govtech review

PUTTING THE I.T.
INTO SPORTS INTEGRITY

NEW ZEALAND COMMITS
TO ALGORITHM CHARTER

PROTECTING PRIVACY
IN SMART CITIES

TARGET AUSTRALIA
WHY GOVERNMENT IS LOSING THE WAR ON CYBERCRIME

Q3 2020
PP100021607

sas

ETHICS AND AI
WHAT IS ALL THE FUSS ABOUT?

Visit **sas.com/ai-ethics** to learn more

Q3 2020

INSIDE

FEATURES

Insider

Is Australia losing the cybersecurity war?

There have been a number of major IT developments over recent months, such as the release of the federal government's long-awaited 2020 version of its Cyber Security Strategy, which has been welcomed by all involved in the cybersecurity sector.

Others include state and federal IT ministers agreeing to the development of a National Digital Identity Roadmap as part of efforts to align digital identity systems Australia-wide, and the publication by the ACSC and DTA of new cloud security guidance for agencies. These are all positive steps to improving the nation's cyber systems.

Yet as EY's Richard Bergman points out in this issue, "The number of cyber attacks has continued to increase across the Australian public and private sector. We must ask ourselves: why are we losing the war against cybercrime?"

Why indeed. Bergman outlines four priorities that governments should adopt to protect essential government services and the public's security, such as implementing the Essential Eight and increasing investment in cybersecurity defences. None of them are anything particularly new; they just need to done, done promptly and done properly. It shouldn't really be too hard.

As Monash University academic Lennon Chang points out in this issue, one thing that might help the overall cybersecurity ecosystem is a better incident reporting scheme. He cites the arrangement used by the very safety-conscious aviation sector as an example of what can be achieved — incidents occur, they're investigated, recommendations are made and the whole sector learns from the mistakes or oversights. It seems like a very sound idea, and one that the government should take onboard.

Cybersecurity will be a key topic at the annual Technology in Government conference, coming up in November. Always a must-attend event, this year you won't have to the leave the comfort of your home office in order to catch up on all the presentations, since — like many conferences in 2020 — those presentations will all be conducted online. Technology in Government brings together leading public sector IT practitioners from across Australia and around the world to share insights and developments that are of concern to all who work in this field. See facebook.com/TechInGovAU/ for full details.

If leadership is your role or goal, you should also take a look at the online leadership courses WF Media (publisher of this magazine) is presenting over the next few months. Presented by Trevor Manning, a highly experienced tech engineer-turned-executive, the courses will show you how to positively influence your team(s) to set them on the path to success, while learning how to handle those tricky conversations and relationships that always crop up. See comms-connect.com.au for more information.

Jonathan Nally, Editor
editor@govtechreview.com.au

wfmedia
connecting industry

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

EDITOR
Jonathan Nally
jnally@wfmedia.com.au

PUBLISHING DIRECTOR/MD
Geoff Hird

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Colleen Sam, Veronica King

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

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

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

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

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

FREE CYBER SECURITY ASSESSMENT

IS YOUR DATA SECURE AT HOME AND THE OFFICE?

Did you know that working from home can have an impact on the security of your corporate network? 95% of all security incidents originate from an end user device. Securing these devices will improve an organisation's overall security posture.

Acer is excited to team up with technology and security specialists Acurus to provide a free assessment of your organisation's Acer notebook and Desktop fleet. The free assessment will review any quick wins to improve your overall 'work from home' security, giving peace of mind.

How does it work?

Purchase a corporate Acer fleet and we will provide a free SOE security assessment, which will include:

- Review Operating System for vulnerabilities
- Review of applications installed for vulnerabilities
- A review of the current Endpoint Protection utilised and its effectiveness
- Industry recognised best practice security audit for Windows 10 (this is required to be performed on a domain joined PC)

What will I receive?

Acer and Acurus will provide a report of the findings that include:

- Detailed report and security profile score, with remediation suggestions.
- Post remediation report, detailing the fixes and any outstanding remediations proposed.

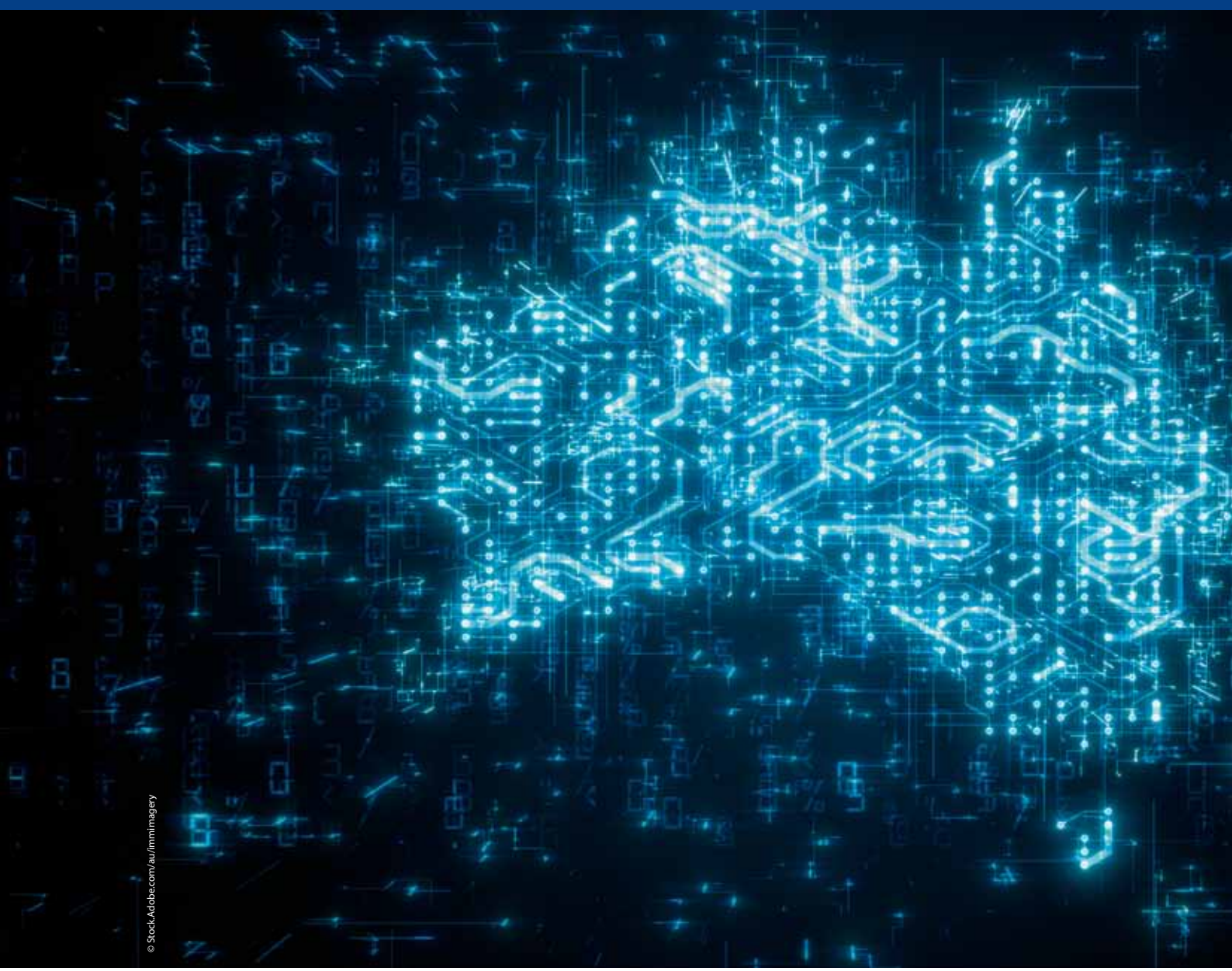
CONTACT US:

sales.aca@acer.com

ACURUS

GOVERNMENT IS LOSING THE WAR AGAINST CYBERCRIME

Richard Bergman



WE NEED MORE LEADERSHIP AND WHOLE-OF-GOVERNMENT ACTION TO LIFT AUSTRALIA'S CYBERSECURITY MATURITY AND MAKE US A HARDER TARGET.

Four years ago, the federal government launched Australia's Cyber Security Strategy, which was widely seen as a welcome improvement on both the prioritisation and amount of investment in Australia's cybersecurity capabilities and overall maturity. However, over those past four years, the number of cyber attacks has continued to increase across the Australian public and private sector. We must ask ourselves: why are we losing the war against cybercrime?

In 2019, the Australian Cyber Security Centre (ACSC) responded to 427 cyber incidents affecting Commonwealth entities. According to the ACSC, these cyber attacks were aiming to steal information that included defence capabilities, research and intellectual property, and the personal information of Australian citizens and government staff.

In June this year, Prime Minister Scott Morrison highlighted the threat to our national security and economic prosperity when he announced that Australia has been subject to continued targeting and attack from a nation-state threat actor. This was not a surprise to those in industry, who have seen the increasing levels of cyber attacks against all levels of government and other sectors.

The frequency and severity of cyber attacks against the Australian public sector will continue to increase as geopolitical, economic, defence and trade tensions remain. The nature of government services require the collection of valuable information and data from citizens, which is why it is targeted by both nation-states and organised cybercriminals.

It is difficult to stop nation-state cyber attackers since they are determined and well resourced. However, we need to be doing much more to make Australia a harder target. The level of cybersecurity maturity across all levels of government in Australia is inadequate. The underinvestment in the modernisation of government technology compounds the risks presented by difficult-to-maintain legacy systems, and increases the likelihood of agencies being successfully hacked. A significant cyber attack against the government will result in interruption to essential government services and the loss of public trust.

The Australian Government has world-class cybersecurity capabilities at its disposal within the Australian Signals Directorate (ASD) and the ACSC. However, outside of these dedicated national capabilities there are huge inconsistencies in the focus or capability to protect Australian citizens' identities and data. There is opportunity for further leadership on cybersecurity across the public sector to support the capabilities of the ACSC and ASD, and to make each agency and department a much harder target.

CYBERSECURITY MATURITY

Tabled in 2020, the Commonwealth Cyber Security Posture in 2019 Report showed clearly that federal agencies had ineffective risk management practices and remain vulnerable to cyber threats. One of the biggest shortcomings across all levels of government in Australia is the failure to implement the ACSC's Essential Eight… a prioritised list of mitigation strategies that will protect systems against a range of cyber adversaries.

The Top Four mitigation strategies of the Essential Eight are mandatory for federal agencies. A maturity level of 'three' — the highest level — across the whole Essential Eight is the recommended security baseline for all organisations. This is achieved when an agency is fully aligned with the intent of the mitigation strategy. In 2019–20, findings from an Australian National Audit Office analysis of 18 government entities showed that maturity levels for most entities were significantly below the Policy 10 requirements of the Protective

Security Policy Framework, 'Safeguarding information from cyber threats'.

To help address the lack of cybersecurity maturity, the ACSC has been working hard with additional activities through the Cyber Uplift program. Yet, while some improvements have been made, they are not enough to adequately protect government services and citizen data and identities.

If you examine the tactics and tradecraft used by cyber attackers, you quickly gain an appreciation for why the Essential Eight needs to be fully implemented to a maturity level of three across all federal and state agencies. ASD and the ACSC do exactly this, and in 'The Summary of Tradecraft Trends for 2019-20: Tactics, Techniques and Procedures Used to Target Australian Networks,' the ACSC states that "A review of investigations performed by the ACSC has shown that implementation of ASD's Essential Eight on victim networks would substantially reduce the risk of compromise by the adversary TTPs identified in this advisory".

This is not a new statement — the ACSC's analysis of the majority of cyber attacks that Australia encounters results in the same recommended mitigations year on year.

THE WEAKEST LINKS

Balancing the right level of investment in cybersecurity and ensuring public value against the risks of cybercrime can be challenging. The federal, state and local public sectors are not spending enough to keep pace with emerging threats, and they are not spending enough on protecting essential services and citizen security. At this stage we are struggling to play catch-up, let alone get ahead.

The ability to prevent a nation state cyber attack would require too much investment for each individual agency, which is why there needs to be reliance on central government capabilities within ASD and the ACSC. However, agencies also need to prioritise what they can control and make sure they are delivering on the cybersecurity baseline recommended by these central capabilities. Otherwise they will be the weakest link in our national security.

The level of cybersecurity maturity across all levels of government in Australia is inadequate.

IN-BUILT SECURITY

One of the challenges facing our public sector leaders is trying to balance the transformation of government services and at the same time protect citizen security. There is an opportunity for leaders to leverage the transformation and digitisation of services to drive an uplift in cybersecurity capability. Unfortunately, the 2020 EY Global Information Security Survey reveals that only 36% of digital transformation programs include security from the beginning.

Globally we have seen the main driver for increasing cybersecurity spend is risk reduction to address emerging threats. Federal, state and local agencies need significant increases in their cybersecurity budget to improve cyber risk management practices and become the backbone to combat cyber threats. It is time we saw a significant amount of increase in spend across the public sector, or else we may see more Australian citizens' data and identities stolen.

A NEW STRATEGY

The NSW Government's Cyber Strategy to be released later this year will bring significant investment into Australia's cybersecurity capability. And the recommendations outlined by the Industry Advisory Panel Report into Australia's 2020 Cyber Security Strategy will go a long way to protecting our nation's economy and national security.

Irrespective of the big-ticket items that are announced and funded, there is an immediate need for all levels of government to take further responsibility for protecting essential government services and citizen security.

Here are the top four things every government agency should do:

1. Fully implement the recommended ACSC Essential Eight to substantially reduce the risk of compromise by an adversary's tactics, techniques and procedures.
2. Integrate cybersecurity capabilities into digital transformation projects as a secure-by-design principle right from the beginning.
3. Increase the level of investment in cybersecurity to keep pace with emerging threats and on protecting essential services and citizen security.
4. Agencies at all government levels should demonstrate further leadership and accountability for what they can control, and ensure they are delivering on the cybersecurity baseline recommended by ASD and the ACSC.

We must see more leadership and whole-of-government action on implementing the Essential Eight, to lift Australia's cybersecurity maturity and make us a harder target for nation-state-sponsored cyber attackers.

Richard Bergman is EY's Oceania Cybersecurity, Privacy and Trusted Technology Leader.

Defence to bolster cyber training capabilities

The federal government has provided more details of its planned $1.4 billion investment in improving Defence's cyber capabilities over the next 20 years.

The commitment will include an initial investment of $575 million to support the development of a comprehensive training program to support the growth of the ADF cyber workforce, including virtual cyber training environments and tools.

