significantly improved clinical outcomes in a number of ways, according to Shearer.

"We've reduced our workload of having to recall and move records around the hospitals," he said.

"We've seen around 50% less medication errors, and [the EMR system] has also fostered antimicrobial stewardship by helping us more accurately diagnose pathology orders in terms of what's being ordered by whom and when. We can then focus on educating clinicians about the types of orders that are being placed and if they're appropriate. Not over-ordering antibiotics is very important in hospital environments."

Shearer said the EMR solution also enables GHA to audit its operational processes more accurately and identify any missing information in patient episodes. This has the added benefit of helping educate doctors and nurses in how to document these episodes.

For Simone Redpath, General Manager of Critical Services at LHR, the EMR system helps her determine whether patient transfers are required.

"I have been able to look at information on the EMR while on the phone with my colleagues at other local hospitals to discuss whether a patient required a transfer or could be cared for closer to home," she said.

"Without the quality of information shared via the EMR, the patient may have been transferred away from their family, friends and community unnecessarily."

Rebecca Wittmer, Critical Care Nurse Unit Manager at LHR, said the EMR solution assists her team in working out which patient referrals to prioritise.

"For example, we received a referral of a patient with high-level needs from our very busy Emergency Department to the Critical Care Unit (CCU), which had limited bed capacity," she said.



“Our CCU team was able to review the patient’s notes on the EMR and, with the help of our intensivist, begin planning for treatment while we progressed efforts to secure them a bed. As a result, the patient was prioritised for admission.

Without immediate access to this information on the EMR, our team would not have been able to fully review the complexities of the case and treatment may have been delayed.

KEEPING COSTS DOWN

As well as enjoying improved clinical outcomes and scalability, GHA has been able to avoid purchase, installation and maintenance costs associated with traditional IT infrastructure.

“One of the current challenges for us due to the COVID-19 pandemic is there would be a significant risk right now with the provisioning of physical hardware,” Shearer said.

“That’s not a concern for us with the

Azure environment and our hosting with Altera Digital Health as part of this project. If we were doing this by ourselves, we would have had an impact on resources trying to put this equipment in.”

And, if any of the hardware used to help power GHA’s system needs upgrading, there is no additional cost to make it cloud-compatible.

SAFE AND SECURE

By moving its EMR system to the cloud and hosting it on a secure network, GHA has been able to take advantage of several security and business continuity benefits.

These include Azure’s built-in firewalls, which are designed to reduce downtime for the EMR system and prevent extensive damage to it by detecting potential threats.

System performance is constantly monitored using another built-in service, which generates alerts that the support team at Altera Digital Health and Microsoft Azure can respond to.

In the event of its primary EMR system going offline, GHA can have a backup system ready to go in a matter of hours. And, by using backup and disaster recovery sites located in Australia rather than overseas, the alliance can also achieve data sovereignty.

By having the EMR system hosted on a secure network, it can prevent extensive damage to it by detecting potential threats.

The resilience of GHA’s cloud-based EMR platform was put to the test in 2019 when it was subjected to a sophisticated cyber attack that prevented access to a number of critical systems, including its financial management system.

Although the alliance was forced to quarantine some of its systems following the attack, there was no evidence of unauthorised access to patient data.

“While we had to disable connectivity to our EMR due to security reasons, it was ready the day we said we were ready to come back online,” Shearer said.

“And that was purely based on the fact that it was hosted in Azure and protected by the Azure infrastructure.

“As soon as we were given the green light, the servers to the EMR were turned back on, and it was genuinely the first application that was ready for us to start.”

GHA has also boosted its risk resilience by rolling out a scanning and document management capability, embedded within the Sunrise EMR system. This enables hospitals to digitise old and new paper records from other connected health sites and ancillary services.

According to Shearer, Sunrise Document Manager addresses the inevitable need for the ongoing management of paper records in an EMR system.

“It achieves this in a risk-resilient, seamless and sustainable way,” he said.

5G IoT CONNECTIONS TO GROW 1100% IN THREE YEARS

istockphoto.com/metamorworks

A combination of sharp growth in the healthcare sector and provision of smart city services is predicted to create a 1100% increase in 5G IoT connections by 2026, according to a new study from Juniper Research. This will see global connections shoot from just 17 million to 116 million in only three years.

