govtech review

LEADERS IN TECH

OUR EXPERTS' PREDICTIONS FOR 2024

Q4 2023
PP100021607

Series 2005 is the leading brand of 19" rack mount enclosure for data and communications installations, with a huge range of sizes. MFB have the right cabinet for your needs.

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 ANNIVERSARY

**PROUDLY
MANUFACTURING
IN AUSTRALIA**

AUSTRALIAN MADE
MAKES AUSTRALIA

bsi. ISO 9001 Quality Management ISO 14001 Environmental Management

19" Rack Cabinets
Licence No. 44394

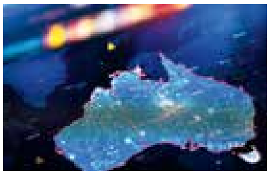
www.mfb.com.au **VIC** (03) 9801 1044 / sales@mfb.com.au **NSW** (02) 9749 1922 / sydney@mfb.com.au

Q4 2023

INSIDE

LEADERS IN TECHNOLOGY

FEATURES



Cover image: iStock.com/piranka

Insider

Well, we might not have a pandemic to contend with any longer, and many more of us are working in our office environments again (some maybe reluctantly), but it has certainly been an eventful year in the world of information technology.

This time last year we had just experienced the Medibank data breach, and all signs were pointing towards an increased threat of cyber attack throughout 2023. We were not disappointed! Apart from the high-profile breaches to Latitude Financial, Optus over the last two years and more recently DP World, there have been a slew of publicly announced breaches affecting government services, across most states and territories, and in unexpected places in the federal government such as myGov, Defence and the AFP.

As I write this, the Home Affairs Minister has announced a new package of cybersecurity support for small and medium businesses, and we can expect more announcements over coming months in relation to issues like ransomware and risks to critical infrastructure. There is certainly a lot that needs to be done by all organisations to keep up with the ever-increasing evolution of cyber threats. There is also an ongoing high demand for personnel skilled in cybersecurity, with an increasing incidence of burnout among these essential experts.

It will come as no surprise that cybersecurity concerns are expected to heavily influence strategic direction and investment in 2023.

The other hot topic is artificial intelligence, another player in the abovementioned cybersecurity challenges we all face, but also a technology already changing the way many aspects of business and government function. It is looking like all the subjects we hope to cover in 2024 will be in some way influenced by cybersecurity and AI across the board.

In this issue, we are once again presenting our annual Leaders in Technology feature in this, the final print issue of the magazine for 2023. Each December, we ask industry leaders to give us their thoughts on the year ahead — and, what technologies will gain ground, where the pain points are and what's on the wish list from government, innovators and the industry at large.

You will also notice that I have taken over from Dannielle Furness as the Editor of *GovTech Review* and *Technology Decisions*. WF Media and I thank her for her great work as Editor and wish her well in her new and future career. As for myself, I come to this role with a past experience of around 15 years in the IT industry, which I hope will further enhance the content moving forward.

As this year draws to a close I'd like to wish you the very best for the holiday season. I look forward to returning next year to bring you all the latest in technology news.

Glenn Johnson, Editor
gtr@wfmedia.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
Glenn Johnson

gtr@wfmedia.com.au

ACTING PUBLISHING DIRECTOR/MD
Janice Williams

ART DIRECTOR/PRODUCTION MANAGER
Julie Wright

ART/PRODUCTION
Linda Klobusiak, Marija Tutkovska

CIRCULATION
Dianna Alberry
circulation@wfmedia.com.au

COPY CONTROL
Mitchie Mullins
copy@wfmedia.com.au

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

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

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

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

Cognitec

The trusted face recognition company since 2002

Most experienced and highly trusted

Cognitec has been providing face recognition systems to government and commercial clients worldwide for more than 20 years. Proud to maintain a stable, leading position in the industry, we are committed to delivering the best solutions available on the market.

Focused research and development

We use state-of-the-art machine learning techniques and deep learning principles to achieve continuous advancement of the various algorithms contained in our core technology.

Reliable customer service

Cognitec's clients rely on collaborative customer service, fast response times and competent work.

Superior technology

Our algorithms perform the most important face recognition tasks with market-leading speed and accuracy. Independent evaluation tests and real-life installations continue to prove the exceptional performance of Cognitec's technology.

Successful projects worldwide

Alongside image database searches that prevent ID fraud and support criminal investigations, Cognitec's technology drives cutting-edge video security, eGate, people analytics, and photo indexing solutions.

www.cognitec.com

CAN AUSTRALIA'S BOLD DIGITAL GOVERNMENT GOALS BE MET?

Garry Valenzisi, Vice President & General Manager, Asia Pacific, Global Industries, Iron Mountain

iStock.com/da-kuk

Australia has set a goal to become one of the top three digital governments in the world by 2025, an ambitious vision that will require a coordinated effort across public sector services.

For years, governments have been discussing the oncoming 'wave' of digital transformation — how to automate administrative processes and move traditionally non-digital information, such as health care, tax records, vehicle registrations, birth certificates and much more, online.

The ultimate ambition of digitising these services and operations is to make it more efficient for public servants to access and manage necessary documents and information, and in turn, make it easier for citizens to securely and easily access vital government services.

The COVID-19 pandemic helped accelerate the pace of digital transformation efforts as public bodies were forced to move services online to accommodate remote administration needs. But with just 47% of Australia's federal services digitised so far, there is still a long way to go.

Following in the footsteps of the UK's Digital Transformation Strategy, the Australian Government has developed its own Data and Digital Government Strategy, set to be released in full at the end of 2023. The strategy will outline the government's vision to deliver simple, secure and connected public services for all people and business through world-class data and digital capabilities. It takes over from Australia's Digital Continuity 2020 Policy, a strategy released in October 2015 which set in motion a whole-of-government approach to modern digital information governance.

Some areas of the Australian Government are already seeing dividends from this new roadmap to digitisation.

For example, last year Service NSW made digital vehicle registration certificates and push-notifications for renewal reminders available to motorists via their Service NSW online accounts. Digitising the process end to end allows Service NSW to address the 16% of registrations that are not renewed on time for various reasons — including damaged, misplaced or forgotten paperwork — while reducing the 7.2 million paper renewal notices sent by Transport for NSW each year.

The digitalisation of these records not only allows government to optimise their resources, but also be more agile in their information management. By not having to deal with fragmented archives of both hard-copy and digital records, public sector offices are better equipped to deal with large volumes of documentation and achieve turnover in tight timeframes.

Adopting a digital-first strategy means workers can identify, track and respond to requests with the correct documentation at speed, while saving digital copies and protecting against future damage to records. Fewer repetitive tasks also paves the way for higher levels of job satisfaction productivity benefits.

Australian citizens are likely to embrace these changes too, enjoying the personalisation and timesaving benefits that digitalisation brings to administrative tasks.

According to data from the Publicis Sapient Digital Citizen Report 2023, Australians are confident in using technology to engage with digital citizen service. 94% have used at least one digital government service, most notably MyGov (56%), health care (55%) and financial services/taxes (45%). 95% of users who participated in the pilot trial for the digital vehicle registration system for Service NSW in 2022 were happy with the digital process.

THE CORE OF DIGITAL TRANSFORMATION

If the benefits of digital transformation are clear, then why is just over half of the Australian public sector still dealing with a patchwork of traditional and digital archives?

To achieve digital transformation is to tackle the digitisation of sensitive and confidential document collections, in many cases in a variety of different formats, usually for long-term preservation. To do this, technology providers need to understand the pain points of the public sector and work with them to understand workflow issues and regulatory compliance requirements and overcome inertia.

Data protection laws, such as the federal *Privacy Act 1988*, which includes the Australian Privacy Principles (APPs), establish strict requirements and processes to safeguard the confidentiality of documents and personal data. These regulations must be taken into consideration throughout any digitisation program.

Some areas of the Australian Government are already seeing dividends from this new roadmap to digitisation.

iStock.com/ookawa

Many industries encounter the same challenges faced by public administrations — they have to digitise a mixture of traditional, physical and digital archives.

It is therefore essential to analyse how the documents within these archives are organised and managed, as well as the frequency with which they are consulted to determine the digitisation workflow to use and best document management platform to use.

In some cases, it is necessary to develop new software to work with legacy systems. Administrations must also consider how they want to digitise. Looking at outsourcing services, undertaking a complete transformation of systems and processes or staggered digitisation of records are all viable paths dependent on need.

DIGITISATION IN ACTION: BEST PRACTICES AND KEY STEPS

To digitise documents in a secure, compliant manner that optimises their usability, it is essential to start from the ground up, classifying documents by type, security and confidentiality level, as well as by frequency of use and safeguarding times.

At this essential first step — on which the rest of the digitisation workflow is based — it is essential to carry out a cleaning process. Documents that are no longer valid, or that must legally be destroyed after a certain period, should be identified and destroyed or removed from digital systems. This destruction process also makes it possible to optimise space and reduce costs for digitisation projects.