The funding will also go towards constructing a purpose-built Joint Information Warfare Facility in the ACT which will offer critical Defence cyber training and simulation systems.

This facility will form part of a staged investment in efforts to develop the training, tools and infrastructure required to ensure the effectiveness of the ADF's defensive cyber operations capability.

The lab will be structured in a way that it can provide direct opportunities for small and medium-sized businesses to collaborate with Defence on innovative training and cyber tool solutions.

Minister for Defence Linda Reynolds said the Joint Project 9131 Defensive Cyberspace Operations project is designed to bolster Defence's ability to respond to cyber threats to their networks and systems that have the potential to undermine their ability to operate.

"This project ensures Defence can actively defend its deployed networks and combat platforms against the rapidly evolving cyber threats. This investment builds on the government commitment that was made in the 2016 Defence White Paper to strengthen Defence's cyber capability," she said.

DTA to hold Digital Summit in November

The Digital Transformation Agency will hold this year's Digital Summit and Australian Government Digital Awards virtually in November.

The event will be held across four days from 10–19 November, with award announcements each day.

The agency has now put out a call for speakers, case studies, exhibitors and sponsors for the event, based on this year's four themes.

Day one of the event on 10 November will focus on disruption and change. The second day on 12 November will have the theme of human-centred government services. Day three on 17 November will be based on leadership and people, and the final day on 19 November will have the theme of technology and data.

This year's program will also have events based on the current state of digital government services, the impact of recent crises and events including COVID-19 and an exhibition showcasing digital transformation successes from industry and government.

It will also feature interactive virtual workshops and case study sessions and virtual networking opportunities.

Minister for Government Services and the National Disability Insurance Scheme Stuart Robert will deliver the opening keynote for the summit.

According to DTA CEO Randall Brugeaud, the event will bring together digital leaders and practitioners, giving them an opportunity to see the innovative work taking place across government and industry in the digital space.

"[This] has been a challenging year, but it has driven many of us to think and work differently. As with many industries and programs, COVID-19 has led to an acceleration of our digital transformation journey," he said.

"The Digital Summit 2020 will bring together government and industry to share insights and experiences while engaging with new and existing networks."

Web resource launched to teach public sector digital skills

The Public Interest Technology University Network, a partnership of colleges and universities, has funded the launch of a free online resource to support the spread of digital skills in government.

The Teaching Public Digital web resource has been put together by a group of volunteer public service digital experts and institutions.

The website provides free, open access teaching materials on digital era skills for lecturers, teachers and public service leaders.

It includes a list of eight core competencies that digital era public service leaders should have.

These include the ability to anticipate and mitigate the privacy, security and ethical risks that are inherent to governing in a digital era, as well as the ability to use a range of techniques and tools to make government more open, collaborative and accountable.

Other core competencies include collaborating with specialists to understand and develop solutions tailored for the needs and experience of service users, as well as the ability to lead multidisciplinary teams and create a working environment that can continuously learn and improve outcomes.

One of the initiative's co-founders, UK-based mySociety co-founder Tom Steinberg, said the team is also developing a support network for educators to improve their own teaching skills.

This will be backed by a masters-level course which will be released as an open educational resource.

"Universities and in-house teaching academies are the institutions that define the skills of future public service leaders. We want to help these institutions to teach 21st-century skills to help solve 21st-century problems, Steinberg said.

Other core members of the initiative include Canada School of Public Service Director General Chris Allison, Carleton University Associate Professor Dr Amanda Clarke, Harvard University Lecturer of Public Policy David Eaves and Cambridge Digital Slate Policy & Research Leader Dr Tanya Filer.

The Public Interest Technology University Network was convened by New America, the Ford Foundation and the Hewlett Foundation.

Many agencies yet to fully implement DMARC

In the wake of the ACCC warning that cybercriminals are targeting victims with fraudulent COVID-19 support packages by spoofing government websites and communications, Proofpoint has warned that many agencies are yet to implement controls that can help prevent these attacks.

Research from the cybersecurity company found that only two of 18 agencies evaluated — the Department of Finance and the Department of Environment and Energy — are proactively blocking domain spoofing emails from their domains.

While 14 of 18 departments have published a Domain-based Message Authentication, Reporting & Conformance (DMARC) record, only the two departments mentioned have fully implemented the protocols. The remaining deployments are in monitor or quarantine mode.

Proofpoint Australia Country Manager Crispin Kerr said the findings of the DMARC analysis are cause for concern.

"Our research shows that email remains the weapon of choice for cybercriminals, and to prevent cybercriminals from using an organisation's likeness, there are open standards available, such as DMARC, to protect legitimate domains and effectively nullify an entire class of email fraud — domain spoofing," he said.

"DMARC remains the only technological defence that can eliminate domain spoofing. Those organisations that have the strictest level of DMARC implemented will achieve higher success rates in blocking malicious threats and stopping fraudsters from impersonating their brands, potentially saving the everyday Australian thousands of dollars in the process."

HOLDS UP EQUIPMENT NOT PROJECTS

S280 Industrial is an IP66 rated 19" cabinet suitable for harsh and unforgiving environments. - Air Conditioning available.

MFB®

DESIGNERS & MANUFACTURERS OF 19" RACK SYSTEMS

The last thing on your mind is the first thing on ours.

Whether it's ready-made, pre-configured or custom racking solutions, MFB's short turnaround capabilities speed your product from the warehouse to where they should be – fast. Our unwavering commitment to timely delivery ensures your projects run on time, every time, reducing deadline pressures while maximising results. With a solid history of over 50 years supplying innovative, off-the-shelf and custom built racking systems, you can rely on MFB for consistent delivery, on time, every time.

50 YEARS

PROUDLY MANUFACTURING IN AUSTRALIA

AUSTRALIAN MADE **MAKES AUSTRALIA**

ISO 9001 Quality Management

ISO 14001 Environmental Management

19" Rack Cabinets Licence No. 84944

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

WA Govt commits $8m for Electronic Medical Record System

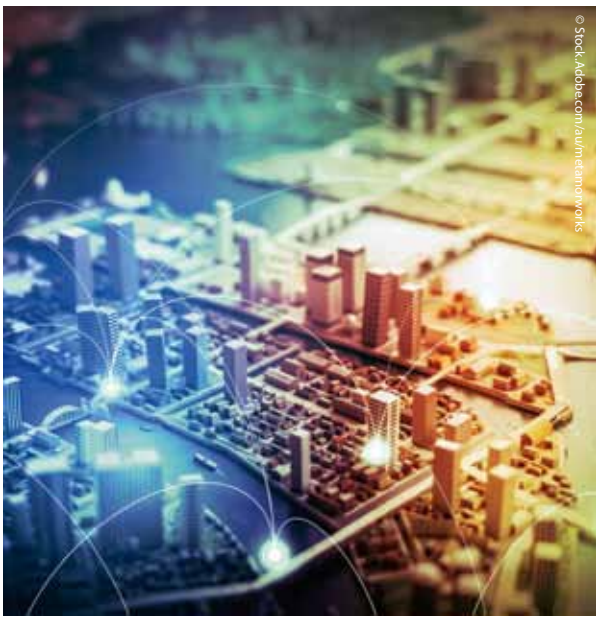
The McGowan government is injecting $8.1 million to commence planning for a Western Australian Electronic Medical Record System, as recommended by the Sustainable Health Review, to improve safety, efficiency and patient experience. The Electronic Medical Record System creates a linked digital environment capable of providing rapid access to information, to support patients through their health journey in the WA health system.

"The development of an Electronic Medical Record System will enable information to be available across the full continuum of care — not only promoting safety and quality but also saving lives," said Health Minister Roger Cook.

Once developed, the system will enable clinicians to view information such as patient notes, assessments, medical histories and diagnostic test results, in one place, helping them make safe and informed decisions. With the system, patients will not need to wait for medical records to be transferred between clinicians, with records held electronically on the system.

This investment will help provide a modern, resource-efficient, digital platform that prioritises safety and improves patient outcomes. The Electronic Medical Record System will also create a foundation for future digital growth and clinical innovation within the Western Australian health system.

"It is wonderful to see the advancements being made in health as we progress on our digital journey, and planning for an Electronic Medical Record System is a key component of this," Cook said.



NSW Govt unveils strategy for smart places and infrastructure

The NSW Government will incorporate smart technology into infrastructure and buildings as part of the Smart Places Strategy and Smart Infrastructure Policy, which will see sensors and technology built into cities. The move is predicted to create jobs, reduce traffic and commute times, reduce crime and boost the economy.

Smart traffic signalling, real-time route planning and sensors on parking spots are expected to reduce commute times by up to 20%, while smart meters and real-time alerts will allow residents to reduce water waste and use by up to 30%. Advanced digital models are also predicted to reduce construction costs and improve planning, while real-time air quality sensors will provide localised information to health providers.

Minister for Customer Service Victor Dominello said the strategies will also boost the COVID-19 recovery, as similar strategies have proved effective in Dublin, Barcelona and Boston.

"Whether it's easing cost of living pressure for households, busting congestion or improving health outcomes for communities, technology is the new weapon in our arsenal. Data and precision modelling is just as important as bricks and mortar. Information is power and technology should be embedded in every major infrastructure project," said Dominello.

The strategies build on the government's commitment to making NSW a digital capital, the launch of the Spatial Digital Twin, and a $240 million investment in cybersecurity.

ABB Wireless

Broadband wireless mesh technology

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

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

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

WirelessTech

ABB

LEARNING FROM USERS THROUGH DISCOVERY RESEARCH

The DTA Observatory team

THROUGH IN-DEPTH RESEARCH INTO HOW PUBLIC SERVICE ANALYSTS GATHER AND USE DATA, THE DTA HAS LEARNED HOW TO BETTER SUPPORT THEM IN THEIR WORK.

The Digital Transformation Agency's (DTA) Observatory team uses data science to learn how people interact with government and to manage several whole-of-government data services.

Part of the team's mission is to empower data practitioners to improve government services. We wanted to move past assumptions and make our own data-informed decisions about where we could provide more value for users. So we asked the users what they need.

We began this mission by providing Google Analytics 360 subscriptions, training sessions and analytics.service.gov.au; however, we wanted to better understand the realities of what being an Australian Public Service analyst is like. We wanted to understand how our users' worlds work, what their professional pain points are, and whether there are opportunities to enhance their practice so they can deliver more value to their organisations.

Research started with analysts who subscribe to the Observatory and use our services daily. We spoke with 18 users across 13 agencies during our first phase of discovery interviews. They told us about their experiences interacting with our service and using analytics in their organisations.

DEVELOPING OUR LINE OF ENQUIRY AND CONDUCTING INTERVIEWS

Our main aim is to empower data analysts across government, so we designed our line of inquiry to match. We explored:

- how our users engage with analytics in their day-to-day work
- what kinds of questions our users are trying to answer through analytics
- what barriers and opportunities our users see in reaching their desired goals.

We designed our interviews to be semi-structured — we followed a line of inquiry but allowed participants to guide the conversation with the stories they wanted to share. This approach allowed us to organically explore our research objectives without leading conversations too strongly. This helped uncover new and unexpected insights.

SYNTHESISING AND ANALYSING OUR FINDINGS

Two members of the Observatory team attended each interview with the analyst. We then synthesised what we heard using a collaborative online whiteboard. We captured key observations, quotes and ideas. The board became the space where we could group and theme similar ideas that came out of all the interviews.

In user research we say, "It only takes one person to notice the missing step on the staircase". Even if only one subscriber gave an insight, we treated it as having analytical importance to make sure we heard our users.

Once we had themed our interview findings, we analysed themes together to see what they told us about the user experience. This is how we uncovered insights.

In our Discovery Insights Report we capture the high-level findings — users' experiences with analytics and engaging with the current gov.au Observatory service.

WHAT WE LEARNED

We learned that we have primary and secondary users. We assumed the research cohort was obvious, since our assumption was that data analysts are our

primary users. From our conversations we also learned there are relevant stakeholders on the fringe of data analysis — those whom analysts report to, or those needing data to explore or validate assumptions and hypotheses.

Through our research with primary users, we learned that these secondary users are also important to the Observatory's mission as they represent the end users of analytics work. In future, we aim to further research the stakeholder experience to improve the focus of our work.

TYPES OF BARRIERS OUR USERS FACE

Barriers for users include:

- culture
- technology
- visibility
- capability
- resources
- security
- relationships
- perception
- data literacy
- user perspective

These barriers occur at different rates and in different forms across agencies and represent a challenge to our mission. By exploring them, we will better understand how to navigate the challenges faced by our users as they try to improve agencies' services.

PAIN POINTS AND OPPORTUNITIES

It can be difficult for our users to establish an 'analytics service' within their organisation. This is due to the ad hoc nature of how they receive and answer requests. A lack of awareness among stakeholders about the power of data leads to infrequent and less-strategic use of data.

We also found that users would like to have a greater sense of purpose behind the use of Google Analytics and know how to define and measure success. Some also face barriers to adopting user-centred design principles, which affects their ability to work with Google Analytics.

RESPONDING TO USER NEEDS

Three ways the Observatory can respond to user needs include:

- analytics leadership through best practice guidelines, standards and advice
- the creation of practical tools and templates to support users which are aligned to best practice
- facilitation of sharing and learning relationships across government.

A deeper exploration of these insights can be found in our Discovery Insights Report.

MOVING FORWARD

We are beginning to refine, design and test possible solutions. We are adopting a dual-track, agile approach to working. This means we will use a parallel discovery process to explore hypotheses and test prototypes. This will also improve our ability to deliver viable solutions.

If you would like to help with future research, we'd love to hear from you! Contact the Observatory team at observatory@dta.gov.au.

Do you want to help your agency enhance its data practice? Sign up for updates from gov.au Observatory to learn about our work, get access to insights we uncover, and hear early announcements about the launch of new tools and initiatives.

NEW CLOUD SECURITY GUIDANCE ISSUED

Dylan Bushell-Embling

AGENCIES WILL NOW NEED TO PERFORM THEIR OWN ASSESSMENTS DUE TO THE END OF THE CCSL PROGRAM.

The Australian Cyber Security Centre and the Digital Transformation Agency have collaborated on the development of new cloud security guidance for agencies to use while assessing and choosing cloud solutions.

The new guidance, designed in consultation with industry partners, has been designed to help walk government agencies, cloud service providers and Information Security Registered Assessors Program (IRAP) assessors through the process of assessing the integrity of cloud services.