The comprehensive research examined 5G adoption across key sectors — including the automotive industry, mobile broadband and smart homes— and forecasts that the healthcare and smart cities market will account for over 60% of 5G IoT devices by 2026. The ultra-low latency and high bandwidth of 5G IoT technology will be the key factors

in driving this proliferation of new connections.

SMART CITIES OFFER THE SINGLE BIGGEST OPPORTUNITY FOR 5G IoT

The report anticipates that 5G networks will experience significant growth in smart city services; owing to 5G's cost-effectiveness in deployment and ability to carry significant amounts of data.

By 2026, there will be over 60 million 5G smart city connections globally, and the report urges city-planning authorities to leverage 5G connectivity as high-bandwidth gateways. It found that the monitoring of transportation networks, including road and rail networks, will be key services that require 5G-enabled high-bandwidth cellular connectivity.

DIGITAL TRANSFORMATION IN HEALTHCARE DRIVES 5G ADOPTION

Investment from healthcare providers into 5G-based services will be driven by the need to modernise services, as the global COVID-19 pandemic exposed inefficiencies in healthcare provision. The report identified services including telemedicine, connected ambulances and emergency services, and real-time remote monitoring as key services that will be immediately improved by the integration of 5G services.

Research co-author Olivia Williams commented: "5G will enable more efficient and dynamic healthcare provision that was not feasible with 4G or Wi-Fi. However, healthcare providers must first implement 5G in areas which provide a strong return on investment; most notably connected emergency services."

CYBER ATTACKS ON HEALTH CARE ARE HERE TO STAY

Serkan Cetin, APJ Technical Director, One Identity



istock.com/fpopba

Data breaches have notably been an ongoing and increasing threat in Australia across all enterprises and organisations.

With the recent waves of cyber attacks compromising the data of millions of Australians, it has never been more important to have measures in place to protect sensitive data.

To bring greater awareness to cybersecurity issues, The Office of the Australian Information Commissioner (OAIC) started the Notifiable Data

Breaches (NDB), a scheme where all organisations under the *Privacy Act 1988* are required to disclose all data breaches involving personal information.

NDB STATISTICS

The most common source of data breaches varied for the top industry sectors, while, historically, the most attacked industries have reported that most data breaches are caused by compromised credentials, followed by malicious or criminal attacks.

Since the very start of the NDB in 2018, it has been interesting to see

that healthcare service providers have been reporting the most data breaches compared to all other industries, followed by finance.

Out of 464 notifications received in the last NDB report (July–December 2021), the healthcare sector reported 83 attacks (18%), with an equal number of breaches from malicious or criminal attack and human error (47% each).

As a comparison to the second latest NDB report (January–June 2021), the scheme reported on 446 overall, while the healthcare sector had informed of 85 breaches.

It has never been more important to have measures in place to protect sensitive data.

WHY ARE MALICIOUS ATTACKS INCREASING IN HEALTH CARE?

Just in the last five years, the state of Victoria reported two major cyber attacks, affecting several hospitals.

The recent Medibank attack allowed criminals to obtain access to the details of approximately nine million customers, including personal information and health claim-related data. Medibank is not the only healthcare organisation to have fallen victim to cybercrime. Australia Clinical Labs was also hit with a cyber attack earlier this year in which data of approximately 233,000 people was accessed. In an incident which occurred in 2021, elective surgeries at some Melbourne hospitals had to be postponed as a precautionary measure. During the same time, the Australian Cyber Security Centre issued a warning regarding the significant increase of cyber attacks in the healthcare industry, recommending a variety of strategies to combat the issue.

Experts have since wondered why these attacks got so predominant, and the answer is quite simple.

Patients need to share sensitive information with their hospitals, doctors and other healthcare providers to receive care. This information includes full names, identification details, medical histories, credit card details, public and private insurance details, and more. Because of this, experts have found that medical data can be between 10 and 20 times more profitable than credit card or banking details alone, resulting in a major impact for not only health facilities but also their patients. Attackers can sell this data on the dark web for profit, or to facilitate identity theft, blackmail or extortion.

Another potentially contributing factor as to why malicious attacks have increased is due to the rapid digitalisation of processes across multiple business units, which accelerated during the pandemic.

The pandemic was a challenging period for healthcare organisations and specifically hospitals and their staff as most facilities were unprepared for COVID-19 spikes. The priority and focus for health care and management had to be reallocated to patient care. Unfortunately, attackers see this as an opportunity to strike, thus making healthcare organisations more vulnerable to cyber attacks.