Once the identification phase is complete it is necessary to begin the actual digitisation. For hard-copy records this will include scanning, but existing digital documents may also need to be made searchable or use AI and machine learning to identify and extract data which can then be transferred to a database.

iStock.com/Galeanu Mihai

Digitisation can be carried out by Australian government agencies either on their own premises or externally at a secure, third-party site. Some third parties also offer on-site scanning at customer premises, and due to the large amount of sensitive documents government and public bodies have in their custody, many prefer this approach, as it saves time and ensures a secure chain of transfer end to end.

After the digitisation phase, digitised documents are stored in an appropriate system. This step should be adapted to the needs of the organisation, so that it can be done either on its own platform or on a third-party platform. A system suited for ongoing information management or archiving will give civil servants the ability to automatically apply document retention rules for data privacy compliance.

The final phase, automation, involves creating automatic process flows, often between different sets of data, for maximum efficiency. This enables employees to access information more quickly and easily, improving response times and agility in customer service.

TRANSFORMING PUBLIC SECTOR THOUGHT

Resistance to change is a common element in all public administration and has been a serious barrier to digitisation and digital transformation efforts. However, ‘change fatigue’ is also increasingly common.

This challenge can be addressed by highlighting the benefits of adopting new technologies, demonstrating the benefits of implementing this type of initiative and keeping programs as simple and goal focused as possible. Additionally, allowing civil servants to use flexible systems so that they can optimise their own workflows means they can see for themselves what digital transformation can do.

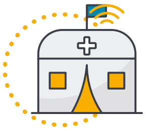
The end goal of digital transformation in the Australian public sector is to remove the obstacles that limit access to government services, speed up processes while maintaining or improving accuracy and improve the experience of citizens. Through the digitisation of legacy documents from health services, tax offices and social security departments, governments can guarantee the security and confidentiality of the records that shape the lives of their citizens and empower civil servants to optimise services.

The rise of the digital native calls for the creation of a digital world that works for all, and it is the role of technology providers to work closely with governments to make this a reality.

How Government Agencies Use LTE and 5G for Digital Transformation

Every government agency needs consistent and reliable access to a host of digital tools on a daily basis. Citizens are also demanding enhanced communication and services – which rely on great connectivity. Departments need the right network assets deployed today, that have the ability to scale to meet the requirements of the future. Cradlepoint's NetCloud Service and cellular-enabled routers and adapters unlock the power of 4G LTE and 5G to securely connect government workers no matter where their mission takes them.

SOLUTIONS Wireless Edge Routers and Adapters for Locations, Vehicles, and IoT

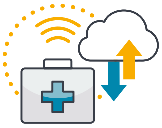


Pop-Up Networks

LTE and 5G allow government employees to quickly deploy wireless connectivity for operations including emergency services, food and safety inspections, and aircraft maintenance. Staff can easily set up connectivity in the field without reliance on another organisation's network.

Reliable networks for connected vehicles

Secure, nonstop LTE and 5G for connected government vehicles and the people and equipment inside them. Cradlepoint NetCloud Service, delivered through wireless edge routers, unlocks the power of mobile broadband — making it possible for field-based emergency services organisations and other agencies to connect vehicles and on-board IoT to critical applications and the cloud, everywhere they go.



Disaster Response Kits

Disaster response kits serve as a highly portable tool for setting up a dependable and secure network to ensure critical work can begin immediately. Hardened kits featuring ruggedised LTE routers can be used in a range of harsh environments as an integral part of emergency response.

Smart Bases

Today's military bases use IoT technologies including surveillance cameras, security equipment, and drones. Using a cellular router to connect each IoT device and/or application enables IT teams to deploy these technologies anywhere quickly, and on wireless connections that are separate from other parts of the on-site network architecture.

Mobile Command Centres

When responding to an incident, agencies need flexibility to take their operations into the field. Mounting a ruggedised, cellular- and Wi-Fi-enabled router in a mobile command centre provides the 24x7 connectivity that field agents need to work and communicate efficiently "on the move."

Smart Cities

There are many ways wireless technology can make cities run smarter, faster, and cheaper. Benefits of wireless cellular connectivity include day one connectivity and remote management, while use cases can include sensors and surveillance, and in vehicle connectivity.

Learn more at **cradlepoint.com**

Phone: (02) 8916 6334

NATHAN MCGREGOR

SENIOR VICE PRESIDENT ASIA PACIFIC, CRADLEPOINT

LEADERS
IN TECHNOLOGY
2024

IS ON-PREMISE OFFICIALLY DEAD? WHERE IS CLOUD HEADED IN THE YEAR AHEAD AND WHAT ARE THE IMPLICATIONS FOR GOVERNMENT?

While not a new concept, distributed organisations continue to grow in number with no sign of slowing down. Globalisation, changing working environments, a general acceptance of working 'on-the-go' as the primary way to work across many industries, and the evolution of consumer demands, has meant that hybrid hosting and cloud computing is increasingly the norm. We're also seeing increasing utilisation of cellular connectivity across organisations.

The emergence of 5G as a primary WAN technology and the growth of cloud computing creates new opportunities for organisations and governments but also brings a larger threat vector. Government departments will need to implement tight security controls, like Zero Trust Network Access technology that prevents lateral movements, limits user access to 'just enough', verifies before trusting, and never stops monitoring.

MACHINE LEARNING, AI AND AUTOMATION GRABBED ALL THE HEADLINES LAST YEAR — WHAT SEPARATES THE HYPE FROM REALITY IN TERMS OF USEFUL APPLICATION?

Mordor Intelligence[1] predicts the smart mining market will triple by 2025, when it's expected that 25% of mines will have adopted autonomous operations and half of all mines will connect their employees to improve safety and raise productivity. A main driver: the rising adoption of wireless monitoring and centralised solutions by large mining organisations. Wireless networks are the true backbone that connect the devices and enable data sharing.

AI will also become one with the network, impacting all organisational operations. We'll begin to see the benefits of AI being integrated into all applications related to the network, bolstering network predictability, troubleshooting, security and more. Organisations will need to ensure AI transparency and security practices are adequate in order to make the most of it.

PRIVACY, DATA SECURITY AND THE EXCEPTIONAL CUSTOMER EXPERIENCE... CAN THEY COEXIST?

According to Techmonitor[2], there was a 98% spike in cyber attacks on IoT devices within the last quarter of 2022. To defend against the growing number of bad actors within the growing 5G landscape, Gartner's SASE framework is an attractive option. While many of its principles are for protecting users, the zero-trust network access principle in SASE also provides a great foundation where the network plays a major role in protecting IoT devices. Using cloud-based management allows an easier approach to network configuration, identifying resources and setting up access policies for each device. This is especially important on networks with both IoT devices and users.

IN AN IDEAL WORLD, WHAT WOULD GOVERNMENT, INNOVATORS AND THE TECH INDUSTRY SUCCESSFULLY DELIVER IN 2024?

In countries like Singapore, the main international airport (Changi) is a hub of automation, making the travelling experience for passengers more efficient. Applications like digital facial recognition for passport control, digital queue management with check-in booking, seamless digital parking voucher redemption programs, and IoT-based intelligent mapping out to the cleaning team to prioritise areas for cleaning based on real-time flight data and passenger traffic, are the norm. Given our culture of innovation and available 5G telecommunications infrastructure, it would be great to see parts of Australian industry take a similar approach to digitalisation.

[1] Mordor Intelligence 2023, *Smart Mining Market Size & Share Analysis - Growth Trends & Forecasts (2023 - 2028)*, https://www.mordorintelligence.com/industry-reports/smart-mining-market

[2] Morrison R 202 *Hackers increasingly targeting Internet of Things devices*, Techmonitor, https://techmonitor.ai/technology/cybersecurity/hackers-targeting-internet-of-things-devices

Nathan has over 20 years of leadership experience in the telecommunications and IT industry working for prominent companies. He has successfully led technology businesses across APAC delivering networking, IoT, and analytics solutions across all industries. Nathan joined Cradlepoint in 2021 from Cisco Meraki, where he spent more than two years as Australia and New Zealand Country Manager.

2023 State of Threat Detection
The Defenders' Dilemma
83%

CHRIS FISHER

DIRECTOR OF SECURITY ENGINEERING, VECTRA AI

LEADERS IN TECHNOLOGY 2024

AFTER YEARS OF EXTENSIVE DISRUPTION, WILL 2024 SEE THE DUST SETTLE OR CAN WE EXPECT THE SAME RATE OF CHANGE?

No, the dust won't settle, particularly when looking at cybersecurity vulnerabilities. In 2023 the biggest change was that attackers moved away from traditional endpoint style attacks to focus on network infrastructure. There have been huge — almost weekly — occurrences of security vendors experiencing significant vulnerabilities that have allowed attackers to access organisations.