The guidance includes a cloud security assessment report template that will seek to improve the consistency of the reports, a new Cloud Security Controls Matrix designed to augment the government's Information Security Manual security controls for cloud computing and guidance outlining the anatomy of cloud assessment and authorisation.

Published in time for the wind-up on Monday of the former Certified Cloud Services List (CCSL) list, the guidance is designed to facilitate the transition to a new assessment framework that will give government agencies greater choice over their selection of cloud services.

Meanwhile, smaller cloud service and related providers will be able to deliver their services to Australian government, according to Minister for Defence Linda Reynolds.

"The cessation of the [CSSL] will open up the Australian cloud market, allowing more homegrown Australian providers to operate and deliver their services," she said.

Minister for Government Services Stuart Robert added that the new guidance will "help and guide organisations to assess the suitability of a range of secure and cost-effective cloud service providers to securely handle their data and ultimately boost Australia's cybersecurity resilience".

But industry experts such as Vault Cloud CEO Rupert Taylor-Price have questioned the wisdom of putting the burden of risk management assessments on individual government entities.

"The bar for achieving ASD certification was extremely high and provided certainty into data protection. By decentralising compliance requirements we are concerned that government agencies may experience inconsistent standards, not only impacting the service the government receives, but also their ability to interoperate with other agencies and in turn the outcomes for citizens," he said.

"Although there may be initial cost savings for the ASD there may be overall cost, delays and security implications in the future. However, if Australia continues to experience a threat landscape at the level the Prime Minister outlined recently, the continued investment in a certification program is in our national interest."

Taylor-Price said recent announcements from across government have shown that there is still a need for government entities to access standardisation certificates.

For example, Robert has recently announced that the government will examine local sovereignty requirements on certain datasets to be hosted on-shore in an accredited Australian data centre, and only be accessible by government and local service providers across Australian networks.

"[Without standardisation certificates] it will be difficult for a cloud provider to achieve the same level of trust or security. The key for us is to come together as a security ecosystem to improve the security, compliance and risk posture of all agencies," Taylor-Price said.

Secure networking infrastructure & monitoring solutions.

For efficient remote management of cities and transport networks.

Intelligent Transport.
- Traffic radar
- Temporary signaling

Asset/Process Monitoring.
- IP video systems
- Thermal imaging cameras
- Incident detection

Secure Industrial Networks.
- Networking infrastructure
- Cybersecurity solutions
- Edge-to-cloud connectivity solutions

MOBOTIX · Portable Traffic Light · MOXA · RAJANT · CYBERTEC · inhand · smartmicro

A Madison Company

madison Technologies

Connect with confidence.

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

Sales Enquiries 1800 72 79 79 **www.**madison.tech

well connected

David Abouhaidar, CEO Secure Agility

Secure services in GovDC for NSW Government departments

Secure Agility has partnered with Cisco, Rubrik and Pure Storage to offer OurDC^4, a modern data centre-as-a-service residing within GovDC.

Australian MSP, Secure Agility, has developed a secure, enterprise and government-grade cloud platform with partners Cisco, Rubrik and Pure Storage. OurDC^4 is a collaboration between four partners that delivers a modern data centre-as-a-service for customers across three, Tier 3 data centres. It is ideal for government agencies and enterprises who need application and infrastructure hosting in government-grade data centres. This includes residing within NSW GovDC, meaning it is approved for use by NSW Government departments.

According to CEO, David Abouhaidar, this environment enables Secure Agility "to offer the absolute best of breed technology when government and enterprise clients require cloud-based infrastructure and multi-cloud services. We built three identical environments to ensure we could provide efficiency and simplicity".

The partners were chosen for their capabilities and complementary services. "For example, the Cisco and Pure Storage FlashStack converged infrastructure enables customers to seamlessly expand beyond their on-premise compute and storage resources into a highly available and high-performance hybrid cloud platform. This is perfect for traditional or modern workloads — such as Kubernetes clusters. Complementing the FlashStack compute and storage architecture, Rubrik (built on Cisco) underpins the recovery capabilities in the environment, and can deliver near-zero recovery times and accelerate application development."

Products available on OurDC^4 include:

- **IaaS^4:** Cloud hosted on-shore with native security and data protection.
- **DaaS^4:** A hosted desktop to reduce management costs and improve access.
- **DPaaS^4:** A data protection service to keep business running in the event of a problem.
- **SDwan^4:** SD-WAN with the choice of Viptela or Meraki solutions.

OurDC^4 in detail

A complete and secure DC-as-a-Service that delivers a secure, high availability, predictable cost platform for IT service delivery and digital transformation.

OurDC^4 is hosted in the Equinix SY6 and SY7 data centres — both of which are GovDC rated — complemented by a third Equinix data centre for enterprise use. As part of its commitment to secure and robust processes, Secure Agility holds ISO 27001 and ISO 22031 accreditation.

OurDC^4 storage and backup platforms provide standard encryption-at-rest. The architecture is designed and implemented with data security as a top priority. Similarly, OurDC4 capabilities extend from securing customer data to providing backup, recovery, archive and replication.

Secure Agility provides a managed service offering, which enables it to complement and enhance existing IT teams. Benefits include:

- Pay-as-you-go pricing and no penalty for expansion and contraction of services.
- Next-generation security that keeps applications online with high availability for individual VMs and a fault-tolerant architecture.
- Cloud edge and burst enabling workloads on demand.
- Geographic separation and redundancy across three data centres, each with identical configurations.
- Advanced security with software-defined infrastructure that does micro-segmentation, a next-generation approach to security deployed at the VM/application level, and infrastructure that enables only approved access to applications.

With the evolution of workplaces into a more distributed architecture — and with organisations supporting work from home, BYOD and multiple SaaS vendors — Secure Agility will be extending the capabilities and product range of OurDC^4 to assist customers with securing and protecting their users and data, as well as enhancing collaboration between remote staff.

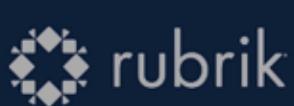
For more information visit ourdc4.com.au

SECURE AGILITY

www.secureagility.com

GovDC to the power of 4

Your move to the cloud that is cost predictable and Australian-secure.



ourdc4.com.au

OurDC 4

PUTTING THE I.T. INTO SPORTS INTEGRITY

Jonathan Nally

A NEW BODY, SPORT INTEGRITY AUSTRALIA, HAS BEEN GIVEN RESPONSIBILITY FOR MANAGING COMPLEX ISSUES INVOLVING LOTS OF SENSITIVE DATA.

In 2018, the findings of the Review of Australia's Sports Integrity Arrangements — known as the Wood Review — were presented to the federal government, with one of the prime recommendations being to merge the functions of several bodies which had had separate responsibilities for aspects of sports integrity issues.

The first stage of that merger has seen the Commonwealth sports integrity functions of the Australian Sports Anti-Doping Authority, the National Integrity of Sport Unit from the Department of Health and the safeguarding functions of Sport Australia all combined into a new body, Sport Integrity Australia.

The second stage will see other functions fulfilled, including an Australian Wagering Scheme and more outreach and education.

Sport Integrity Australia has a very important role to play in the administration of integrity measures across Australian sports, which of course

brings with it heavy responsibilities when it comes to the collection, use and storage of sensitive personal data of thousands of athletes and others.

The agency currently has 292 FTE staff, including Canberra-based personnel and a large network of casual and full-time staff spread around Australia.

To find out what it was like having to merge the ICT operations of several separate bodies, we spoke with Andrew Collins, CIO of Sport Integrity Australia.

What was the timeline of the merger?

Following the government's endorsement of the Wood Review recommendations in 2019, the Department of Health, ASADA and Sport Australia established a machinery of government (MoG) change program and governance structure to facilitate the merger. This body was comprised of property, security, IT, finance, HR, branding, subject matter leads and so on, and oversaw the integration of staff and services for Sport Integrity Australia on the 1st of July 2020.

Were the three bodies' systems very disparate?

Yes, as the security requirements and core functions of the parent agencies are all quite different and hence their ICT and security postures were tuned to each of their businesses.

How big a job has it been?

In mid-2018 ASADA commenced a major technology uplift program to realise the CEO's vision of an engaged and data-informed organisation. Realising this vision required digitisation of almost all ASADA processes and toolsets and saw a migration of internal systems to the Azure Protected cloud and an organisation-wide uplift in capability through the use of cloud services such as Office 365 and Dynamics 365.

As a part of the MoG process we looked at the potential ICT platforms for the new agency, and the ICT leads for Health, ASADA and Sport Australia supported using the ASADA ICT environment as the basis for Sport Integrity.

Because of this, the final merging of staff was quite simple and involved adding new staff and moving TRIM data records from Health. I wish all MoGs were so straightforward!

Is BYOD and working from home a challenge?

The protection of athlete health information is of critical importance and as a result we do not allow BYOD access to our systems or data. This approach allows us to enforce strong, risk-based authentication and access controls on all our data and systems.

Working from home and our business continuity process (BCP) response is a great testament of the value of the mobilisation of staff and the cloud-based Office365/D365 platforms we have established. On the day we enacted the BCP, we moved to 100% work from home with no real impact of our functions. We are still operating very effectively with around 80% of our staff working from home. And the value of the investments in ICT and security we have made continue to pay off.

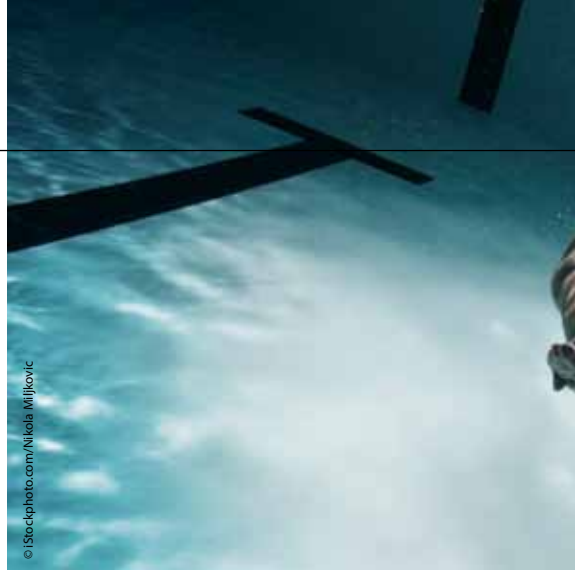
There are certainly challenges with working from home, and long-term WH&S of staff is a prime concern. But collaboration tools like Teams and Stream have significantly reduced the impact COVID would have had on operations. In some ways it has made our teams stronger, with the collaboration platforms also being used for team bonding. For example, we recently held a trivia competition with Drug Free Sport New Zealand and I have picked up a lot of gardening advice from our deputy CEO!

Do AI and machine learning play a role in your operations?

We have the Microsoft Artificial Intelligence platform in our environment now and are starting to use the platforms for automation of common workflows; also key to this is the Power platform. These tools are aimed at moving ICT innovation and automation into the hands of business and power users rather than being exclusively an ICT tool.

Examples are a PowerApp we developed to attach to meetings allowing minutes, attendance, paper and decisions to be tracked and action items integrated into staff planners to allow tracing of the delivery of action items.

Another example that we are currently implementing is automation of the media analysis function. As you can imagine, sport and anti-doping are in the media regularly around the world. Traditionally this summary process was a manual task; we are building a solution using cognitive


© iStockphoto.com/Nikola Miljkovic

services to automate a large part of this. There is also some groundbreaking AI work led by the World Anti-Doping Authority (WADA) that is using AI to detect drug cheats based on variations in their athlete biological passports.

As exciting as these are, they are only just the beginning and I expect in two years' time the number of AIs will outnumber the staff, allowing those staff to focus on the difficult and challenging programs that require creativity and imagination... leaving the mundane process work to the AIs.

How much do you rely on external partners?

To completely transform and grow previous operations from a paper-based operating model to the modern, cloud-based, data-informed Sport Integrity Australia is a massive task. The ICT team is comprised of two permanent and three contract staff.

Our transformation was based on a preface of 'Lead at what is important, partner for everything else'. As such we have a strong partnering model which has allowed us to undertake such a large transformation; but it is a partnering model where the key ICT governance and operations remain with the agency.

Typically, this is referred to as the MSI (Master Service Integrator) role. In keeping this role in-house, we have been able to bring a range of vendors on board and deliver a series of complex, interrelated projects very quickly and cost-effectively. It is quite different to the operating model used in other government departments and has worked very well for us.

We have a set of very good, long-term partners who lead the delivery of various technologies under the operating model, namely:

- Forward IT (ASI) is responsible for mobile device management, O365 migration, Azure security, network and a host of smaller functions. I can't speak highly enough of their professionalism and willingness to go well beyond my expectations.
- We have taken a leadership position in terms of government adoption of Protected Cloud and O365 services, and the support we receive from Microsoft is exceptional.
- Dialog is managing the implementation of Dynamics365, which digitises our CRM and business processes, and they have delivered a world-class service.

We also have formal MoUs and working partnerships with a range of government agencies and commercial vendors, including:

- VA & Jade — Intelligence systems
- Service Australia — Gateway and border security services
- Health — Financial and HR shared services
- AIHW — Mentoring data custodian staff
- ACSC — IT security
- AGD — Physical security

And some global and national sports partnerships:

- We are working with the Institute of National Anti-Doping Organisations (iNADO)/WADA on establishing a global security and privacy compliance program for all anti-doping agencies.
- It took a bit of a break due to COVID, but we plan on re-establishing a National Sporting Organisation security and privacy program, similar to the iNADO program, to help uplift the security and privacy controls of sports nationally.
- We are actively engaging with every national sporting body in Australia on integrity education and compliance. Ultimately it is better to work together and prevent the problem in the first place.

We partner extensively for services for which we do not have the volume or staffing or support, or which are not critical to our core business. The services offered by Health, Service Australia, ACSC etc are exceptional and we are constantly looking at how we can improve the relationships and integrations further.

Do issues such as doping and match fixing present any special challenges?

Absolutely. There are two key challenges in this space:

- The security and privacy of the athlete health information we hold. This is an area we have invested heavily in and is something that is discussed each Monday morning with the CEO and senior executive; it is taken extremely seriously right across the organisation. We are now looking to work globally and nationally to lift the security and privacy capabilities in the smaller national sporting organisations and globally with anti-doping organisations globally via iNADO/WADA.
- The legal rigour around the testing process and any ensuing arbitration processes. We need to ensure all processes are consistent, timely and fair. Our largest ICT investment in the past two years has been in this area, aiming to digitise every aspect of the anti-doping process. Of the 5500 tests we do each year, any of them could wind up in the Court of Arbitration for Sport, so process, rigour and fairness are paramount.