However, there is light at the end of the tunnel as there are solutions that can be implemented to protect the healthcare sector.

HOW TO PREPARE FOR AND PREVENT THESE INCIDENTS?

With the constant rise of data breaches, as well as their severity and consequences for not only big companies but also their consumers and customers, organisations are highly encouraged to take measures to ensure their data, applications and people are kept secure.

This particularly applies to healthcare providers, as the data breaches become a constant threat to the sector. With that in mind, here are just some of the actions that can be taken for effective preparation and prevention for these attacks:

- Investment in education on basic cybersecurity best practices and defences against phishing and social engineering attacks.
- Multifactor authentication for all users accessing from any location to any application.

- Implement password management best practices.
- Patching and keeping systems up to date.
- Review processes and technology to ensure they are still fit for purpose.
- Secure access to sensitive information and systems.
- Implement robust auditing and logging across systems.

CHANGES IN LEGISLATION

In light of the recent breaches in Australia which have impacted millions of Australians, one area which we predict will change and evolve is legislation and regulatory requirements.

The Australian Parliament passed the *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* earlier this year with mandatory periods for cybersecurity incidents to be reported by organisations categorised as critical infrastructure and a new obligation for responsible entities to create and maintain a critical infrastructure risk management program.

In addition, and as a consequence of the recent breaches, new legislation is being introduced to increase the penalties for repeated or serious privacy breaches. Under this new legislation, organisations could be fined \$50 million, or 3x times the value of any benefit of misuse of information, or 30% of annual turnover.

Cyber attacks and threats to health care, and to all industries, have evolved to new levels which pose significant consequences to people and organisations. Unfortunately for many organisations, the attackers have been successful in their mission in compromising their defences and obtaining access to their data. Cybersecurity needs to be a top priority at the board and management levels to enable organisations and their cybersecurity teams to implement the strategies and technologies to mitigate the risks of cyber attacks.



Digital innovation

HOW WESTERN HEALTH TACKLED DIGITAL INNOVATION AT SPEED

30 | GOVTECH REVIEW Q1 2023

WWW.GOVTECHREVIEW.COM.AU



istock.com/metanetworks

WESTERN HEALTH (WH) MANAGES FOUR ACUTE PUBLIC HOSPITALS AND A HOST OF OTHER HEALTH FACILITIES IN VICTORIA. IT PROVIDES A COMPREHENSIVE INTEGRATED RANGE OF CLINICAL SERVICES, RANGING FROM ACUTE TERTIARY SERVICES IN AREAS OF EMERGENCY MEDICINE, INTENSIVE CARE, MEDICAL AND SURGICAL SERVICES, THROUGH TO SUBACUTE CARE AND ONSITE AND VIRTUAL AMBULATORY CLINICS.

When the organisation's digital transformation plans escalated thanks to the pandemic, WH needed to pivot quickly to ensure remote availability of its systems. This included its Active Directory, which manages identity authentication and authorisation of all network and IT resources users.

When WH requested assistance in moving from an Active Directory it shared with two other major hospitals to one of its own, it was already one of the fastest growing healthcare providers in Australia, having onboarded 3000 new staff over a 12-month period. The organisation was about to embark on a significant amalgamation project and the old Active Directory was a major impediment to a smooth transition.

With the onset the pandemic — and, in particular, its impact on the state of Victoria — WH became an epicentre of action and priorities naturally shifted. Within a 48-hour period, the healthcare provider shifted some of its working model to remote and redirected resources to establish a vaccination hub, which saw 1.4 million doses provided to the community. At one point, WH also took over management of nursing homes in its district, something it hadn't done before.

Faced with such rapid change, WH relied on Logicalis Australia to complete the now highly complex Active Directory rebuild project and navigate additional new and unforeseen challenges that the pandemic presented. The focus was to

avoid unnecessary changes for staff, who were navigating the provision of quality health care to patients in a new remote-based setting.

Cameron McBride, Director of Digital Technology Services at Western Health, said the perfect storm of events was putting real pressure on the staff.

"With everything going on, we also experienced supply chain issues due to the semiconductor crisis, and were feeling the impacts of the significant pressure placed on our staff," he said.

"Logicalis was able to alleviate the pressure due to their strong healthcare expertise and understanding what is required to run a 24-hour emergency service. They were also able to architect the work around our amalgamation. The team at Logicalis was accommodating, and never took a rigid view when a challenge was presented."