As we move into 2024, this will continue. We recently saw a level ten vulnerability released by Cisco, and we don't see this type of level of vulnerability very often anymore. It indicates that attackers see networks as a soft target, and they will continue to exploit this as organisations struggle to stop lateral movement. Once attackers get a foothold, they can do very significant damage and move in a way that they're not being seen.

DESPITE INDUSTRY-WIDE LAYOFFS, SPECIFIC TECH SKILLS ARE STILL HIGH IN DEMAND AFTER MANY YEARS. HOW CAN THIS BE EFFECTIVELY ADDRESSED IN 2024?

Right now, we're not getting many people coming through from university pathways. Not to mention that we often hear comments that security analysts are under a great amount of pressure and experience huge alert fatigue.

What's promising as we look to 2024 is we should see more generative AI toolsets being adopted and this will continue to grow. Already it's proving how the technology can be used to alleviate a lot of those pressures facing security teams. The best-case scenario is that we strike a balance of having human analysts supported by AI. I believe this will attract more people to the sector because they're far better supported and there are more career opportunities.

MACHINE LEARNING, AI AND AUTOMATION HAVE GRABBED THE HEADLINES — WHAT SEPARATES THE HYPE FROM REALITY IN TERMS OF USEFUL APPLICATION?

First and foremost, we must understand what we mean when we say AI. Generative AI is what's making headlines but it's only one small aspect of the technology. While GenAI can be utilised in a security context, it's applied and adaptive AI that will drive true change.

To consider what security teams desperately need, it's to sift signals of attack from a multitude of data, and then respond quickly and effectively. Applied and adaptive AI can help us to find the needle in the haystack, to then stop the breach and remediate impact of the attack.

When utilised correctly, AI can help SOC teams to battle the 'spiral of more', that is, more attack surfaces, more methods used by attackers and more complexity of hybrid attacks.

PRIVACY, DATA SECURITY AND THE EXCEPTIONAL CUSTOMER EXPERIENCE, CAN THEY COEXIST?

I think privacy, data security and customer experience can coexist. The challenge is understanding where the data is and how it's being used. We hear all the time that security ruins customer experience, but we simply must look at the critical flow of data and utilise the likes of cloud to enable better customer experiences.

Traditionally, security teams may put in network devices that sit in line so they can inspect and run checks that ultimately slow down the experience. When we use cloud, we can still gather information, while still building the policies and controls to ensure we're protecting the privacy of the individual, and streamline user experience. As security teams catch up with how cloud technology works, customer experience will inevitably improve.

Chris Fisher is the Director of Security Engineering for Vectra AI in the Asia Pacific and Japan markets. Fisher ensures that Vectra's customers have the security foundation to embrace new technology and lines of business, allowing them to digitally transform whilst reducing business risk and improving their security posture.

See where unified security can take you.

93% of organizations that moved to a unified platform saw a decrease in compatibility issues across their security system. This is why our Security Center platform excels. It delivers a cohesive operating picture through modules that were built as one system. So, whether you're securing an airport, a parking structure, a multi-site enterprise, public transit, or an entire city, you can access all the information you need in one place. This is unification.

To learn about the benefits of unifying your security operations visit
genetec.com

Genetec™

GEORGE MOAWAD

COUNTRY MANAGER, ANZ, GENETEC

LEADERS IN TECHNOLOGY 2024

AFTER YEARS OF EXTENSIVE DISRUPTION, WILL 2024 SEE THE DUST SETTLE OR CAN WE EXPECT THE SAME RATE OF CHANGE?

It was widely believed that supply chain constraints and HR challenges would improve after the pandemic disrupted the business climate. However, as of now, our latest State of Physical Security Report indicates that these problems have not yet been resolved in the physical security industry.

DESPITE INDUSTRY-WIDE LAYOFFS, SPECIFIC TECH SKILLS ARE STILL IN HIGH DEMAND AFTER MANY YEARS. HOW CAN THIS BE EFFECTIVELY ADDRESSED IN 2024?

One of the things we are most proud of at Genetec is that we have not engaged in the industry-wide layoffs affecting much of the technology sector. Our growth and commitment remain strong. We've bucked the trend and significantly bolstered our Australian team from five to twenty-four team members in the past two years. We plan to hire an additional five people in the remainder of 2023 and are excited to continue our investment in Australia, expanding the team further in 2024 and beyond. Genetec is committed to investing into its workforce, platform and customers in Australia.

And, unlike many other international businesses, we are not solely hiring salespeople in the region. For each salesperson, we hire two engineers — for pre and post sales — to support customers through their entire journey with us.

MACHINE LEARNING, AI AND AUTOMATION GRABBED THE HEADLINES LAST YEAR — WHAT SEPARATES THE HYPE FROM REALITY IN TERMS OF USEFUL APPLICATION?

Since the public unveiling of ChatGPT, AI has been the biggest news in the technology industry. But we see it as a buzzword and not the reality of what is happening in the public and private sector. Our focus is on intelligent automation and machine learning as tools to accelerate processes and enhance efficiency gains.

Genetec doesn't believe people will be replaced with AI. There are too many important decisions and nuances to manage that algorithms simply can't handle. These technologies can only replicate events and data they have seen before. They are not capable of original thinking, problem solving or creativity. The world still needs humans in charge and accountable for decision-making, especially in the public sector, and that remains as important as ever.

Our focus is on delivering tangible benefits that enable government departments and agencies to deliver better services to the communities they serve more efficiently. Not what science fiction shows tell us might be possible.

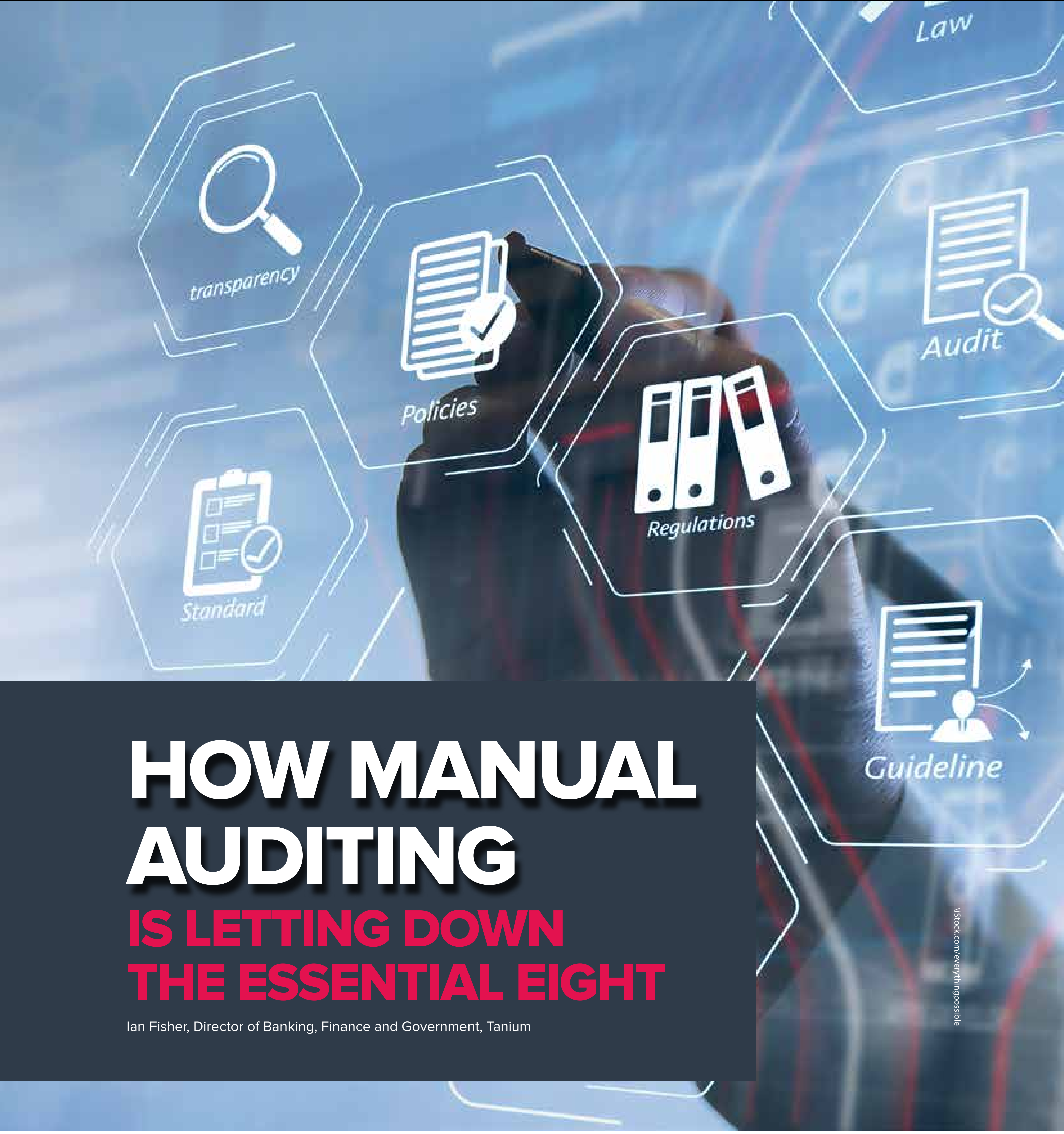
PRIVACY, DATA SECURITY AND THE EXCEPTIONAL CUSTOMER EXPERIENCE… CAN THEY COEXIST?