Do your operations require any special IT structures or practices?

Our technology platforms are based on the tools that can be used across government, but have been configured to meet the business needs of Sport Integrity Australia. This ranges from the digitisation of the anti-doping program through to the use of virtual and augmented reality for athlete education.

The strength of the Office and Dynamics platforms is that we have zero customisation in our environment, making upgrades etc automatic; but the

environment has been configured to suit our business process.

Keep an eye out for our education presenters, most of whom are current professional athletes, all equipped with iPads and web-based education tools like our VR and AR applications!

Is data sovereignty a big issue?

We do have mandatory reporting requirements with WADA for some athlete information as part of our obligations under the world anti-doping code. We work closely with WADA security staff to ensure their system security is at a level where we are confident in their capacity to protect the athlete information that we have been entrusted with.

A great global initiative is that WADA and iNADO (plus the 10 largest anti-doping organisations globally, including us) are working together to lift the anti-doping community's cyber resilience.

That said, all our data outside of the mandatory reporting to WADA is held in Australian-owned data centres, in Australia (Canberra Data Centres and Azure Central)... and anyone who has visited knows how good the security is in CDC!

What is your background in ICT and government?

I started my career in Defence intelligence before moving into the security sector with a company called SecureNet (now Verizon after many mergers), where I managed the security and compliance operations in the Asia–Pacific.

Since then I've held a range of CTO/CIO roles in the government and commercial sectors, the most notable being CTO for nine hospitals in the northern region of New Zealand and at Sport Integrity Australia. Although the scale is vastly different, the journey I took both organisations on to the cloud and modern technology is remarkably similar. It has been amazing to see the difference staff mobility and modern tools have made to the work practices in these organisations.

Where do you see ICT going next?

I started my career in ICT in the days of 286 computers and dial-up modems... so there has been a bit of change. The capacity for genuine transformation that is given by technologies such a cloud (SaaS), modern security practices, blockchain and artificial intelligence is greater than the realisation of computers in general.

I think over the next decade we will see a seismic change in the way government and business operate; some very visible, but a lot of the change will be using technology like blockchain to streamline and automate workflows and simplify the way we work and allow staff to focus on the important and complex work and not simple process management.

Another big area of change we are already seeing realised is around integration. A seemingly never-ending problems in business are siloes of workflow and information. There is a lot of great work occurring in Microsoft and others to both simplify the integration progress and empower staff to tune the IT environment to suit themselves through codeless application development and automated workflows.

One of the most exciting aspects to ICT service delivery I see occurring is a shift from traditional ICT maintenance to being business-focused and working in partnership with business stakeholders to configure the environment. At Sport Integrity Australia we have business staff now doing their own dashboard reporting, integrated application development and have just starting looking at artificial intelligence to automate routine tasks... all without any technical IT skills. Exciting times!

What can we expect to learn at the Tech in Gov conference?

We present regularly at Technology in Government. Last year we talked about organisational courage to make change and overcoming some the common inhibitors to large-scale organisation improvement.

This year we have two presentations scheduled:

- Using Artificial Intelligence to Transform Business. The benefits that blockchain and AI offer are well known; what is harder is realising the value. This talk will be on challenging traditional thinking to transform work.
- David v Goliath, a story of government collaboration to defeat a state-sponsored cyber campaign (presented between Sport Integrity Australia and Service Australia). We have been the subject of state-level cyber attacks since November 2019, and the response between SA, ACSC and Sport Integrity Australia is a great example of how the use of strategic partners (but retaining the MSI role) can result in a cost-effective capability that far exceeds the cost of delivery.

Any final points?

The journey ASADA/Sport Integrity Australia has been on for the past two years has effectively been a comprehensive transformation of business capabilities; but this is not the end. We have built a capability that allows the business to challenge and optimise itself, and for IT to respond rapidly to changes as required. It has been a tough journey but one that any organisation can take, and it has been successful because of our partnerships across the commercial and government sectors.

This year's Technology in Government conference will be a virtual event, held over two days on 3 and 4 November. You can find full details at https://www.terrapinn.com/conference/technology-in-government/index.stm.

Five critical ICT priorities for the public sector

A smart nation connected with digital tools and data analytics will pave the way for widespread digital transformation.

Australia has taken a significant step toward modernising the digital infrastructure of all government and public sector agencies by launching the Digital Transformation strategy and establishing the Digital Transformation Agency (DTA) with a mandate to "improve people's experience of government services".

But what should the public sector focus on as it becomes digitally ready heading towards 2025? The following five priorities are those that our research has identified as being the most critical.

The smart platform

According to the latest Global Interconnection Index (GXI), an industry study published by Equinix that tracks, measures and forecasts the global growth in interconnection bandwidth between businesses and organisations, public sector digital transformation is rapidly accelerating private interconnection.

Interconnection bandwidth reflects the total capacity provisioned to privately and directly exchange traffic, with a diverse set of counterparties and providers, at distributed IT exchange points inside carrier-neutral colocation data centres. To capitalise on these trends, Australians need a fast, reliable, scalable and secure interconnection platform that enables private and direct data exchange.

The government must create a robust, private and secure platform that segments and controls data traffic to address scenarios requiring the highest levels of cybersecurity. A highly secure platform includes protecting blockchain networks, securing data repositories for data privacy, protection and compliance, and preventing data breaches initiated by bad actors.

Modern infrastructure

Government agencies need a new architecture that offers direct interconnection to clouds, partners and ecosystems, with closer proximity to consumers and other agencies. The resulting seamless and integrated experience will enable a digital supply chain of rich ecosystems of agencies, industry, clouds, networks and partners.

To that end, by deploying hybrid and multicloud infrastructures, the government can seamlessly integrate cloud with other infrastructure capabilities.

There are many benefits from integrating cloud. Firstly, the government can optimise cloud networks to control costs while monitoring bandwidth to increase capacity, reduce latency, and improve distribution, resilience and security. For example, the Driver and Vehicle Standards Agency, a UK government body, chose to move services to the cloud with an interconnection strategy powered by Equinix Cloud Exchange Fabric® (ECX Fabric®). By so doing, they cut latency by two-thirds and reduced the time to add new connections from months to hours.

The Australian government, too, is growing cloud partner ecosystems to enhance distributed cloud security. It should continue to build workforce skills to drive cloud adoption and implementation.

An interconnected digital government

Modernisation is shifting agencies from

traditional IT architectures to more distributed, interconnected IT platforms that can directly and securely connect all the locations, people, data and things needed for success. Creating a robust private interconnection foundation will prepare Australia to ride the next wave of digital innovation with confidence and greater agility and flexibility.

The DTA has defined three major strategic priorities that are needed to produce a government that is:

- Easy to deal with
- Informed by the citizen
- Fit for the digital age

These priorities call for securely collecting, storing and sharing data, including interconnection with various multicloud and edge strategies.

The Australian Government's Vision 2025 promise is the ability for citizens to "access all government services digitally," identifying 68 high-volume transaction services that each have more than 50,000 transactions per year. Through a digital identity service such as myGovID, Australians can easily prove their identities for a secure online access without having to log in to multiple sites.

This sort of transformation enables a real-time insights capability, as a government agency can collect data just once with a user's digital identity and share it with multiple other agencies when the occasion arises. With the right technology partners providing top-notch digital ecosystems and interconnection, the government can remove the inefficiencies of duplicate services and multiple layers of administration.

Investing in the edge

Investing in edge capabilities ensures that public data is collected close to the source (that is, end user) so that applications can access the data instantly. Managing data at the source is of increasing importance as companies start to develop 5G and IoT capabilities, and as the public will increasingly expect services to be delivered in real time.

Government applications are undergoing their next seismic shift as they move from being cloud-delivered from the centre to cloud-enabled at the edge. The GXI forecast and supporting deployment data reveal that workloads are indeed moving to the edge, where data is exchanged in proximity to people and partners.

Delivering experiences and exchanging data at the edge improves responsiveness and business processing capabilities. For example, 5G is expected to reduce the last-mile (endpoint) latency to 5 milliseconds, meaning that edge-delivered services will have a major advantage over regional core delivery.

Distributed IT services require a digital platform for superior performance, security and data exchange at the digital edge.

The GXI found that these distributed IT services correlate to an increased need for interconnection bandwidth to achieve a digital-ready state.

Upon the advent of 5G technology, 5G networks will accelerate critical agency efforts to collect and analyse data. Fast analysis of vital intelligence will be necessary to protect everything from ports of entry to government employees coming under continuous phishing attacks.

Smart cities

According to the UN, 55% of the world's population live in urban areas, and that is expected to increase to 68% by 2050. Supporting urban density will require the local interconnection and analytics of applications, data, content and networking through advances in 5G, IoT, robotics and hyperautomation.

At the core of any smart city is its information-driven, interconnected foundation. With the widespread adoption of smartphones and the internet, connectivity is available everywhere. Sensors and mobile technology will be embedded in IoT devices, and location technologies will enable administrators to predict failures and resolve issues. Advanced analytics will enable technology agencies to convert operational data into real intelligence, catering specifically to each citizen in a connectivity dependent marketplace.

In 2014, Yarra City Council in Victoria needed a digital transformation strategy to update its architecture to provide services in environmental initiatives, building and construction applications, employment services and local business schemes. The city migrated its backup disaster recovery to the cloud via Platform Equinix® and rolled out a number of cloud-based software applications to bring services to the edge and make community services more efficient.

What's next?

The public sector must build a highly interconnected digital ecosystem that connects governments to governments, governments to citizens and governments to enterprises, so that population centres, commerce, and digital and business ecosystems can meet and interact in real time. A smart nation connected with smart digital tools and data analytics will pave the way for widespread digital transformation and give citizens access to smart technology to improve their quality of life.

EQUINIX

Equinix Australia Pty Ltd
www.equinix.com

STRENGTHENING AUSTRALIA'S CYBERSECURITY ECOSYSTEM

Jonathan Nally

A BETTER INCIDENT REPORTING SCHEME WOULD BE ONE WAY OF REINFORCING AUSTRALIA'S CYBERSECURITY POSTURE.

As cyber attacks become more prevalent and ever more harmful, governments at all levels are taking action to beef up their capabilities — and those of the private sector — to tackle the threat. As part of its efforts to improve Australia's cybersecurity posture, the federal government recently released its 2020 Cyber Security Strategy Industry Advisory Panel report, which has received overall widespread support.

The report recommends more transparency about government investigative activity, more protection for critical infrastructure, better real-time blocking of attacks, and strengthened incident response and victim support programs.

But is this enough, or are there still gaps that need to be filled? How can and should the public and private sectors work together in the cause of cyber defence? And what actions need to be taken once a cyber attack occurs?

To find out more about what can be done, we spoke with cyber researcher Dr Lennon Chang from Monash University's School of Social Sciences.

Is the federal government doing enough to strengthen cybersecurity, both for itself and for the wider community?

Over the past few years, the Australian Government has put extensive resources into strengthening cybersecurity. We saw the launch of the Cyber Security Strategy in 2016 and the establishment of Australian Cyber Security Centre. These all show the government's determination to contribute to a secure cyber space in Australia.

And as cybersecurity and cybercrime are not limited by borders, the government launched its International Cyber Engagement Strategy to help developing countries, especially countries in our neighbourhood (the Indo–Pacific region), to strengthen their cyber capacity and cybersecurity.

These are all good approaches but they will never be enough, as new technologies keep providing new opportunities for cybercriminals to create new types of cyber threats.

How does Australia compare with other countries when it comes to national cybersecurity?

In my opinion, Australia is doing well. It is good to see the Prime Minister being willing to stand in front of the media and talk about cyber attacks on government agencies. It is a good change of attitude as it tells the public that agencies under attack are victims and shouldn't be blamed. This might encourage corporations and other victims to not hide the fact that they have had a cyber attack.

What should the government do to improve protection of critical infrastructure?

It is important for the government to have a good plan to not only protect critical infrastructure but also to build resilience. Based on my research, this includes a better incident reporting scheme that takes into consideration fears of reputational damage and further auditing requirements as well as providing incentives to encourage reporting.

Sharing knowledge and experience is essential to alert other companies and organisations of the risk and to encourage vigilance and cooperative responses. It is so important that I would argue that the government should consider a compulsory reporting system. Currently we have a voluntary reporting system and anyone can report an incident to ACSC, but they don't have to.

The ASD has the authority to take offensive action against foreign cyber attackers. Should Australia go harder on this?

First of all, not all cyber attacks come from state-backed entities. Some are lone wolf attacks and others are from criminals or groups supporting a particular cause. There is little, if any, risk in fighting back in these circumstances.

Taking offensive action against a state-backed foreign cyber attack might not be ideal if it results in an escalation, and possibly even a full-scale cyber war. It is important to know your enemy before taking offensive action, but often we may suspect who the enemy is but we don't know for sure. However, it is important that the Australian Government has the capacity to do this when needed. It might contribute to a cyber war, but just having the capacity for retaliatory action might also be a way to prevent a cyber war from happening. At the very least Australia needs to maintain an advanced capacity to defend itself from cyber attacks/cyber war and be prepared to use it.

You've said that Australia needs a better incident reporting mechanism. What would this look like?

The US has long had a Federal Information Management Act which guides computer incident reporting. Taiwan and China have similar schemes. Although we have Cyber Incident Management Arrangements guiding incident reporting, they are not comprehensive enough as recommended in the Industry Advisory Panel Report. It is important to include industry in the scheme, especially industries related to critical infrastructure.

Also, while designing the scheme, it is important to embed 'safe harbour clauses' and ways to promote reporting. As mentioned in my research, the current reporting scheme used by the aviation industry to report near misses would be a good model to consider when we design an incident reporting scheme for cyber attacks.

Does the 2020 Cyber Security Strategy Industry Advisory Panel report go far enough?

The report has several important messages, such as the need for incident reporting and cybersecurity awareness. The current focus on cybersecurity has mainly been on technology, not on human factors. However, human error has been the main factor enabling cyber attacks and cybercrime. It is important to raise the general public's cybersecurity awareness — how to design an effective way to do that will be something that the government will need to consider.

Take the issue of virtual kidnapping of international students, for example. It is obvious that the message from the police about preventing virtual kidnapping has not gotten through to international students, with a spike in kidnappings after two to three years of warnings.

With regards to cyberskills, I would suggest that the government invest not only on the science side of cybersecurity but also include professionals from disciplines such as criminology, law, psychology and human behaviour in the Joint Cyber Security Centres to encourage the development of strategies and responses that are both feasible and effective.