Sam Psathas, Health Care Sector Lead at Logicalis Australia, said the Active Directory rebuild has delivered more than modernisation.

"One of the most exciting results of the Active Directory rebuild is that it is an enabler for modernising the business further, particularly around the digital workplace," Psathas said.

"Importantly, Western Health has a significantly improved security posture, and its identity system for onboarding and offboarding staff can now be practically instantaneous. It is an infinitely better end-user experience with a single sign-on and one identity for all internal systems — instead of having to remember around 15 separate user IDs and passwords previously."

MITIGATING ATTACKS ON CRITICAL INFRASTRUCTURE

Rob Le Busque, Regional Vice President, Asia Pacific, Verizon Business Group

Australians have recently experienced the devastating impact of cyber attacks on critical infrastructure. The data hacks of telecommunications giant Optus and private health insurer Medibank have thrust the cybersecurity practices of critical infrastructure operators, government organisations and agencies into the spotlight.

Tech professionals in government play a vital role in shoring up the cybersecurity of Australia's most important pieces of critical infrastructure. In addition, they also shoulder the burden of constantly staying ahead of malicious online actors to adapt to an ever-changing threat landscape.

According to the Australian Signals Directorate, Director-General Rachel Noble, a quarter of cyber attacks identified in 2021 were against critical infrastructure. In nearly 60% of the ransomware incidents in the same year, the victim company agreed to pay the ransom to avoid further disruptions to their business.

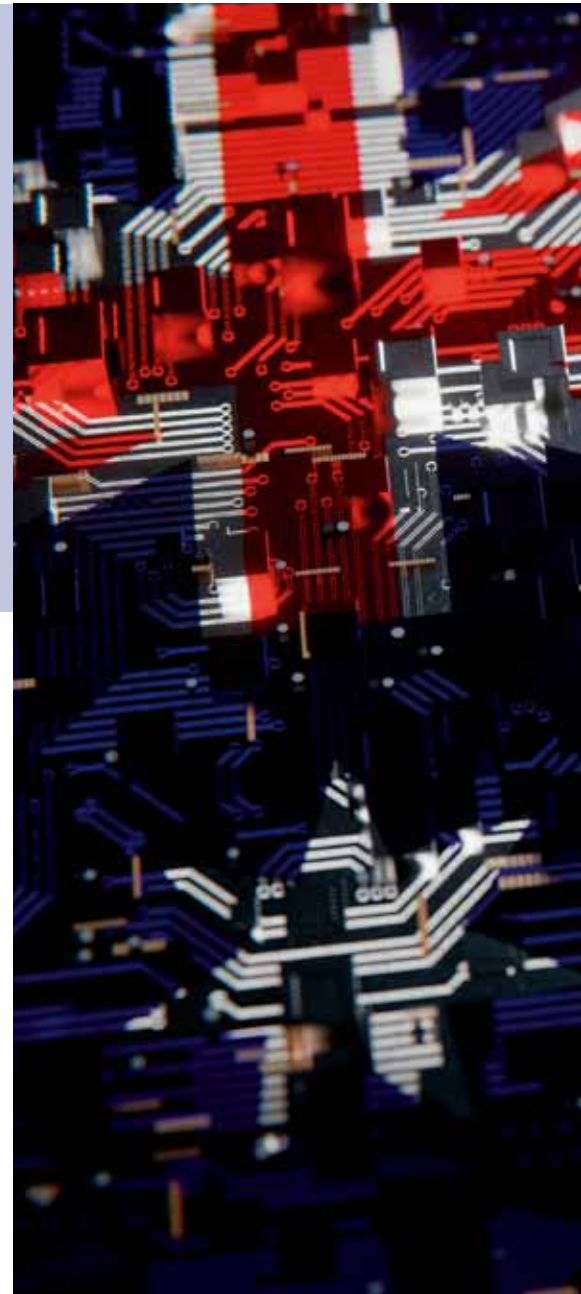
The 2022 Verizon 'Data Breach Investigations Report' (DBIR), which studied 23,896 security incidents,

of which 5212 were confirmed data breaches, found that ransomware from organised crime groups targeting critical infrastructure increased by 13% in 2021 — more than the previous five years combined.

THE LEGISLATIVE LANDSCAPE HAS EXPANDED

Following the introduction of legislation earlier this year, the stakes have never been higher for critical infrastructure operators and tech experts in the public service, and the risks have never been greater.