For a long time, people were told that ensuring privacy and security would come at the cost of a positive user experience. At Genetec, we don't believe that is true. Privacy and security are at the top of mind when we design and improve our products and services. We firmly believe that great security and privacy should not come at the cost of the user experience.

The challenge we face today is that the threat environment is dynamic. What protects us today may not protect us tomorrow. Defeating malicious actors depends on transparency and clear communication from vendors, the public sector and private organisations who share threat intelligence, newly discovered vulnerabilities and exploits. There is no silver bullet to counter cybersecurity and physical security threats. It requires a team effort.

Government departments and agencies are in a unique position. By taking the lead in using new technologies, sharing information and educating the private sector, they can be a beacon that shines a light on what technology can do to help us become safer and more effective.

As Country Manager for Oceania at Genetec, George leads a team of professionals delivering cutting-edge network-based security solutions for private, public, corporate and commercial clients. With over 27 years of experience in the electronic physical security industry, George has a deep understanding of the challenges and opportunities in this dynamic field.



HOW MANUAL AUDITING IS LETTING DOWN THE ESSENTIAL EIGHT

Ian Fisher, Director of Banking, Finance and Government, Tanium

iStock.com/everythingpossible

While the Essential Eight has been welcomed by the public and private sector as a strong, world-leading initiative to build Australia's cyber resilience, its implementation has been anything but easy. Now mandated for federal government agencies under Policy 10, in 2022–23 the ANAO found maturity levels for most entities were still significantly below the policy's requirements.

In both the public and private sectors, CIOs and CISOs face significant challenges in achieving and maintaining Essential 8 compliance levels. It's important to note that an accurate, comprehensive auditing process is still not a regulatory requirement, meaning gaps are being left. And while it's one thing to implement policies and procedures, without an effective auditing process, the mandate becomes nothing but lip service.

Much of the challenge with implementing the Essential Eight is due to a lack of confidence in identifying true compliance levels in real time across all endpoints, which is hard when up to 20% of endpoints are unknown in 94% of organisations, according to Tanium research.

To identify gaps, most organisations manually sample only a small amount of endpoints to gather a point-in-time view. The audit may spit out a compliance score, but that doesn't necessarily provide an accurate indication of success against the Essential Eight. Given the manual process, it's also highly open to individual interpretation.

Without precise, up-to-date insights, auditing becomes a box-ticking exercise with no way to remediate issues in a timely manner. This leaves organisations open to non-compliance and lowers their defence levels. So, what are the limitations of manual auditing and how can organisations overcome them?

FLYING BLIND ON COMPLIANCE

The first limitation of manual auditing is that it often involves taking manually collated snapshots from disparate sources of information collected from across an organisation's thousands of endpoints. Stitching together that many data sets is an arduous task, meaning by the time it's collected, analysed and acted on, it's already out of date, hindering the security team's ability to effectively manage and secure its IT infrastructure.

The second issue with manual auditing is that it only takes a sample of devices from across an organisation. Results are then extrapolated to create a score that is not representative of the entire environment and provides no real understanding of where the actual risk lies. Let's consider a large bank with 50,000 employees and over 80,000 endpoints. Manually testing each endpoint is near impossible, so they might choose to test a 10% sample. However, this means there is no way of guaranteeing compliance across 72,000 endpoints. Naturally, implementations of policies and procedures will likely differ from one part of the organisation to the other. Therefore, sampling one device in one part of the business should not provide peace of mind that the same level of security has been applied across every function and/or device.

Leaving security to chance based on statistical maths rules and the balance of probability is completely inadequate in today's modern threat landscape.

TAKING THE GUESSWORK OUT OF AUDITS

The way around the challenges posed by traditional auditing systems is through real-time continuous auditing. By creating visibility across all endpoints, organisations can establish always-on compliance monitoring with no blind spots. Comprehensive views of device inventories and compliance levels mean any gaps in the implementation of the Essential Eight can be picked up and remediated immediately rather than staying undetected for weeks or months.

> *Leaving security to chance based on statistical maths rules and the balance of probability is completely inadequate in today's modern threat landscape.*

This approach completely removes the need to undertake manual periodic audits that rely on outdated qualitative data. Instead, it provides a unified view that gives certainty and peace of mind around compliance instantaneously, empowering organisations to make more informed security decisions. Taking a proactive approach to compliance will also reduce liability for leadership teams and board members as well as significantly reduce the costs associated with auditing consulting and labour.

National benchmark or not, if auditing against the Essential Eight is not comprehensive or accurate, then the risk is still present. Having real-time visibility into all endpoints is the only way organisations can ensure they're maintaining the Essential Eight strategies. With continuous auditing capabilities, organisations can save significant internal resources while streamlining risk mitigation and remediation. When it comes to cybersecurity, there's too much on the line to leave compliance to chance.

Areas
35%
Furniture

10:48

JASON MACBRIDE

REGIONAL DIRECTOR FOR AUSTRALIA AND NEW ZEALAND, NEAT

LEADERS
IN TECHNOLOGY
2024

AFTER YEARS OF EXTENSIVE DISRUPTION, WILL 2024 SEE THE DUST SETTLE OR CAN WE EXPECT THE SAME RATE OF CHANGE?

The dust shows no sign of settling anytime soon.

As we know, the last few years have led organisations the world over to adapt and re-adapt to rapid change. Optimising hybrid work with certain technologies and processes has been a big focus and shows no signs of slowing down.

Organisations are actively planning for their next-generation workforce and how to bring people together both physically and virtually in a way that is seamless. Now, it's about creating meeting equity for all: ensuring everyone can be seen and heard, regardless of their location.

We're seeing huge growth driven by customers looking beyond traditional videoconferencing solutions for tools that are aligned to their hybrid workforces. Within a healthcare setting this might include mobile video carts that can move with the patient. Within a council department this may include video booths to improve citizen communication.

IS ON-PREMISE OFFICIALLY DEAD? WHERE IS CLOUD HEADED IN THE YEAR AHEAD AND WHAT ARE THE IMPLICATIONS FOR GOVERNMENT?

Many government organisations still have some on-premises infrastructure that is not easy to lift and shift. While change management can be overwhelming, to put it bluntly, cloud is more capable than on-premise and those making the transition are reaping benefits.

The ability to leverage the cloud for enhanced productivity, functionality and ease of use is paramount. As such, we offer in-built cloud management and monitoring capabilities, and we see this as reflective of the broader cloud trend.

Looking forward, we anticipate that cloud will enable other capabilities, such as artificial intelligence and machine learning, with an emphasis on equity and accessibility. Ideal for those who are hard of hearing or have visual impairments, for example.

MACHINE LEARNING, AI AND AUTOMATION HAVE GRABBED THE HEADLINES — WHAT SEPARATES THE HYPE FROM REALITY IN TERMS OF USEFUL APPLICATION?

Artificial intelligence and machine learning can improve experiences and amplify what organisations can do. This shouldn't be scary: used in the right way, this technology can help us make informed decisions faster. It also allows for moving away from repetitive tasks to those that are deemed higher value.

Across the board everyone is curious about what these technologies can do. Some are moving with caution, and others jumping right in. The biggest impact so far is on small problems. If you can take a small problem, but it touches many individuals, and utilise smart technology to remove the problem, the output of that is substantial, improving many lives.

In the context of video collaboration, AI is helping us and our partners such as Zoom and Microsoft to automate mundane tasks like transcribing.

PRIVACY, DATA SECURITY AND THE EXCEPTIONAL CUSTOMER EXPERIENCE — CAN THEY COEXIST?

They can absolutely coexist.

Some of the most secure government locations on the planet are using technologies that are connected to cloud-based platforms, and these devices are delivering some of the most critical important meetings in the world at any given time.

For instance, Neat devices are being used by the President of the United States and the staff in the White House. To reach this level of security clearance, we've had to invest in R&D efforts to ensure we're delivering products that are not only capable but extremely secure.

Jason MacBride, Neat's Regional Director for Australia and New Zealand, leads the expansion of Neat in the region, ensuring that clients and partners maximise the benefits of their Zoom Rooms and Microsoft Teams Rooms. With over two decades of experience, he is a seasoned solutions specialist with expertise spanning multiple industries.