Are current penalties sufficient incentive for making systems more secure, or do they need to be tougher?

An approach to combating cyber attacks that relies solely on punitive measures will not be successful. And it is important that the government not exaggerate the problem as this can lead to denial, apathy and fatalism. It is also important that messaging around cybersecurity be connected to values other than security alone — values such as the economic benefits of secure infrastructure and online payment systems, for example.

The most important point is that cybersecurity is everyone's responsibility — government, private sector, NGOs and individuals. Cybersecurity is not just a matter for the ASD and the police; it is also about human error and the need for changes to online behaviour.

The case for cloud networking in government

Julian Critchlow*

Analysts predict the growth in enterprise IT spend for cloud-based offerings will be faster than the growth in traditional, non-cloud spending through 2022 (*Gartner Market Insight: Cloud Shift 2018 to 2022*). This shift of enterprise IT spend, coupled with the speed of innovation of IT cloud services, has seen 50% of organisations pivot to cloud networking.

In the government sector, many Australian agencies are adopting cloud services to facilitate digital transformation; however, barriers to a cloud-first approach include perceived risks around security, integrity and availability of critical government systems across cloud deployments. And of key strategic importance to government agencies is the need to protect the information of citizens and the assurance that data stored in the cloud is secure, accurate and reliable.

As the industry shifts gears, Extreme Networks is innovating to become the first cloud-driven end-to-end enterprise networking vendor, and we've gone out of our way to make sure companies sleep better at night when trusting us to safeguard their data.

ExtremeCloud IQ is the industry's first 4th generation cloud network management platform that works across Extreme's entire wired and wireless portfolio. By leveraging artificial intelligence and machine learning capabilities, the ExtremeCloud IQ platform automates routine network administration and configuration functions such as alerts, diagnosis and rectifying of security issues to provide better insights, visibility, control and automation across the network.

To ensure the highest levels of information systems and data protection, management and compliance, Extreme Networks' ExtremeCloud IQ platform is ISO/IEC 27001 certified by the International Standards Organization (ISO). By end of 2020, ExtremeCloud IQ will be the only cloud management solution with all three major ISO certifications for cloud, giving agencies assurance that Extreme is protecting their data.

For government organisations looking to transform their current modes of operation, the implementation of an automated, cloud-managed infrastructure has significant benefits. The move away from traditional on-premise owned and operated infrastructure to "evergreen" type service offerings will provide huge upsides and workload shifts. IT departments no longer have to purchase, deploy and maintain computing hardware and software in-house, while cloud services are quick and easy to deploy, scale as needed without involvement from IT, and are automatically updated to the latest release level.

ExtremeCloud IQ enables such transformations by securely protecting critical data and improving service delivery for constituents through an increase in the agility, flexibility and speed of delivery of digital services to the public sector. Now more than ever is the time for government agencies to look to cloud networking to underpin their strategic shift around digital transformation.

**Julian Critchlow is the General Manager of Extreme Networks Australia and New Zealand.*

Extreme networks

ADVANCE WITH US

Extreme Networks Australia
www.extremenetworks.com

Extreme networks

Get Your Head in the Cloud

Evaluate ExtremeCloud IQ at no cost – it's unlike anything you've seen before

Manage your wired and wireless network in the cloud, unlock the potential of ML and AI

ExtremeCloud IQ is the industry's first 4th Generation end-to-end cloud management platform that leverages machine learning and artificial intelligence to provide insights, visibility, control, and automation across your entire network.

Simple, Efficient, Secure
Cloud-Driven Networking

EFFORTLESS NETWORKING

DEPLOYMENT FLEXIBILITY

ACTIONABLE INSIGHTS

Extreme Networks is:

- A Leader in the Latest Gartner Magic Quadrant for Wired & Wireless LAN Access Infrastructure
- Named Fastest growing vendor in the Latest Omdia Cloud Managed Networking Report

ExtremeCloud IQ - a subscription based service offering:

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

Contact Extreme Networks Australia today for a demonstration of Extreme IQ

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

COVID-19 INTENSIFIES THE NEED FOR RAPID ADOPTION OF DIGITAL HEALTH

Steven Issa*

AUSTRALIA'S DIGITAL HEALTH STRATEGY INVOLVES TURNING ASPIRATIONS INTO PRODUCTS THAT PROTECT INFORMATION, IMPROVE WORKFLOWS AND DELIVER IMPROVED OUTCOMES.

Internationally, COVID-19 has put health and wellness at the centre of government and community attention. In Australia, it has brought intense focus to the ability of our healthcare system to meet the challenge posed by this global pandemic.

It has also highlighted the incredibly important role of digital technologies and the health sector to plan and manage health services: protecting patients and clinicians by enabling the delivery of care in new ways.

Since Australia saw the initial spikes in COVID-19 cases and our first waves of lockdown restrictions, virtually every individual has been impacted in one way or another. For many of us this impact has been experiencing what a health ecosystem can provide using digital health technologies; for example, the ease with which we can access essential primary health services through the expansion of Medicare-subsidised telehealth services.

For software developers and IT professionals working in the health sector, medium- and long-term plans have had accelerated delivery timeframes; for example, the delivery of electronic prescriptions nationally. This initiative was pursued by the Australian Government under the National Health Plan for COVID-19 to enable Australians to receive their medications electronically while in self-isolation.

Australia's healthcare system is held in high regard internationally and we have a clear strategy for a national health system enabled by digital health technologies. From a technology perspective, this involves turning aspirations into products — products that meet our uncompromising requirements that protect people's personal health information, improve the workflows of healthcare providers and deliver improved health outcomes.

BETTER HEALTH FOR ALL AUSTRALIANS

If you are interested in technology, it is likely that you already appreciate the importance of a healthcare system where you can access your medical information online and your healthcare providers share information online rather than by fax or mail.

In addition to increasing awareness of how technology can support healthcare, COVID-19 has pushed us to accelerate industry innovation, as well as digital health literacy among the wider public and healthcare industry.

People were reportedly putting off usual health checks — or even urgently needed treatment — due to COVID-19 related fears. This prompted industry concerns of an 'infodemic' and was the basis of the 'Don't put your health on hold' awareness campaign.

To support awareness efforts, the Australian Digital Health Agency (the Agency) launched a digital health guide to help Australians find the latest health information and advice about navigating the healthcare system.

Two accelerated digital health features — telehealth and electronic prescriptions — were always planned to be part of our health system. COVID-19 gave telehealth a kickstart and prompted a quicker implementation of electronic prescriptions.

Also, along with supporting and expediting advances that already exist, further innovation is still vital. Continued innovation is a key pillar of the National Digital Health Strategy (the Strategy).

With the Strategy as the foundation and to support the national COVID-19 response, the Agency ran an Innovation Challenge to champion digital health innovation across Australia and to provide a healthier future for Australians

© StockAdobe.com/au/BillionPhotos.com

through connected health care. It invited participants to address one of three themes: digital clinical care, digital social care, and digital health population management and future preparedness.

Across the applications received and the challenge's five winners, we were impressed with the breadth of innovation focused on solving key healthcare challenges.

The idea behind this initiative came from consulting international partners — which leads to the next area of focus.

DEEPER INTERNATIONAL COOPERATION

A global pandemic has swiftly highlighted the value of international coordination and collaboration on key health challenges. Government responses around the world provided guidance and helped to inform our response here in Australia: preparedness and speed in Taiwan, public–private partnership in Iceland, and mass testing and contact-tracing technology in the Republic of Korea (South Korea).

The Agency has long-since prioritised international collaboration, as the inaugural Chair and Secretariat of the Global Digital Health Partnership (GDHP). Until the development of a vaccine and with mobility restrictions likely to continue, Australia will need to recommit to new and creative ways to engage with our global partners and learn from approaches unfolding in other countries. As a member of GDHP, Australia played a lead role in the development of a series of recently released white papers on digital health best practice.

Our National Digital Health Strategy offers a blueprint for Australia's digital health future. To realise its aspirations, though, we'll need to continue engaging with all Australians on the importance of digital health, proactively seeking out innovation and collaborating with other countries on what we've learned.

This isn't just necessary for improving Australians' health outcomes during the current pandemic, or even future public health crises. It's necessary for addressing the myriad other health problems and systemic issues that predated the pandemic — especially now that we've all felt the personal impact of these issues a little more widely and a little more acutely.

**Steven Issa is Chief Digital Officer at the Australian Digital Health Agency.*

Emerging cybersecurity threats affecting government

Glenn Maiden

The impact of COVID-19 saw a scramble to get departments and agencies up and running with a remote, distributed workforce. Secure, remote access became crucial and will remain equally important well into the future.

In this challenging environment, businesses, individuals, and Australia's government agencies have all been targeted by significant cyberattacks from nation states and cybercriminals alike. Attackers continue to become more sophisticated and personalised, contextualised attacks continue to rise.

COVID-19 provided an ideal attack theme, with the Australian Cyber Security Centre responding to dozens of incidents and shutting down more than 150 malicious COVID-19-themed websites targeting Australian interests. SMS-based phishing attacks contained malicious links disguised as government warnings about COVID-19.[1]

The Copy-Paste campaign has also targeted numerous Australian government organisations. This attack exploits vulnerabilities in Telerik UI software, which is widely used and often needs to be patched manually. Many organisations aren't even aware they're using Telerik, so it's important to check this and patch the software.

Ransomware attacks are also becoming more targeted, especially against operational technology (OT) and industrial control systems (ICS). Ransomware attacks against healthcare and aged care organisations are also common, and the attackers often steal medical, personal, and business information.

In the face of sophisticated attacks, most private and public-sector organisations have focused on patching end points and making employees aware of social engineering methods. However, one largely overlooked attack vector is the home router, often purchased cheaply or as part of an internet bundle and rarely secured to acceptable levels for remote work. Now that the home has become part of the organisational perimeter, it's imperative for government organisations to ensure higher grade, more secure access infrastructure for remote users.

These types of attacks will persist regardless of the evolving situation with COVID-19. Therefore, the onus is on organisations to implement strong security without compromising their ability to provide remote access to mission-critical systems. Protecting home-based users and devices in ways similar to those undertaken for office-based users and devices should be a priority.

The complexity and rapidly evolving nature of today's business networks means that government organisations require a cybersecurity platform that provides comprehensive visibility and protection across the entire attack surface, including devices, users, mobile endpoints, multicloud environments, and Software-as-a-Service (SaaS) infrastructures.

Software-defined wide area networking (SD-WAN) has emerged as a way to improve the user experience and effectively route traffic for organisations that have embraced the cloud. SD-WAN lets branch and remote users access the systems and data they need without having that traffic slowed down by having to travel through a centralised data centre. Instead, using SD-WAN, users access the cloud directly from their location. While this increases the speed of business, it also potentially increases the speed of attacks.

Given the crucial importance and potential sensitivity of information and processes under the purview of government agencies, it's essential for these organisations to choose a secure SD-WAN solution. The security component is missing from most SD-WAN solutions, leaving them exposed to the growing threat landscape. Fortinet Secure SD-WAN doesn't just manage traffic; it analyses it for threats and then remediates those threats as appropriate.

Secure SD-WAN protects the network edge, endpoints, and access. A truly secure SD-WAN solution such as Fortinet's has security built in from the ground up, not bolted on as an afterthought. It provides both networking and security that lets branch and remote workers access even bandwidth-heavy applications with a strong user experience without compromising security.

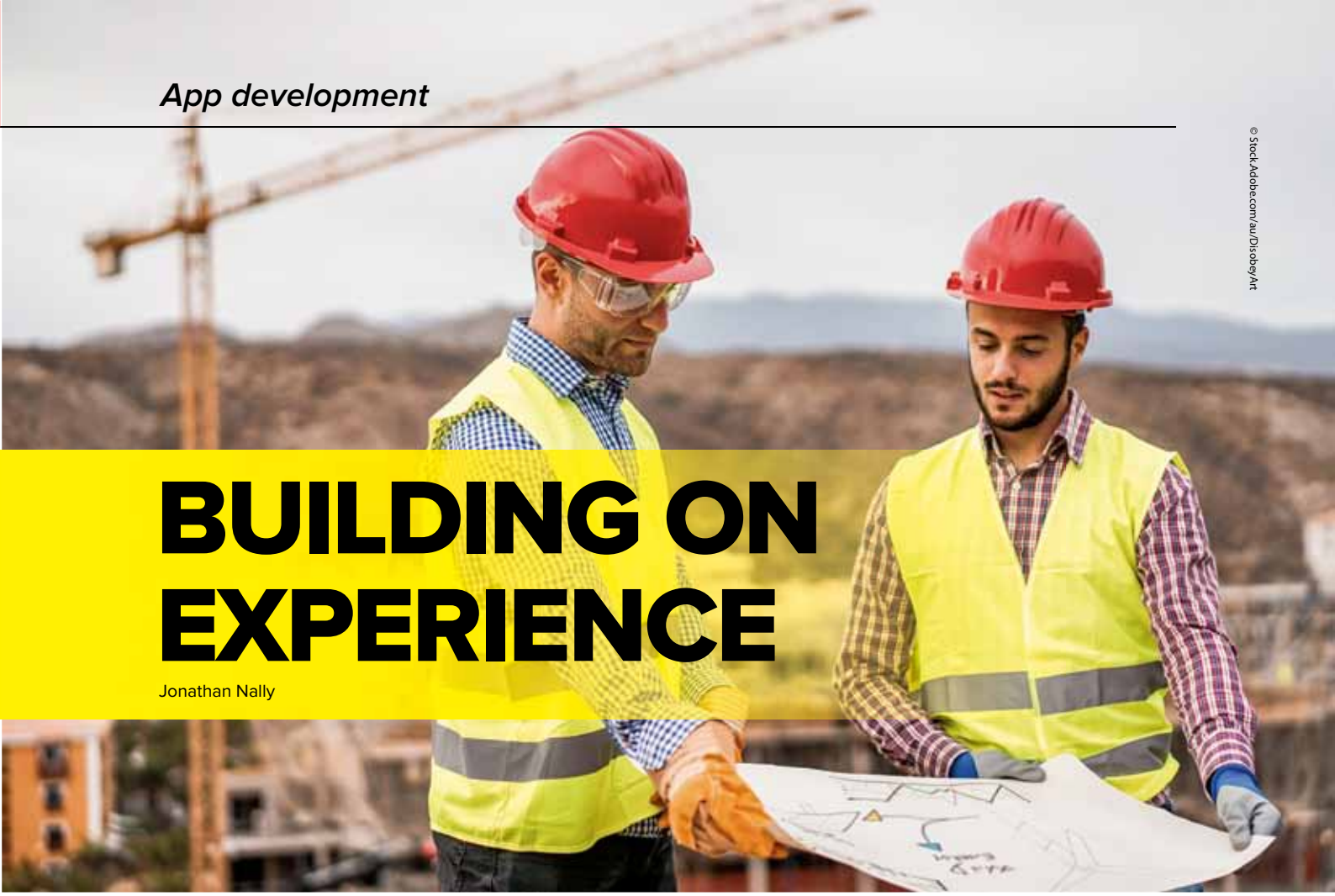
Given the rise of the distributed workforce, it's essential for government organisations to proactively manage security alongside remote access to facilitate effective remote working well into the future.