The federal government recently made significant reforms to Australia's critical infrastructure policies in terms of cybersecurity, which expanded the definition of critical infrastructure to include 11 industry sectors. These reforms expanded the obligations and application of critical infrastructure laws and made incident reporting mandatory within 12 hours of an incident. Furthermore, this legislation now covers organisations within electricity, communications, data storage or processing, financial services, water, healthcare, medical, higher education, research, food and grocery, transport, space technology, and defence industries.



This has led to more focus on strengthening cyber protections within the public sector and expanded the government's role in protecting critical infrastructure.

FOCUSING ON THE BASICS

There are many things that government tech experts can do to improve



The stakes have never been higher for critical infrastructure operators and tech experts in the public service

cybersecurity within government agencies and departments, and the broader critical infrastructure network of the country.

Getting support from C-suite executives has typically been one of the central challenges, but things are starting to change for the better. Awareness is growing among company executives —

the recent high-profile incidents have illustrated why cybersecurity needs to be at the forefront of all elements of a business's operations.

But funding for these practices is still a major issue, and more budget is always needed.

This is where tech experts need to be looking to partnerships to help to

combat a lack of adequate funding and resourcing. The Australian Cyber Security Centre (ACSC) has a partnership program, cybersecurity assessments, certification frameworks and specific programs like the Cyber Security Business Connect and Protect Programme.

State governments have also become increasingly active in this

space, with Victoria making its water utilities subject to the Victorian Protective Data Security Framework. New South Wales has made its own utilities subject to the ICT Purchasing Framework and Cyber Security Policy.

For most tech experts within government, managed service partnerships are an effective and efficient way to combat the issue of a lack of funding. These providers have the scale to deal with attacks that most critical infrastructure organisations probably cannot. They can also provide around-the-clock support.

The public sector should participate in more of these partnerships and encourage critical infrastructure operators to adopt the same approach.

LESSONS LEARNED FROM ENTERPRISE

This year's DBIR has identified that the supply chain is the most likely place threat actors will start an attack. The report found that the supply chain was responsible for 62% of system intrusion incidents this year and was responsible for 9% of the total incidents in the report.

Protecting supply chains has also been identified as a key aspect of developing cyber resilience by the federal government in its critical infrastructure reforms, being included as one of the four key 'hazard domains' in the risk management program that is now mandatory for critical infrastructure companies to comply with.

Take Japanese multinational Astellas Pharma. With 14,000 employees around the world, Astellas is a major global pharmaceutical player — a highly regulated industry. The company has worked with Verizon to deploy a next-generation secure network infrastructure that allows Astellas to securely manage its tens of thousands of devices and endpoints across its 70+ locations.



istock.com/anyberfut

Fujifilm, a company traditionally viewed as a photographic and film equipment business, has now expanded into health care, materials, business innovation and imaging. The company has deployed Verizon Business Group's Advanced Security Operations Centre in Canberra, to strengthen its global cybersecurity monitoring and cyber intelligence capabilities.

These are examples of partnerships that can help a company strengthen its cyber protections without 'breaking the budget', and ways that companies in the supply chain for larger critical infrastructure firms can shore up their defences in an efficient and effective manner.

REMAINING CYBER VIGILANT DURING A CYBER SKILLS SHORTAGE

These partnerships are also an effective tool to assist in combating the growing cyber skills gap.

According to a 2020 report by the Cybersecurity Workforce, companies need about three million qualified cybersecurity workers, a huge gap

between the current availability. Nearly 65% of those surveyed for the report said their organisations have been impacted by this skills gap.

Partnering with third parties who specialise in providing security services can help to reduce the huge impact the skills gap is having, and can also provide 24/7/365 coverage, something which is needed to combat the cyberthreat.

Government organisations and critical infrastructure operators need to continually reassess their defences and realign their spending with their needs. Too many organisations still have legacy security measures in place that will have little impact in the event of a sophisticated cyber attack, and these systems need to be regularly reassessed for efficacy and efficiency.

With the recent government reforms, complying with the various new regulations can be onerous and costly for organisations. But this must be viewed as a positive way to incorporate cybersecurity across all company objectives and into the roles of all employees.

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

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.



DESIGNERS & MANUFACTURERS
OF 19" RACK SYSTEMS



PROUDLY
MANUFACTURING
IN AUSTRALIA



AUSTRALIAN MADE
MAKES AUSTRALIA



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