SPONSORED CONTENT

Taking the next steps on NTN and Satellite 5G

Reiner Stuhlfauth*

Non-terrestrial networks utilising 5G technology will soon complement terrestrial 5G systems and provide connectivity in underserved regions.

The era of commercial communications satellites began on 6 April 1965 with the launch of Intelsat 1, also known as 'Early Bird', into geostationary orbit (GEO). While geostationary communications satellites are ideal for providing television, radio and data broadcasting over large areas, their use for telephony services is limited due to the high latency of signals traveling over 36 000 km into space and back. Despite this obvious disadvantage, various operators have successfully offered voice and data services over GEO satellites.

In the 1990s, with the advent of terrestrial cellular communications systems, plans for global low latency telephony and data (internet) services via constellations of medium earth orbit (MEO) and low earth orbit (LEO) satellites emerged. However, early systems such as ICO, Iridium, Teledesic and Global Star failed commercially due to the extremely high costs of such mega constellations.

While many satellite operators seem to prefer ETSI/DVB satellite standards for the air interface, operators of emerging NewSpace satellite constellations and high-altitude platforms may consider using modulation and coding schemes that were developed in the context of 5G wireless communications systems.

With its Release 17, the 3GPP standardisation organisation supports 5G New Radio-based satellite access, described as non-terrestrial networks (NTN). With respect to the business-related applications, one may observe a convergence between the traditional wireless and aerospace ecosystems as both parties drive innovations further.

In 5G, non-terrestrial networks represent a plethora of connection scenarios, from satellite-based communications via airborne stations, considering connection scenarios like air-to-ground (ATG) or unmanned aerial

vehicles (UAV) flight control. The holistic contemplation includes various satellite-based connectivity scenarios where the satellites differ in flying altitude, for instance GEO, MEO and LEO, and coverage area. There is also a distinction in the UE type, for instance whether it is a handheld device or a very small aperture terminal (VSAT) UE with better receiver capabilities, for example directional antennas or higher transmit power.

ATG communications provide in-flight connectivity for aircraft. Lastly, the context of NTN also considers the flight control of unmanned aerial vehicles (UAV) or unmanned aerial systems (UAS) in general.

Our understanding of 5G NTN is that it represents a technology evolution. While 3GPP Release 17 can be considered as the inception of NTN and the technology enabler in 5G systems, later releases will incorporate several enhancements and extensions, for instance the incorporation of airborne stations, so-called high-altitude platform systems (HAPS) and more onboard processing within the nodes. On the path to 6G we identify NTN as an essential part of such unified or organic networks, that will include airborne and spaceborne stations from its inception, allowing node appearance and disappearance as well as movement of network nodes relative to each other. Future network nodes will possess much higher onboard processing power, and concepts like multi-access edge computing will be incorporated in such intelligent nodes, trailblazing the path to beyond cellular.

To incorporate NTN, 3GPP launched a Release 15 study [TR 38.811] on channel models and deployment scenarios. After completing this study, 3GPP continued with a follow-up Release 16 study [TR 38.821] on solutions for adapting 5G NR to support NTN. The main objective of this study was to identify a feature set that enables NTN within the 5G system while minimising the impact on the existing 5G system.

As the major motivation to foster NTN communications we identify the request to provide ubiquitous connections all over the globe. According to several market statistics by industrial organisations such as GSMA, in 2020 wireless communications technologies covered more than 80% of the world's population, but less than 40% of the world's landmass. NTN satellite-based communications may tackle this aspect and focus on worldwide ubiquitous coverage in maritime, remote and polar areas.

Given RF challenges, satellite constellations and spectral circumstances such as frequency ranges or available bandwidth, we assume the first 5G NTN deployments will focus on ubiquitous connectivity and coverage. With respect to the expected data rates, NTN 5G cannot compete with terrestrial 5G, so our primary understanding is that 5G NTN will complement terrestrial 5G systems and provide connectivity in underserved regions.

**Reiner Stuhlfauth is Technology Manager (Wireless) at Rohde & Schwarz GmbH and has more than 20 years' experience in teaching and promoting mobile communication technologies. He is involved in several projects concerning 5G, 5G advanced and 6G research.*

ROHDE&SCHWARZ
Make ideas real

Rohde & Schwarz (Australia) Pty Ltd
www.rohde-schwarz.com.au

SMART CITIES NEED EVEN SMARTER SECURITY

Matt Caffrey, Senior Solutions Architect at Barracuda Networks

The smart city movement in Australia has been gathering momentum for at least a decade and many people living in Australia's largest cities already benefit from this. Parramatta, in Sydney, developed its first smart city masterplan in 2015. In 2016 the Turnbull government set out a federal Smart Cities Plan, promising to embrace disruptive new technology and real-time, open data-driven solutions across the country.

Smart city technology is leveraging sensors, cameras and data to — among other things — improve transportation, energy use, public safety, health care and waste management. A prime example is the provision of real-time bus and train information to commuters on their smartphones.

However, any system that relies on connected digital technologies and devices to function is also susceptible to cyber attack. The risks are particularly high for critical services such as health care and traffic management. The protection of connected systems and the data they store and share is imperative.

SECURITY CHALLENGES

Earlier this year the Australian Cyber Security Centre in collaboration with similar bodies in the US, UK, Canada and New Zealand issued a guide: Cybersecurity Best Practices for Smart Cities.

It identifies multiple cyber risks that the widespread adoption of smart city technologies can introduce. For example, smart cities depend heavily on operational technology (OT), such as sensors, for monitoring the physical environment and remotely controlling devices in facilities. The sheer volume and distribution of these devices, combined with the fact they are now all connected to the internet, increases the attack surface and heightens the potential spread and impact of successful attacks.

For example, in 2021 a hacker remotely gained access to sensors controlling the water supply to the city of Oldsmar in Florida and attempted to poison citizens by increasing the quantity of sodium hydroxide in the water.

Smart city technology can also create opportunities for threat actors to exploit a vulnerability — often in a low-cost and insecure device — to gain initial access, and then move laterally across networks to disrupt operations in other more important areas.

In one such incident, hackers gained access to the core systems of a US casino by hacking a smart thermometer being used to monitor the temperature in their aquarium.

To add to the problem, much of the technology used across smart cities is from different vendors and is owned and operated by different companies. This may hinder effective visibility, collaboration and communication, which is necessary for ensuring robust security.

Any compromise of smart city systems carries potentially severe consequences, including substantial disruption to city operations, financial losses, potential breaches of personal data and, in the worst-case scenario, significant damage to infrastructure and the risk of injury or loss of life.

Other security challenges facing smart cities include data protection and privacy breaches, particularly if data and applications are stored in the cloud.

BEST PRACTICES FOR SECURING SMART CITIES

Effective security in a smart city requires a holistic approach, regardless of the

iStock.com/Jackie Niam

Effective security in a smart city requires a holistic approach, regardless of the individual security level of a product or solution.

individual security level of a product or solution. National, regional and local authorities need to prioritise the careful and secure integration of new technologies into the existing infrastructure, employing secure connectivity measures.

While there are specific security challenges unique to smart cities, governments should first adhere to widely accepted standard approaches such as the Essential Eight, outlined in the ACSC's Strategies to Mitigate Cyber Security Incidents.

For example, across all systems, user access should adhere to the principle of least privilege. This principle dictates that users should only be given access to the resources/networks that are vital to perform their jobs. The implementation of a zero trust approach, such as Zero Trust Network Access (ZTNA), including multifactor authentication, is well suited to this — and agile enough to adapt quickly to changing security scenarios, such as an active attack.

It is also essential that those responsible for the devices and applications that are being implemented in smart city systems understand the environment into which they will be deployed. For example, the security posture of devices they will be installed on or connected to, and how they will integrate with existing systems or applications. They must also be alert for any new points of weakness that emerge following the implementation and ensure appropriate security controls are applied.

A typical smart city has an ever-expanding attack surface, using thousands of different devices from many different vendors. Software vulnerabilities are likely to be discovered on a regular basis and these will need patching. This is a formidable but essential task to uphold smart city security.

The Cybersecurity Best Practices for Smart Cities guide also contains recommendations covering secure planning and design, proactive supply chain risk management and operational resilience for communities and organisations looking to implement smart city technologies.

Lastly, in the event of system failure stemming from an attack or malfunction, it's crucial to have a well-prepared response plan at the ready. This involves comprehensive contingency planning to ensure the most critical aspects of a city's functioning, such as transport networks, can remain operational in the face of disruption.

THE TAKEAWAY

More and more cities are embracing smart technologies, and those already leading the way are expanding their portfolio of technologies, fostering innovation and continually enhancing existing offerings to enhance overall 'smartness'. Therefore, it is paramount that national, regional and local governments build strong security policies into the planning process for any new services or improvements to existing ones.

Simultaneously, every partner organisation deploying or managing smart city technology should maintain a constant state of vigilance and stay abreast of the evolving threat landscape to assess how each new threat could impact their smart city systems.