[1] https://www.cyber.gov.au/acsc/services/covid-19-cyber-security-advice

Glenn Maiden is director of threat intelligence, FortiGuard Labs ANZ, Fortinet.

FORTINET

Fortinet International Inc
www.fortinet.com



BUILDING ON EXPERIENCE

Jonathan Nally

ACT GOVERNMENT BUILDING INSPECTORS AND REGULATORY OFFICERS ARE BENEFITING FROM A SOFTWARE TOOL THAT HAS AUTOMATED TIME-CONSUMING MANUAL PROCESSES.

A software tool that helps speed the building audit and inspection process, developed by the ACT Government in conjunction with Esri Australia, has taken out Esri's top Special Achievement in GIS Award, beating solutions from more than 400,000 other organisations globally.

The tool automates many formerly manual steps in the process of identifying building projects and recording and reporting detailed audit and inspection data, while ensuring compliance with stringent building standards.

"This project is helping the ACT Government strengthen the integrity of the building industry in Canberra by giving our inspectors more tools at their fingertips when they are carrying out inspections on apartments and commercial building sites," said ACT Minister for Building Quality Improvement Gordon Ramsay.

The Minister said the project reflected the ACT Government's commitment to ensuring safer, more sustainable communities.

The government assessed various software tools to find the one that would help it develop the tool to its satisfaction, settling on Esri's ArcGIS Survey123 package.

"The ACT Government's innovative use of GIS technology to create this world-first solution has direct transferable benefits for every government agency, council and construction firm across the country and around the world," said Esri Australia National Business Manager Lisa Dykes.

"Beyond introducing greater efficiencies and more rigorous auditing standards, the solution provides transparency on building compliance and safety issues for all stakeholders.

"We congratulate the ACT Government for their meaningful achievements in this field, which will make a significant difference to the inspection and regulation of building work in the ACT — and potentially for communities across Australia and around the world."

To learn more about the development of the tool and what it does, we interviewed David Middlemiss, Senior Director in the ACT Government's Building Audit team.

What was the genesis for this project?

The genesis for the project was a review of the ACT's building regulatory system, which identified a need for a way of recording information on audits and inspections of building work to support regulation and policy analysis and evaluation.

The project is part of the ACT Government's current reform program to strengthen the regulation and integrity of the ACT building industry, under the reform to implement a government risk-based auditing and inspection system for regulated building certification and building work. The reform project was initiated and managed by the Environment, Planning and Sustainable Development Directorate's (EPSDD) Building Policy team.

How long did it take to bring it to fruition?

The work to develop the tool was [done] in two stages to align with other reforms in the program. Work on the first stage started in late 2018 and was completed for operational use by June 2019. The second stage is currently being implemented and the project will be finalised by the end of September 2020. The tool doesn't have a name at this stage.

Was it developed in-house or by an outside consultancy?

The audit program was developed by EPSDD's Building Policy team in conjunction with Esri Australia working under contract to the ACT Government. A skilled technical officer from Esri worked in-house alongside members of the policy team, including members with building, building inspection, building surveying, fire engineering, structural engineering and policy evaluation and development backgrounds, including officers that will be using the tool. The team also included project management and coordination from both the contractor and government staff and collaboration with an in-house government IT professional.

Were there any challenges in developing the tool?

The audit tool relies on data from a range of different sources to prepopulate information on each project. This required a large amount of testing to make sure data was accurately and consistently imported into the tool. The standards and regulations the tool is based on are very complex and it was important to consider how to best represent them. The amount of information that could also be included in the dashboard was also extensive, so it was a challenge to select which information would be included and decide how best to present it for end users.

How does the tool use GIS?

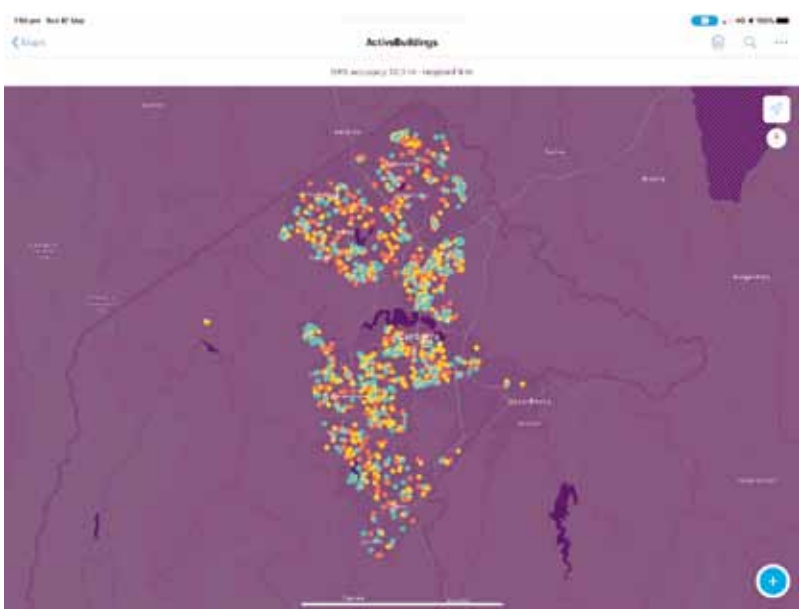
The program links directly with the ACT Government's interactive mapping service, ACTmapi, allowing government building inspectors to identify a building site by location on a geospatial map, or by building approval data. It can identify all building approval sites and basic information reaching back to 2018. Using the GIS system is important to minimise the time building inspectors spend on accessing records and selecting and scheduling projects for auditing or inspection.

Have any other governments shown interest?

The program has been purpose-built for only the ACT Government's needs. Some of the surveys relate to building standards common across Australian jurisdictions, which could be replicated. Others are specific to ACT legislation, guidelines and code of practice.

Does the tool gather data from other systems?

The tool is populated with data from the ACT Government's building approval data records, which is contained in another government system. It sources relevant information from that system to automatically prepopulate a range of fields outlining important information about the project, the type of work and relevant licensees, thus minimising human error and reducing search time. The program is also linked to other systems, including ACTmapi and the licensing database, and captures ABN



Screenshot from the building audit and inspection and software tool, courtesy ACT Government.

details from ASIC portals. It also links to a range of standards and regulations, including the online Building Code of Australia.

Who is allowed use it?

It has been designed for use by ACT Government building inspectors and regulatory officers. At this stage it has not been configured for external use as the data it collects includes information generally protected by privacy laws. As well as its use by the regulator to identify areas in which to focus targeted industry audits and information releases, the outputs will also be used by building policy officers for evaluation and development of policy and regulation.

What sort of feedback have you had?

ACT Government building inspectors have provided positive feedback on the new program, which is accessible both out on construction sites through iPads and within the office on laptops, iPads and desktop computers, for desktop audits. After receiving training on the use of the audit tool, they have found it both easy and efficient to use.

What sort of savings in time, money, effort does it provide?

Prior to introducing the audit program, many processes had to be carried out by building inspectors for each project, including sourcing information and building approval data, identifying the relevant version of the building standards, and inputting all data into report formats. The new program enables quick access to this information, removing potential for human error in data collection, reducing search costs and enabling detailed analysis without manually extracting data from individual inspection reports. It is expected this will make audit and inspection processes more time efficient, enabling a greater number of audits to be conducted in a period than previously.

Are there any plans for expanding the tool?

The second phase of the audit program was introduced on 1 July 2020 as an extension to the original tool. This new phase incorporates additional versions of building standards applying to new projects, relevant regulations, as well as new guidelines and code of practice developed under the reform program. The way the program was designed allows us to add in additional content if required, and we see its potential for expansion into other areas of regulation applying to the building and construction industry.

How important was the collaboration with Esri?

It's been great to work with Esri to push the bounds and find out what Survey123 is capable of. We weren't sure at the beginning if the tool could be developed as we'd envisioned, so it's been rewarding for all involved to see this project come to fruition.

Calendar

AusCERT Cyber Security Conference
Online: 15–18 September
Speakers, tutorials, workshops and networking opportunities.
conference.auscert.org.au

IoT Festival 2020
Online: 28 September–December
Explore trends, challenges, opportunities and applications of the IoT.
www.iothub.com.au/iotfestival

Technology in Government 2020
Online: 3–4 November
Two days of learning and networking for government ICT leaders.
terrapinn.com/conference/technology-in-government/

EduTech 2020
Online: 9–10 November
Two days of learning and networking across all levels of education.
terrapinn.com/exhibition/edutech-australia/

Data Loss Prevention
Online: 1 October
Safeguarding confidential and critical information.
publicsectornetwork.co

Australian Security Summit
Online: 1 December
Ensuring security through multilateral collaborations.
publicsectornetwork.co

Australian Cyber Conference 2021
Canberra: 16–18 March
Providing leaders with cybersecurity insights and best practices skills.
cyberconference.com.au

Comms Connect New Zealand 2021
Wellington: 5 May 2021
Panels, case studies, tech insights and training for critical comms users.
comms-connect.com.au/event/comms-connect-nz/

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

Comms Connect Melbourne 2021
Melbourne: November
Showcasing the latest technologies and solutions in communications.
comms-connect.com.au

PROTECTING CITIZENS' PRIVACY IN SMART CITIES

Neil Lappage

COUNCILS MUST FORMULATE A POLICY ON THE USE OF VIDEO ANALYTICS EARLY ON TO ENSURE THAT COMPLIANCE IS ACHIEVED.

The rise of video analytics is enabling local councils and government agencies to gain insights to improve operations; make more informed, data-driven decisions; enhance citizen engagement; improve transportation; and create safer communities.

However, it also poses a challenge for security and privacy professionals — how to balance the organisation's desire for information while preserving public privacy. This is compounded by the fact that the service can be outsourced, so proper due diligence is required when selecting a vendor.

With a carefully thought-out approach, value from captured information can be derived and privacy can be preserved without increased risk. Furthermore, where feasible, compliance with privacy legislation can be achieved by not collecting personal information in the first place.

There are a couple of approaches to avoid collecting personal information when using cameras of a high enough resolution. The most effective is to process the video stream in memory and not to store it on disk. Another approach is to obfuscate faces, effectively applying a de-identification technique. In both cases, advice should be sought to ensure that legislative requirements are met.

Special thought should also be given to collecting personal information and law enforcement. If cameras collect footage, then law enforcement may approach the council for footage, which can place a burden on both the council and vendor. For example, video footage that is requested by law enforcement may need to be retained for a longer period.

In some cases, compliance can be achieved by collecting video of a low enough quality that would not allow a person to be reasonably identified. However, in such a case there is also the risk that the quality of the video stream may experience false positives and produce count statistics that are not accurate.

If a vendor does collect personal information on behalf of a council, it is imperative that controls are implemented to ensure the ongoing confidentiality of that information. This often starts with a notice that informs the public that data is being collected for analytical purposes.

From here, security and privacy professionals need to translate 'privacy by design' into software engineering. Using a blend of controls such as encryption-in-transit, encryption-at-rest and access control, solutions can be secured to reduce the risk of unauthorised access.

Specific consideration should be given to the access control applied to live feeds to ensure that internal teams can only access video streams on a 'need to know' basis and with the principle of 'least privilege' applied.

For larger councils and government departments, privacy impact assessments (PIAs) can be used as a tool to better understand the privacy impacts of data being collected and processed by the solution. Since video analytics is a relatively new technology, PIAs can be used by privacy and security professionals to provide guidance and protocols for best practice.

As an example, councils must ensure vendors understand their responsibilities with collecting personal information and the impacts of using this information for purposes other than its intended use, such as selling it to third parties.

It is important that councils formulate a policy on the use of video analytics early on to ensure that compliance is achieved, controls are standardised and ultimately that the organisation benefits from its investment. It is a prime example of where security architecture and risk professionals need to apply privacy by design. This will ensure unauthorised access does not lead to financial loss and reputational damage.

Neil Lappage is a partner with LeadingEdgeCyber and an advisor in ISACA's Emerging Technology Group.

Don't wait for the bushfire to strike to digitally transform

Regional councils who've lived through a natural disaster say digital preparedness is key.

It's time to learn the lesson our colleagues in regional and regional councils already know — you don't wait for the bushfire till the bush fire is upon you. Now's the time to be investing in the tools to help you fight the next fire.

While the level of disruption from COVID-19 is unprecedented, for many Australian local governments, planning for disruptive events is a common practice — and it's leading them to cloud-based solutions.

At Tablelands Regional Council, based in Atherton Queensland, Senior Business Services Officer Sarelle Sinclair says the risk of severe weather events was a key part of the reason for the recent decision to move parts of its information technology infrastructure to the cloud.

"We wanted to modernise our systems and overcome limitations such as ageing infrastructure, and the risks of operating in a remote, cyclone-prone area. The purpose of all of that was improved stability, mobility, speed and service — and resilience," she says.

While working away from the office during bushfire events, Noosa Shire Council's ICT Manager Justin Thomas shared on LinkedIn a vote of thanks to software solution vendors including TechnologyOne, which were helping the council's team members continue to deliver services.

Mr Thomas said his team had seen requests for IT support from within the council double in the month of March as the organisation moved to set up team members to work remotely as a result of the coronavirus situation.

So, does hands-on experience with some of the many challenges nature can throw at us influence communities — and the local government authorities which represent them — in terms of their attitudes to risk management?

"It is certainly a factor," says Ed Chung, CEO of TechnologyOne, whose software powers many of Australia's local governments. "Councils in regional and rural areas by default need to have a level of independence and self-reliance."

"We work with local government authorities all across Australia, New Zealand and the UK. And we've been in this business for thirty-three years. That's enough time to be able to observe some general trends."