TeamViewer

Centralised remote connectivity for state & local government

The remote connectivity solution built for scale, productivity and security. Learn how centralised remote IT connectivity helps you manage and maintain all of these critical services – without requiring additional staff or infrastructure.

www.teamviewer.com

ANDREW BELGER

HEAD OF SALES FOR AUSTRALIA AND NEW ZEALAND, TEAMVIEWER

LEADERS IN TECHNOLOGY 2024

AFTER YEARS OF EXTENSIVE DISRUPTION, WILL 2024 SEE THE DUST SETTLE OR CAN WE EXPECT THE SAME RATE OF CHANGE?

Innovation cycles have been getting shorter for decades. With the latest developments in artificial intelligence (AI), organisations will not experience a slowdown, but rather, a further increase in disruption.

Business-focused disruption tends to happen behind the scenes, irrespective of the hype. For example, the impact of AI has been significant in the business-to-business (B2B) and industrial sectors for several years. Recent improvements in its processing power means the ability of AI technology to analyse and visualise vast amounts of data and provide real-time insights has resulted in a plethora of use cases.

Furthermore, organisations will encounter another major disruption once quantum computing technology is available on a wider scale.

IS ON-PREMISES OFFICIALLY DEAD? WHERE IS CLOUD HEADED IN THE YEAR AHEAD, AND WHAT ARE THE IMPLICATIONS FOR GOVERNMENT?

There are a variety of needs for both cloud and on-premises environments, especially when considering critical infrastructure that must be maintained. Some organisations need to comply with the data residency regulations of countries such as Australia and regions including the European Union that mandate that data isn't stored in a distant cloud.

Government organisations must ensure data is stored and processed in a controlled environment while leveraging the latest technology to maintain maximum security and efficiency. This presents a challenging balance for IT departments; however, solutions are available, including for specialised use cases. For example, an on-premises server protected by conditional access can facilitate secure external collaboration while all data is hosted and processed in an on-premises environment.

MACHINE LEARNING, AI AND AUTOMATION GRABBED ALL THE HEADLINES LAST YEAR — WHAT SEPARATES THE HYPE FROM REALITY IN TERMS OF USEFUL APPLICATION?

The potential applications of AI have been most associated with the rapid rise of generative AI (GenAI) since several companies made their tools publicly available. However, the most significant impact of AI lies in data analytics and workflow automation, including process automation and accessing real-time analytics.

For business applications based on AI that conduct data analytics, the primary challenge faced by business leaders is ensuring the quality and quantity of data. As a tool is trained based on the data it receives, every digital interaction can be used to improve organisational processes and ultimately drive automation. It is essential for users to investigate and distinguish between useful data and useless data for this to succeed.

IN AN IDEAL WORLD, WHAT WOULD GOVERNMENT, INNOVATORS AND THE TECH INDUSTRY SUCCESSFULLY DELIVER IN 2024?

The technology industry is currently focused on the compliant, accessible and inclusive use of AI; however, innovators face challenges that must be addressed including the reliability and trustworthiness of AI.

Once AI-integrated solutions are reliable and in strict compliance with regulations, the industry may see an increase in the level of trust afforded to this technology. Regulators and innovators must work together to create an inclusive AI environment and dispel the fear of the dystopian Skynet narrative.

Andrew Belger is the head of sales for Australia and New Zealand at TeamViewer. He manages enterprise and channel sales, including business development and strategic partnerships. Andrew has more than 20 years' experience in the technology sector and has previously held various sales leadership roles at specialised technology companies.

NATIONAL ID SCHEME: IT'S TIME TO ASK THE HARD QUESTIONS

Albert van Wyk, Regional Director, Australia & New Zealand, GBG

Digital identity is in its infancy in Australia. While we have seen great strides recently in collaboration between federal and state ministers announcing the National Strategy for Identity Resilience, collaboration is the first step towards building an effective solution that will be trustworthy and fit-for-purpose for all Australians.

In a remarkable first step, all Australian governments have agreed to adopt 10 shared principles that will guide their approach to identity. This will be underpinned by biometrically anchored digital identity credentials for all Australians.

However, getting governments to collaborate is only the first hurdle in building a successful national identity scheme. While the government has promised a consultation process with industry later this year, now is the time to ask the hard questions before going down the path of a single identifier of Australians' identities.

We need to draw upon lessons learned from other nations and consider a scheme that allows citizens to present themselves in the most convenient manner. This needs to be supported by a system that can ingest wide sources of data and verify at speed with the least amount of friction.

IT'S A TRUST THING

A key challenge for the Australian Government is overcoming citizens' lack of trust in implementing a national identifier and their ability to manage personal data. While the issue of citizen trust is not necessarily targeted at the current government (as it has developed over time), it should be a key factor to consider in the implementation of any scheme. Trust is only derived through understanding. A key shortcoming has been the lack of a simple explanation of how a national identity scheme would work in Australia that clearly outlines the benefits.

Without delivering these simple, transparent benefits and risks for the layperson, the scheme will continue to drive uncertainty, which leads to assumptions, and ultimately fear and mistrust.

WHAT DOES A 'NEXT STEP' LOOK LIKE?

It all starts with consumer-focused consideration, which uses simplistic language that makes it transparent for the layperson what the scheme does, how it will operate, what is connected and the benefits for them to participate

iStock.com/Iaremenko

— assuming there is an option.

In my view, a national digital identity scheme should aim to drive greater access to services for its citizens, and better connections between government and business, with the ability to connect faster and with less friction.

Any such scheme should remove barriers to accessing valuable services such as health, medical and financial services as well as a variety of different government schemes and initiatives.

It's important that such a scheme does not create a further barrier for anyone vulnerable due to being disconnected from technology, which would create further disenfranchisement and a potential new set of challenges.

From a business perspective, the scheme should aim to drive greater efficiencies and deeper understanding of customers. Greater understanding should improve communications, offers, and products or services.

Failing to provide these benefits will result in a low rate of adoption and will risk making access to government services harder for citizens.

AVOIDING THE HONEYPOT RISK

The third challenge to implementing a successful scheme is overcoming the risk of cybersecurity and data breaches from collecting and storing a honeypot of Australian citizens' identity data that would prove irresistible to cybercriminals.

Scams and identity fraud in Australia are becoming industrialised at a rapid rate. According to our Global State of Digital Identity 2023 report, more than nine in 10 (94%) Australians surveyed are concerned about fraud attempts in the future.

We also discovered that 56% of Australian consumers consider biometric information to be private data that is integral to their identity. Considering the scheme will incorporate biometric information along with other personal identifiers, it will require careful thought to mitigate Australians' fears around the risk of cybersecurity attacks and data breaches involving their identity.

Even if the trust and perception issues are addressed, creating a single source of truth that contains 24 million Australians' biometric and identity data will require a bulletproof technical solution in the current landscape of rising data breaches and increasingly sophisticated socially engineered scams.

This issue will require the government to engage with the technology and consulting ecosystem to execute an effective solution that is implemented with these risks front-of-mind.

BRINGING IT ALL TOGETHER

Sophisticated challenges require solutions that span three categories — technology, people and data. At a minimum, we cannot address the whole challenge without well structured and well understood solutions for all three of these areas.

The technology will underpin the solution to drive efficiency of the system and create service connections. There are great technology vendors that today already provide and deliver systems that can be leveraged to continue investing and maintaining the platforms needed to drive this part of the solution.

On the people side, Australia abounds with consultancy-led organisations, as well as cross-industry and cross-segment experts, that can advise and provide insight into how citizens access services, with policy drivers to ensure the system can gain the efficiencies today and solve tomorrow's challenges. These experts need to be brought into the consultation process to distil and drive consistency of a national approach.

The data piece requires advice on how to access repositories of data, rather than building a honeypot of data on Australian citizens. This means solving the challenge on a business scale to verify not just an individual's identity, but also collating and providing data on behaviours and fraud actors. It must also provide data regarding risk at any point in time during transactions, identities and personas.

A deep knowledge base is required to inform the government's approach, building a system that facilitates understanding of access and transactions that continuously inform and improve processes.

You can't achieve this state of nirvana by consulting on just one of these areas — technology, people or data. We need a holistic approach to address trust and understanding, and to deliver benefits for citizens, industry and government.

These are not easy challenges to solve. But if we continue to set a single pathway without addressing these real issues, we will face the same outcomes that other countries have and end up with another white elephant that does not deliver the service outcomes we set out to achieve.

‘WE AIM TO DELIVER A
WORLD-CLASS SERVICE
TO OUR CUSTOMERS’.
CHIEF INFORMATION OFFICER
SYDNEY WATER
BE YOUR PERSONAL BEST
SAP

RYAN VAN LEENT

VICE PRESIDENT, SAP GLOBAL PUBLIC SERVICES

LEADERS IN TECHNOLOGY 2024

AFTER YEARS OF EXTENSIVE DISRUPTION, WILL 2024 SEE THE DUST SETTLE OR CAN WE EXPECT THE SAME RATE OF CHANGE?