"Many of our local government customers cover non-metropolitan areas. By and large, we find they run leaner operations, which usually mean less resistance to change, so they tend to be early adopters of technologies that help keep the lights in a crisis."

Mr Chung says that in rural and regional areas, council mayors tend to become the community focal point in a crisis. That responsibility also tends to focus the thinking of council executives, leading them to invest in business continuity planning.

"Geography also plays a role. When you're living and working at some distance from the 'Big Smoke' you know that help, when it comes, is going to take a while. That tends to foster a level of self-reliance in the people running rural and regional councils."

"That responsibility means councils themselves have to think long term about their ability to provide those services in an emergency. That invariably leads to business continuity planning and, these days, that leads them to cloud-based solutions," Mr Chung says.

It's time to learn the lesson our colleagues in regional and regional councils already know. You don't wait for the bushfire till the bush fire is upon you. Now's the time to be investing in the tools to help you fight the next fire.

Visit TechnologyOne for more.

technologyone

TechnologyOne
www.technologyonecorp.com

PUBLIC SECTOR NETWORK

Certified B Corporation

Join the social learning platform for public sector

Get **FREE** unlimited access to the latest information and trends transforming the government landscape

Sign up to become a member today!
www.publicsectornetwork.co

COMMUNITIES WE SERVE

Corporate & Shared Services

Cyber Security & Risk Management

Data Management & Analytics

Defence, Security & Justice

Digital Government & CX

Health & Human Services

HR & Future of Work

Innovation & ICT

Local Government & Municipalities

Smart & Sustainable Communities

info@publicsectornetwork.co

+61 (2) 9057 9070

CANBERRA LIFTS CYBERSECURITY COMMITMENT TO $1.67BN

Dylan Bushell-Embling

Australian Federal Police will be equipped with new tools to investigate and shut down cybercrime on the dark web as part of the federal government's new $1.67 billion cybersecurity funding commitment announced on Thursday.

The Cyber Security Strategy 2020 will see the $1.67 billion invested over the next 10 years in what represents the government's largest cybersecurity investment program to date.

As part of the strategy, new laws will be introduced giving the AFP and the Australian Criminal Intelligence Commission the tools and powers required to collect information on investigations of crimes conducted on the dark web or using anonymising technologies such as end-to-end encryption.

Meanwhile, the government has flagged plans to "confront illegal activity, including by using our offensive cyber capabilities against offshore criminals, consistent with international law".

The investment will also fund the establishment of a 24/7 cybersecurity advice hotline for SMEs and families. >

Meanwhile, providers of critical infrastructure will have new obligations imposed on them to shore up their assets against major cyber attacks. The commitment includes a $66 million allocation to help these companies assess their networks for vulnerabilities.

The definition of what will be considered critical infrastructure will also be expanded to incorporate banking, finance, health, food and grocery infrastructure.

The government has also committed to providing support for SMEs to upgrade their cyber defences, including by working with large businesses to develop "bundles" of secure services such as threat blocking, antivirus and cybersecurity awareness training to these SMEs.

Meanwhile, the government has flagged that it will investigate introducing regulatory reforms giving the internet-connected consumer device industry more obligations to protect end users, and is planning to encourage the development of new awareness campaigns for consumers.

The $1.67 billion commitment includes and expands on the $1.3 billion announced in June to allow for the recruitment of 500 new cyber spies for the Australian Signals Directorate (ASD).

Other initiatives in the strategy include a commitment to create a fund to co-invest in counter-cybercrime capabilities with the states and territories, and to spend $62.3 million to develop a classified national situational awareness capability.

Many of the initiatives were informed by the recommendations of the Cybersecurity Industry Advisory Panel, chaired by Telstra CEO Andy Pen, which recently published the findings of its investigations.

© Stock.Adobe.com/au/Andrey

WARM REACTION

Industry representatives and experts have generally welcomed the recommendations. Australian Information Industry Association (AIIA) CEO Ron Gauci said the commitments represent an acknowledgement that critical infrastructure is increasingly becoming a target for cybercrime.

"Operational technology used in critical infrastructure, manufacturing, sensors or building controllers traditionally operate on separate networks with different protocols. In recent years we have seen the line blurred with these devices becoming IP-enabled or connected to IoT-type devices," he said.

"We appreciate that the Prime Minister has listened and understands the need to continue investment and support with cybersecurity — as evident by The Cyber Security Review, which was led by The Department of the Prime Minister and Cabinet, which highlighted that cybercrime is costing the Australian economy in excess of $1 billion annually in direct costs alone."

Meanwhile, Communications Alliance CEO John Stanton praised the planned measures designed to enhance collaboration between critical infrastructure sectors by improving the sharing of threat data.

"We will engage with stakeholders to develop a clearer understanding of the details of the Strategy, such as the definitional aspects around 'systems of national significance' and 'critical infrastructure entities'," he said.

But he said it will be important that the government is clear and transparent about aspects including what will constitute systems of national significance, as well as areas where the government has raised the prospect of "direct action" by government to protect networks and systems in times of cyber crisis.

"Government needs to consult collaboratively with industry on these aspects, to ensure that the infrastructure our industry owns and operates so successfully remains actively and passively protected from cyber interference," Stanton said.

Palo Alto Networks Head of Government Affairs and Public Policy for ANZ Sarah Sloan said the initiatives outlined in the strategy will promote public partnerships to combat cyber threats.

"Only by working together will we be able to identify and address cyber threats at scale," she said. "In our increasingly interconnected world, improving the security and resilience of critical infrastructure entities is crucial to protecting Australia's economy and national security."

But Macquarie Government Managing Director Aidan Tudehope said it will be critical to act on the strategy now rather than waiting 2–3 years.

"With COVID, we are facing the greatest economic crisis in 100 years. And the cybersecurity sector is a key sector to provide the jobs of the future," he said. "The various government agencies responsible for implementing the strategy need to use it to help address the mass levels of unemployment being experienced across Australia. We can't afford to wait two to three years when it will be too late to innovate our way out of this crisis."

TRUST
Frontier Software with your payroll processing

Accurate, secure and reliable

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

Frontier software

Human Capital Management
& Payroll Software/Services

RPA: WHERE IT WORKS, WHERE IT DOESN'T AND WHEN YOU SHOULDN'T

Emily Bone

RPA IS A SOLUTION TO IMPROVE INEFFICIENCIES OR REMOVE ERRORS IN PROCESSING BY AUTOMATING AT A TASK LEVEL WHERE IT MAKES SENSE.

In Martin Ford's 2015 book, *The Rise of the Robots*, intelligent algorithms, automation and artificial intelligence were described as having terrifying societal implications. As it turns out, in 2020, a far bigger threat to unemployment rates and society unravelled.

As we navigate our way out, cutting costs and finding better ways to operate is non-negotiable.

In this race, robotic process automation (RPA) is being met with new optimism, as the application of intelligent automation (IA) and artificial intelligence (AI) prove they can contribute significantly to cost-saving objectives.

With use cases applicable in human resources, procurement, finance and many front office operations, any job that is on some level routine could be automated.

However, that doesn't mean it should.

Not every business process is a good fit for automation. Some are best handled by humans — such as many customer-facing processes — and some, you might find, should be removed entirely.

A common approach we see organisations take when looking to capitalise on automation is treating RPA as a standalone technology solution and leading the solution with the question of 'what processes should we automate'.

The issue with this is that they haven't paused to reflect on parts of the process that may not be needed, or which don't contribute to the outputs of the process. Effectively, you risk automating the process waste.

Another consideration is long-term ROI. Many companies start by choosing 'low hanging fruit', identifying areas where staff hours can be saved and thus benefits realised relatively quickly.

However, unless these investment areas are well integrated into business workflows and can achieve cost, revenue building, safety or other business goals, they run the risk of being categorised as technical debt when revisited two or three years later.

OPTIMISE, THEN AUTOMATE

When building your business case for RPA, you should consider that getting the most value long-term out of your investment relies on the improved outputs and quality, which in turn leads to lower costs and efficient processes.

To achieve this, RPA must be part of a broader business process analysis and optimisation to:

- simplify the process and remove wastage, duplication and over processing;
- re-examine business rules to ensure they are up to date and consistent;
- identify at a task level the best candidates for automation and allow staff to be re-focused on high value;
- implement supporting solutions like centralising data to streamline the amount and frequency of switching between systems.

RPA is a solution to improve inefficiencies or remove errors in processing by automating at a task level where it makes sense.

By identifying the areas that have the most potential for optimisation, and considering automation as one of the potential options, you can identify and implement the most effective strategies to reduce costs and improve efficiencies.

Emily Bone is National Capability Manager for ASG Group.

WEATHERING THE STORM: OVERCOMING TECHNOLOGY SUPPLY CHAIN RISK

BOOSTING AUSTRALIA'S LOCAL MANUFACTURING AND SUPPLY BASE WILL PUT US IN A GOOD PLACE FOR A RETURN TO GROWTH.

With increasing customer uncertainty, many industries have faced a significant drop in consumer demand: but not so for information technology. Demand increased dramatically as the pandemic — and the associated societal shutdown — took hold and sent many of us home to work from our home office. Organisations that have required their workers to take their work home found it necessary to ramp up their supply of mobile computing technology — both to enable their staff to work at home and also to ensure the organisations' applications were fully accessible and usage policies are adhered to.

While the availability of software would never be an issue, and the communications infrastructure in Australia has proven itself sufficiently reliable to enable remote working, the supply of the necessary computing hardware is a different matter. Like many other industries in Australia, the IT industry is heavily dependent on overseas supply chains for the supply of hardware such as desktop PCs, servers and laptops. And with so many countries closing their borders, and internationals flights grounded, the result has been freight costs that have doubled or even quadrupled, as well as long delays in delivery times.

In a report published in April, Gartner said that "worldwide PC shipments declined 12.3% in the first quarter of 2020", and directly attributed this to the coronavirus pandemic.[1] For Australia, which has no appreciable local technology manufacturing, this has been a problem. But for those few organisations that can provide a local supply chain, there has been a significant increase in turnover.

Even if the components are sourced from overseas, local PC and laptop assembly from well-established component stock has provided a buffer to enable companies such as Acer to rise to the challenge of supporting the computing needs of Australian organisations.

We mustn't forget, however, that the pandemic is not the only problem creating headlines in recent times. The growing attention being given to Australia's relationship with its 'largest trading partner' and growing concerns over cybersecurity risk and cyber-infiltration have raised many questions about the technology we use: questions about relying on not only technology sourced from international suppliers — especially for those organisations that may be potential targets for cyber-espionage — but also the greater risk of computing hardware being taken out of the office in larger numbers.

When your staff take your organisation's computing assets home with them, they are no longer in the (hopefully) safe and secure environment of the workplace. The application of a well-designed and implemented standard operation environment (SOE) on those devices has never been more important. Not only does it enable your organisation to have greater control over the security of the device, it also enables easier technical support when your users experience problems.

The rapid deployment of a standardised hardware platform, running an approved SOE — and for a larger than ever mobile workforce — places an excessive demand on IT staff when they need to be focused on ensuring that the backend systems and networks in the data centre can manage reliably with the increased remote access demands.

Outsourcing deployment to a local supplier that can not only provide local assembly but also customisation and SOE deployment at scale can reduce the headaches and overheads in safely and rapidly deploying technology for a mobile workforce.

And when it comes to rotation and upgrade, as well as disposal, of those same assets, a local accredited supplier can also help make sure the old assets are disposed of and recycled safely and securely.

They say that 2020 will be a year Australia will never forget: but what it has shown us is that we can rise to any challenge presented to us. Decreasing our demand on overseas suppliers and growing our local manufacturing and supply base will see us not only weather the storm of 2020, but put us in a good place for growth when it is all over.

Rod Bassi is Oceanic Sales Director for Acer Inc.

1. Gartner 2020, Gartner Says Worldwide PC Shipments Declined 12.3% in the First Quarter of 2020 Due to Coronavirus Pandemic.

Password management solves a council's IT concerns

LastPass password management has become a critical asset in helping Lockyer Valley Regional Council staff members perform their jobs.

Lockyer Valley Regional Council's vision is to deliver sustainable services to enhance the liveability of its community while embracing its economic, cultural and natural diversity. The Council strives to enable opportunities within its region with a strong customer focus, and, as a local government authority, it is committed to providing quality services to residents and visitors in the pursuit of its vision.

With the aim of improving security across the organisation, the Council engaged an external auditor to identify risk factors and potential cyber security threats. It was aware that the security practices of general staff weren't particularly good when it came to storing account credentials, and many helpdesk tickets were being raised to have credentials reset as a result of them being shared between staff members. The ICT team had deployed a tool to manage credentials, but it was too technical and could not scale to cover accounting, consultants, office workers and other departments.

Following the audit, the recommendation was made to deploy an enterprise password management (EPM) solution across the organisation. A team of evaluators was assembled to review the EPM options available. The goal was to find a solution that is easy to use and will deliver the visibility and control that IT security needs.

"When we added up all the scores, LastPass came out on top. It's just really easy to use, and if you want the organisation to use it, then it needs to work for them as much as it needs to work for IT security," said Anjana Ranatunge, Coordinator ICT Projects and Business Operations at Lockyer Valley Regional Council.

The Council believes it is close to delivering on its goals, with Ranatunge saying the feedback has been very positive as "people don't want the hassle of keeping track of passwords, sharing passwords or resetting passwords, so now they do that all via one system".

"It saves employees a lot of time and many view LastPass as critical to efficiently performing their job," Ranatunge added. So far, there has been a significant reduction in calls to the helpdesk and tickets raised for login credential resets, a reflection of the almost-80% adoption rate. This "just shows how user friendly LastPass is," said Ranatunge.

The security team uses the solution's admin centre to gain better insights into the security posture of the organisation, and uses policies to help encourage the right staff behaviours. The LastPass team "excelled at showing us the value of the LastPass suite, which made it easy to sell internally," said Ranatunge. "I can't speak highly enough of the LastPass Customer Success Manager. Always positive and had or could source answers promptly."

LastPass ••• | by LogMeIn

LastPass
www.lastpass.com

Western Parkland City councils join smart city ecosystem

A Randwick City Council digital sign

Western Parkland City councils have joined an ecosystem of 11 other Australian councils to accelerate their smart city initiatives.

There are many examples of Australian councils embarking on smart city journeys, but many of them meeting with mixed success — from vertical/siloed solutions to complex, time-consuming and expensive initiatives — before being able to demonstrate any tangible outcomes and benefits to their stakeholders and the community.

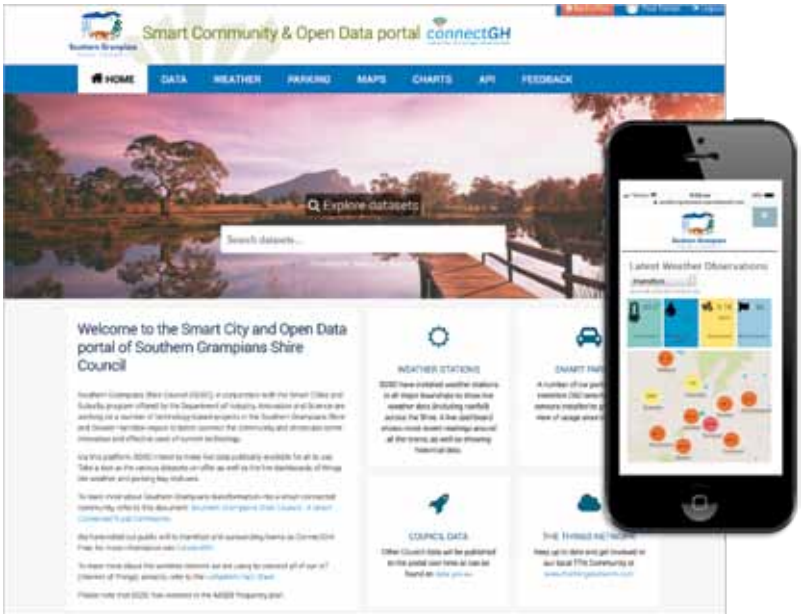
Smart city initiatives don't have to be complex, time consuming or expensive. Take, for example, the Southern Grampians Shire Council, which didn't have the luxury of spending hundreds of thousands of dollars before demonstrating value to its community. The council has been frugal in its approach and spent a fraction of what some councils have spent for similar projects, but nonetheless was one of the first regional councils to deliver an end-to-end smart city solution back in 2018. Southern Grampians' solution is based on a LoRaWAN network and sensors, open source platform The Things Network, and the Opendatasoft open data portal. Within just a few weeks the Council was able to make hyper-local weather data available to local farmers by installing 10 weather stations across the council area and by publishing the data on its user-friendly connect Greater Hamilton (connectGH) platform. Initial use cases also included smart parking sensors installed in Hamilton town centre, with associated real-time maps on connectGH.

Eurobodalla Shire Council is another great example of a regional council that has been able to progress quicker than most larger cities and with minimal spending. Its smart city solution is based on a LoRaWAN network, Ubidots IoT platform and Opendatasoft for data sharing. The range of use cases it has been able to implement is impressive: smart bins and smart parking pilots in Batemans Bay, people counting in the public library, GPS tracking of council vehicles, traffic counting on the Princess Highway and at various boat ramps, flood monitoring, and even flying fox counting! The data it is collecting about the Princess Highway is made available to Transport for NSW and has been instrumental in right-sizing the new bridge at the entrance to Batemans Bay. With flood monitoring the council is able to send early warnings to local businesses that might be affected.

Interestingly, some larger councils such as the City of Greater Geelong have looked at these solutions and realised that — despite their larger size and potentially larger ICT budget — there was no reason why they should over complicate their smart city architecture when turnkey solutions such as Ubidots and Opendatasoft would make their life easy and accelerate delivery. According to Peclet's CTO, Hassan Gabru, "All our components are on scalable AWS infrastructure, so there is no limit on the number of users and size of operations it can support. Huge cities like Paris and Mexico City are using Opendatasoft, and the City of Melbourne is also using Opendatasoft for their IoT and 5G tested."

Collaboration leads to better outcomes

Another key success factor for smart city initiatives is collaboration between councils. This is about councils sharing experience, ICT platforms and data, and even bringing together ICT funding to afford better solutions. Geelong and Ballarat understood this early. When Geelong became an early adopter of Opendatasoft for its Geelong Data Exchange platform, it did not take long for neighbour Ballarat to decide to share the same platform for the Ballarat Data Exchange. Although the two data portals have a different look and feel in line with the respective councils' branding, both portals are underpinned by Opendatasoft with appropriate security controls to keep certain datasets private. Sharing the same platform is providing



The connectGH website

economies of scale on licensing costs and giving them access to greater functionalities… and ultimately providing a better user experience to community members, who are now able to seamlessly search and visualise datasets across a broader geographical area.

More recently, the Western Parkland City councils — comprising Blue Mountains, Camden, Campbelltown, Fairfield, Hawkesbury, Liverpool, Penrith and Wollondilly — is another impressive example of councils collaborating together. Recently awarded a grant from the Smart City Smart Suburb program for their sensor network project, one of the key risks would have been for these councils to follow different technological directions and end up with a complex architecture. But this did not materialise, and Western Parkland can be proud of being one of the largest (if not the largest) Australian group of councils to take such a coordinated approach in shaping its smart city architecture.

According to Sharlene Van Leerdam from Campbelltown City Council, "It did not take us long to reach consensus on selecting Ubidots and Opendatasoft as it is giving each council the flexibility to have their own secured environment and branding while providing us the ability to easily share data between us, with our business partners (e.g. Sydney Water, UoW and UNSW) and with our community. Plus it allows us to roll up datasets from eight councils into one centralised view on our Western Parkland City parent site.

"We also loved that our community can create a login to build their own maps or charts, allowing them to upskill and be innovative. Sharing the same platform also gives us access to leading technology at an affordable price, and also the ability to share components like dashboards that we are going to develop, hence minimising our implementation effort," she said.

"The opportunity to partner with Peclet to solve easily accessible data was brought forward to the councils via the City Deal Digital Commitments Industry Engagement, which allowed companies to pitch their solution. I am super-excited to be leading this initiative."

Open data is a benefits multiplier

One of the requirements for the lucky councils awarded a grant from the Smart City Smart Suburb program is to open up their data. Unfortunately, too many councils see the open data requirement as a constraint rather than an opportunity. Many councils have taken a first step by publishing some static datasets, or some spatial or financial data for transparency purpose.

While this is a great first step, successful open data portals are the ones that bring it all together, i.e. IoT real-time data, static data, spatial data, financial data and so on, all in one place. This is because open data users have different needs and are interested in different things — engineers might need geospatial data, economists might be interested in how funding has been spent, while tech start-ups may require IoT data to come up with the next great innovation.

Some, such as Randwick City Council, even took open data to the next level and developed open data multi-channels. Instead of keeping data just for its internal needs, the data is also made available on digital signage on the beach. IoT data is mashed-up with other open data sources such as lifeguard feeds, Environment NSW's Ocean Bulletin and Transport for NSW data. The benefits to end users is massive, as it is improving the safety and experience of thousands of beach goers 365 days per year. Such an innovative approach would no doubt benefit many other coastal councils across Australia.

Three ingredients for success

In summary, the key ingredients for successful smart city initiatives are *keep it simple*, *collaborate* with your neighbours and *share your data*. At Peclet, our vision is to build an ecosystem where councils can collaborate and share data, but also share platforms and value-add components such as data visualisations — if we develop a great dashboard for one councilÂ, it is made available to all others as open source. This way, councils can invest in new ideas rather than paying for what has already been done elsewhere.

Our approach is also to provide councils with easy-to-use, turnkey solutions that give them the level of autonomy they want. When Ballarat signed up with Opendatasoft, it did all the configuration itself and produced one of the best open data portals in Australia.

peclet
TECHNOLOGY

Peclet Technology Pty Ltd
www.peclet.com.au

Featured products

Behaviour-based intrusion detection

Next-gen IDS solutions require complete and precise data, not partial, sampled data. The single source of truth for any IT environment is network traffic. If any network access occurs or any malicious behaviour takes place, it can be shown in the traffic and data. Accedian Skylight, available from Vicom, examines everything on the wire for complete, high-definition visibility.

To provide strong threat and illicit behaviour detection, 100% of the transactions traversing the network must be analysed for complete visibility. Skylight examines all of the pertinent network layers to achieve that goal.

Skylight is available as an add-on in Splunk Security Essentials, and security use cases from Accedian are also available as an add-on in Splunk Security Essentials.

Vicom Australia Pty Ltd
www.vicom.com.au

Enclosures

MFB's SoHo 210 range of enclosures offers a useful solution for removing desk clutter. The simple enclosures provide a vertical storage solution for equipment that could otherwise take up unnecessary desk space. Simply drop one under a desk to house modems, switches, routers and other peripheral devices.

The enclosures can be supplied unassembled or assembled with common MFB accessories including shelving and power distribution boards. They are available in a range of heights and depths and a range of powder coat colour finishes.

MFB Products Pty Ltd
www.mfb.com.au

Ethernet switches

Advantech 10G Ethernet switches are futureproof Ethernet devices consisting of both 1G and 10G ports. The 10G ports are backward compliant with 1G, 2.5G and 5G. Multiple transmission speeds provide each connected device with the most suitable network service. The 10G Ethernet switches provide users with high network deployment flexibility, making them suitable network devices for those expecting to upgrade their devices or undertake quantity expansion in the future.

For machine vision and video surveillance applications, transmission bandwidth requirements are higher than what traditional 10/100/1000 Mbps can satisfy. The 10G uplink ports prevent users from experiencing data loss or latency — helping to guarantee network transmission quality.

Ranging from 8 to 54 ports, Advantech's 10G Ethernet switch product line includes six different models for all network deployment needs. The rackmount design allows the devices to be either installed in a rack or on a desk. Both managed and unmanaged SKUs are available for various applications. Optional PoE ports deliver both data and power on one wire to PD devices. The SFP ports can further extend the transmission distance from 100 m to 100+ km for widened geographical network coverage.

Advantech Australia Pty Ltd
www.advantech.net.au

Image credit: Juvare

Unify Emergency Response with Juvare Fusion

There is an expectation from Government and Public alike that emergency services and support agencies will work together in the response to incidents and events that impact lives and property. Every Australian State and Territory has previously conducted a review or inquiry into ideal emergency response with similar recommendations; the need for agencies to share incident information to provide a common operating picture and ensure the efficient, timely and effective use of resources to help communities respond and recover from major incidents and events.

In reality, most agencies work on separate systems that do not connect with other systems and work in silos. Agencies find it hard to share information — when they do, it is often outdated or no longer relevant.

The need for a highly configurable yet integrated platform was never more critical than in response to the current COVID-19 pandemic. Agencies need a system that can be configured for their specific use whilst still being able to connect to other agencies.

Western Australia elected to work with Juvare to utilise the WebEOC Incident and Information management system by Juvare for the State's response to COVID-19.

The State needed a platform that could connect-up all agencies using WebEOC and also include other agencies involved in the response that didn't have an incident management system.

The State implemented and used Juvare's WebFusion, a highly secure system that connected all agencies currently using WebEOC, whilst allowing support agencies to use the State WebEOC platform. Each agency could configure their WebEOC system specifically to their requirements, whilst being able to connect to the State Fusion platform to share daily updates and situational reports.

This was the first time in Australia that 30 agencies were able to manage their own response whilst being able to instantly share information across all agencies and to the State response team.

To learn more about how Juvare can help you connect and communicate across the emergency service agencies in your state contact the Juvare Asia Pacific team today on 1800 JUVARE (1800 588 273) or visit https://www.juvare.com/webeoc/.

JUVARE

Juvare
www.juvare.com

NEW ZEALAND AGENCIES COMMIT TO ALGORITHM CHARTER

Dylan Bushell-Embling

THE NZ GOVERNMENT IS CALLING ON OTHERS TO FOLLOW ITS LEAD BY INTRODUCING A CHARTER ON ETHICAL USE OF ALGORITHMS.

The New Zealand government has launched a world-first set of standards to guide the ethical use of algorithms by public sector agencies.

The Algorithm Charter for Aotearoa New Zealand has a core goal of improving government transparency and accountability without stifling innovation or causing undue compliance burden for agencies.

The charter has been signed by 21 agencies, including the ministries of the Environment, Justice and Education, the Department of Internal Affairs, and Inland Revenue.

The charter, which has also been published in Māori, has also been signed by the Ministry of Māori Development, Ministry for Pacific Peoples, the Ministry for Social Development and Land Information New Zealand.

Under the new charter, agencies will conduct a risk impact assessment of their algorithm decisions based on a matrix that has on one side the probability of an impact occurring during standard operations and on the other the anticipated extent of this impact.

For decisions that are found to rank highly on both criteria, agencies have agreed to apply the charter. This approach will allow agencies to focus on decisions that have a high risk while excluding many business-as-usual activities.

Signatories to the charter have committed to maintaining transparency by clearly explaining how decisions are informed by algorithms.

According to the charter, this may include publishing plain English documentation of the algorithm, as well as making publicly available information about the data and processes being used and how this data is collected, secured and stored.

Agencies have also committed to honour the government's Treaty of Waitangi commitments by embedding a Māori perspective in the development and use of algorithms.

Likewise, signatories have committed to regularly peer reviewing algorithms to ensure privacy, ethics and human rights are protected.

Other commitments focused on citizens include consulting with people who have an interest in algorithms or are impacted by their use before making decisions, and nominating a point of contact for public inquiries about algorithms.

Meanwhile, the government plans to provide a channel for challenging or appealing decisions informed by algorithms.

A provision built into the charter will ensure it is reviewed after 12 months to ensure it is fit for purpose.

Minister for Statistics James Shaw said the New Zealand government hopes other governments worldwide follow the nation's lead and establish their own algorithm charters.

"Most New Zealanders recognise the important role algorithms play in supporting government decision-making and policy delivery; however, they also want to know that these systems are being used safely and responsibly," he said.

"The Charter will give people that confidence. It will help to build public trust over the long term, meaning that we can unlock the full potential of data to improve people's lives. Today we have set a world-leading example of how government can work with diverse groups of people, communities and organisations to improve transparency and accountability in the use of data."

FREE

for government and industry professionals

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

wfmedia
connecting industry

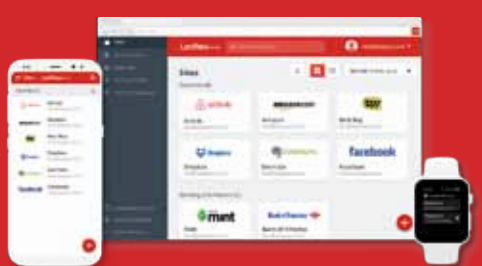
www.WFMedia.com.au/subscribe

LastPass •••|
by LogMeIn

Protect and empower the digital identities of your modern workforce.

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

www.lastpass.com



03.09.2020/PDF/LMI1309