Disruption has become business-as-usual. In addition to the social, economic and environmental upheaval we've experienced in the first part of this decade, we're now in the midst of an AI technology disruption that Gartner's predicting will be as impactful as the steam engine, electricity and the internet.

ChatGPT caused such a stir because it demonstrated that the AI revolution — that had forever been 10 years away — is here today. Generative AI has already changed how content is produced, and very soon we'll start to see it changing how decisions are made, at which point it will fundamentally change how businesses and governments are run.

MACHINE LEARNING, AI AND AUTOMATION GRABBED ALL THE HEADLINES LAST YEAR — WHAT SEPARATES THE HYPE FROM REALITY IN TERMS OF USEFUL APPLICATION?

There's certainly a fear of getting left behind, which has motivated lots of frenetic experimentation. But governments have moved quickly to ensure that AI is being applied rationally and responsibly. Government regulations, like the DTA's interim guidance on GenAI, have helped cut through the hype to uncover solid use cases for AI in business.

The key to applying this new capability in a way that's useful is encapsulated in the 3-R's of Business AI. We need to make AI relevant by embedding it in the systems that users interact with every day; we need to ensure that AI outputs are reliable by grounding the models with appropriate business data and context; and we need to apply AI in a responsible way that's in keeping with societal expectations. It's a lot easier to stay grounded in reality when your AI scenarios are relevant, reliable and responsible.

PRIVACY, DATA SECURITY AND THE EXCEPTIONAL CUSTOMER EXPERIENCE… CAN THEY COEXIST?

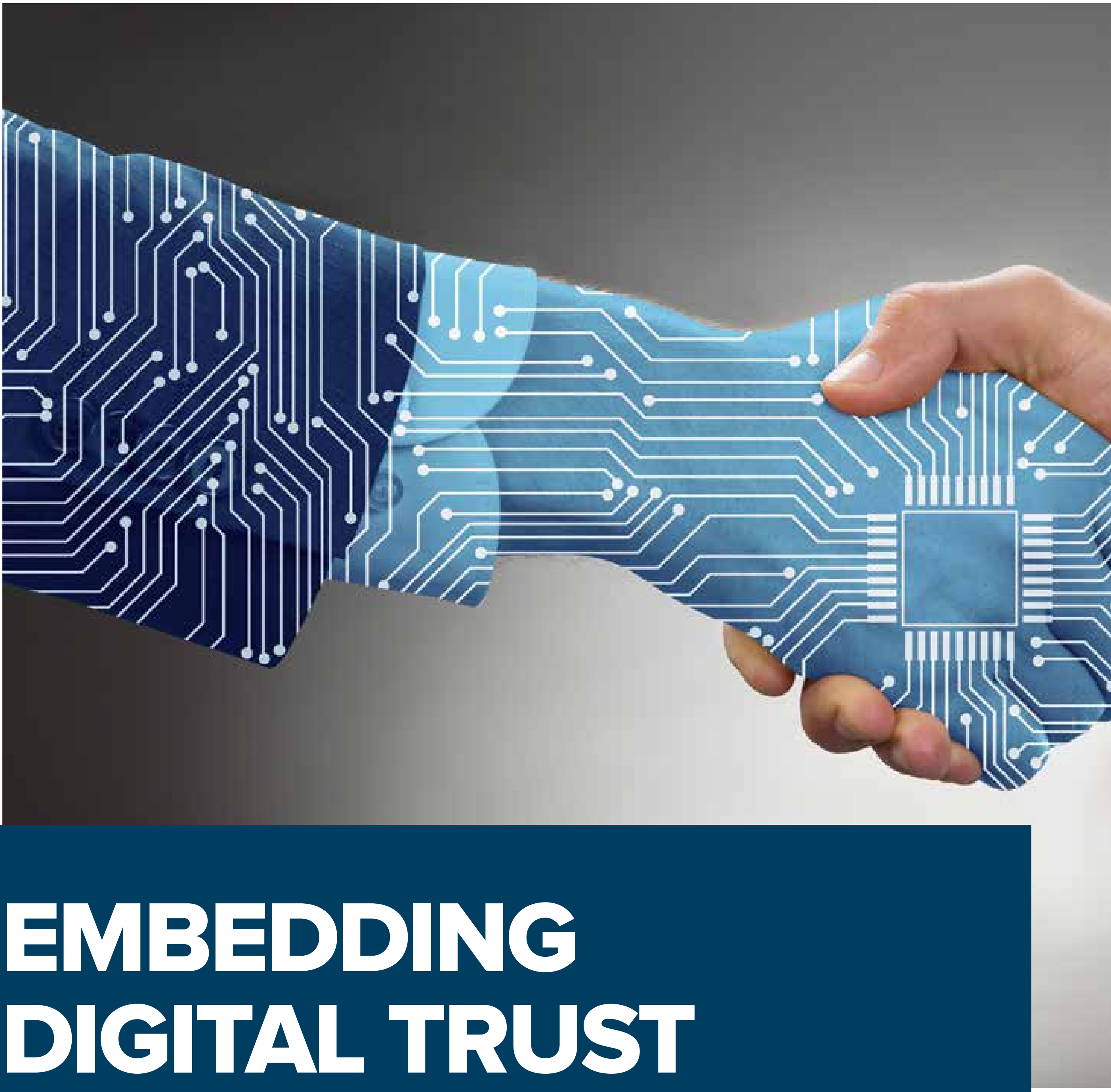
In a recent IDC survey, data protection was identified as the single most important consideration in government scenarios for GenAI. We need to be particularly mindful of this since there's an inherent risk that confidential data could be included in a user's prompt and inadvertently shared with a third party. But there are ways to mitigate this, so it doesn't necessarily mean that GenAI can't be used by governments to deliver a great customer experience. In fact, we're seeing some fantastic scenarios, incorporating GenAI to generate case summaries and communication proposals that improve the efficiency and effectiveness of customer interactions.

IN AN IDEAL WORLD, WHAT WOULD GOVERNMENT, INNOVATORS AND THE TECH INDUSTRY SUCCESSFULLY DELIVER IN 2024?

Although we're growing accustomed to entering prompts in natural language, I don't think we're yet interacting with AI naturally. In most cases AI is ancillary to core business systems and is often still confined to back-office analytics. To realise the potential of AI in the front office, it needs to be embedded as an integral part of core business processes.

We're making good progress with Business AI, and I think 2024 will be the year we start to see more natural human–machine collaboration.

Ryan van Leent is a member of SAP's global leadership team for public services. He is responsible for incubation of emerging and strategic solutions, and is currently focused on Generative AI. Ryan has deep subject matter expertise in social protection, and is passionate about helping governments to improve peoples' lives.



EMBEDDING DIGITAL TRUST

THROUGH A FOCUS ON PEOPLE, DATA AND SYSTEMS

Charlene Loo*, Managing Director of BSI Australia and New Zealand

iStock.com/AndreyPopov

ORGANISATIONS FOCUSED ON THE FUTURE WILL BE THOSE THAT HAVE THE CORRECT PROTOCOLS, POLICIES AND PROCEDURES IN PLACE TO KEEP THEIR INFORMATION SAFE, DATA SECURE AND INFRASTRUCTURE ROBUST.

As working practices continue to evolve, cloud-based and digitally reliant businesses are becoming the norm. But as digital processes adapt, the risks of cyber attacks, security breaches and human error also increase exponentially.

Given today's cyberthreat landscape, how do organisations reassure customers, stakeholders and wider society that they can be trusted and have procedures and controls in place to secure and protect data?

Switching to cloud services can have many benefits: enabling remote working, ensuring effective business continuity and faster disaster recovery. However, introducing new services may also open up risks to security, with large amounts of sensitive data being stored by multiple third parties, potentially held and accessed all around the world.

THE INDUSTRIALISATION OF CYBERCRIME

Consequently, we are beginning to see an industrialisation of cybercrime, with ransomware becoming a commodity service. Earlier this year, the Office of the Australian Information Commissioner (OAIC) reported a 26% increase in data breaches in the second half of 2022, including some of the largest in Australian history, affecting millions of Australians.

Such incidents come at a huge cost to organisations. Latitude Financial recently announced it was forecasting a first-half statutory loss of between $95 million and $105 million after a cyber attack "closed or severely restricted" its ability to earn income for five weeks.

The regrettable truth is that cybercrime has gone through the same rapid transformation we are seeing in our organisations in terms of the adoption of technology, with threats, risks and attacks growing in frequency and sophistication.

As most data breaches have human involvement, people can be the strongest asset in cyber-defence strategies, making it critical for leaders to bring people along with them to ensure organisations remain cyber resilient.

Major cyber attacks have the potential to outpace organisations' abilities to effectively prevent or respond to them. So, what can organisations do to better protect their assets? When it comes to securing data, the instinct can be to focus on building a 'wall'. But walls can be breached. Building cyber resilience is about going beyond constructing walls and employing a proficient and proactive approach to managing information as an asset. Organisations that embed digital trust and resilience through a focus on people, data and systems increase their potential to secure long-term benefits for their operations, customers and society.

CYBER RESILIENCE IS ABOUT THE CULTURE WITHIN AN ORGANISATION

Cyber resilience goes beyond technical controls and is largely about the culture within an organisation. Training, as well as openness and constant engagement with staff about the importance of cybersecurity, can help create a cyber-resilient culture and ultimately better protect the organisation. True digital trust can be built from the top down and bottom up through regular training and policy re-evaluations.

As most data breaches have human involvement, people can be the strongest asset in cyber-defence strategies, making it critical for leaders to bring people along with them to ensure organisations remain cyber resilient.

Ensuring these conversations are not just internal can offer the best chance of success. Maintaining the security of global supply chains is often very complex, with multiple third-party providers of cloud service platforms, technologies and information management systems to contend with. If organisations work closely with the supply chain and procurement managers across their networks, they will be well placed to protect themselves at every point.

EMBEDDING DIGITAL TRUST

By adopting a robust information security posture that embeds digital trust and complies with global best practice, organisations can strengthen information security posture, support an organisation's digitisation strategy, reduce the risks of information breaches and build digital trust in the brand.

Digital trust can be embedded into the organisation, particularly in building an overarching security framework — integrated throughout the whole organisation — and identifying processes, interactions, risk assessments and continuous improvement to ensure robust resilience.

FOCUSING ON THE FUTURE

Amid today's cyberthreat landscape and the emergence of new technologies, having the correct protocols, policies and procedures in place to keep information safe, data secure, infrastructure robust and ultimately, make them resilient, can be key to an organisation's future success.

When digital trust is at the heart of cybersecurity strategies, this can instil confidence that an organisation empowers its people, systems and technology to ensure safety, security, compliance, privacy and its ethical responsibilities are met.

As technology becomes ever more central to life, evolving digital transformation will not be something that we will be able to separate from how we do business, how we live or how society operates. Organisations focused on the future will be those that have the correct protocols, policies and procedures in place to keep their information safe, data secure and infrastructure robust. And ultimately, digital trust will enable organisations to accelerate progress to a digitally safe world.

**Charlene Loo became Managing Director of BSI Australia and New Zealand in April 2023. Her prime responsibility is to drive to grow the business through a culture of innovation and fostering strategic partnerships. Prior to this, she was Managing Director at BSI Singapore, where she collaborated with a government agency to launch a cyber-safe program resulting in Singapore being voted as the top campaigner for the program.*

iStock.com/ipopba

AI DRIVING HEALTHCARE TRANSFORMATION

Regional Vice President of Cloudera ANZ, Keir Garrett

In a world where data has become the lifeblood of innovation and progress, there is one realm where its significance shines brighter than ever — health care. Health data, when harnessed effectively, becomes a powerful ally in the pursuit of better patient outcomes. And it's not just about crunching numbers and creating charts — it's about translating vast volumes of information into meaningful insights that can bring hope to millions and even save lives.

Leveraging this data, acting on it, and yielding results requires organisations to have access to all their data, regardless of whether the data resides on the cloud or an on-premise data centre. Artificial intelligence (AI), generative AI (GenAI) and machine learning (ML) are crucial to a successful data-driven health program. These tools are being integrated into healthcare systems across Australia and New Zealand, and they are bringing about critical benefits for patients and healthcare providers alike.

AU AND NZ RECOGNISE NECESSITY OF DIGITISATION

The ability to leverage advanced, data-driven solutions using AI and the cloud will empower the healthcare workforce as challenges related to supporting an aging population and labour shortage loom in the near future.

As highlighted by Deloitte, Australia's population is estimated to reach 35.9 million by 2050, with the proportion of people aged over 65 increasing by 6% to reach just under a quarter (22%) of the population. At the same time, the workforce participation rate is expected to decline from 66% to 64%. According to the analysts, this combination has the potential to have a catalytic effect on the healthcare system and workers, unless something is done to support staff and facilities.

While initially hindered by restrictive budgets and legacy systems, the COVID-19 pandemic proved to ramp up the urgency of digitisation and kick-started several digital healthcare initiatives. Integrating technology solutions into urgent care centres and implementing virtual care programs showcased how digitisation enabled organisations to cater to pressing healthcare needs.

As a result, healthcare IT budgets have increased, with spending focused on enabling a flexible model of patient support — and just in time, with an aging population calling for greater medical care. As AI and hybrid cloud adoption continue to advance and more use cases become apparent, healthcare providers will be looking to invest.

AI-POWERED ALGORITHMS SPOT PROBLEMS, SAVE LIVES

Using AI-powered algorithms, doctors can now detect diseases earlier by analysing large volumes of patient data, from medical history to laboratory results and imaging scans. Accelerated by the cloud, this early diagnosis service allows healthcare professionals to intervene promptly and provide personalised treatment plans built using ML, leading to better patient outcomes and more lives saved.

iStock.com/Natali_Mis

AI FOR REMOTE AND INCLUSIVE CARE

For patients in remote or underserved areas, AI brings hope. Remote patient monitoring becomes a reality with wearable devices equipped with AI algorithms connected to the cloud using IoT technology. These smart devices track vital signs, detect anomalies and alert medical professionals in real time, ensuring timely interventions and reducing the risk of complications.

Medical imaging has undergone a revolution, all thanks to AI and the cloud. Advanced algorithms can now interpret X-rays, MRIs and CT scans with astonishing accuracy and speed, helping radiologists across Asia identify potential health risks more efficiently. ML models can also identify subtle patterns that may be difficult for human eyes to detect, leading to faster and more precise diagnoses, quicker treatments and improved patient care.

New Zealand recognised the potential of AI way back in 2018 when Dunedin company oDocs created the world's first AI medical system for Medicmind, which was designed for medical researchers and clinicians to create AI to auto-diagnose a large range of diseases based on a single photograph. Fast forward to October 2022 and The AI Forum NZ attested that AI technology will help to support the care of an aging population through faster, more effective diagnoses, as well as building trust and improved outcomes for patients and their communities.

With AI-based predictive analytics, healthcare providers can forecast patient outcomes based on historical data. Armed with this information, doctors can create more effective treatment plans tailored to each patient's unique needs, resulting in improved care and better recovery rates.

Cloud-based AI-powered virtual health assistants and chatbots have also become increasingly popular throughout the ANZ region. Recently released solutions can provide 24/7 support, answer common medical questions and even offer basic triage services on the cloud. This eases the burden on healthcare facilities and ensures patients have access to medical care whenever and wherever they need it.

For instance, Australian hospitals are trialling ChatGPT AI to help track performance metrics, such as how long high-risk patients need to wait before being screened. The Nepean Blue Mountains Local Health District (NBMHD), in collaboration with the Visual Telehealth Lab at the University of Sydney, is testing using AI to remotely monitor patients' vital signs during standard telehealth appointments, collating important data points to build a clearer picture of the symptoms.

THE RISE OF GenAI IN HEALTH CARE

GenAI offers invaluable assistance to healthcare professionals by enabling them to interpret a patient's data more effectively, including their medical history, imaging records, genomics or laboratory results. With a simple query on a large language model (LLM) much like ChatGPT, GenAI can rapidly deliver the data that clinicians need, even if it's stored in various formats and locations, helping healthcare providers quickly gain a better understanding of a patient's health. This also streamlines the decision-making process and empowers medical experts to provide more efficient and accurate care to their patients.

One of the most significant advances in GenAI is the technology's ability to produce synthetic data, including medical images. This synthetic data is invaluable as it enhances the training process by expanding the content and data used for research and medical training. By generating diverse and realistic data and images, GenAI also helps develop more effective ML models, benefiting research and healthcare training.

SECURITY AND PRIVACY OF HEALTHCARE DATA

Medical data is, like financial data, extremely precious to us all and must be secured at all costs. This means AI implementations must adhere to strict ethical standards to earn and maintain public trust. Unsurprisingly, a crucial aspect of ANZ's health care's technological advancement is data governance and security. Fortunately healthcare providers in the region are prioritising patient confidence through robust data governance strategies which meet ever-evolving security requirements imposed by regulating agencies, governments, industries and the general public.

Amid all the wonders of data-driven, intelligent health care, one constant remains — the human touch. Behind every data point and predictive model stand compassionate healthcare providers who embrace data not as a replacement for their intuition and empathy but as a complement to their healing instincts. Democratising the latest AI solutions is central to helping these heroes thrive.

iStock.com/GOCMEN

SOFTWARE SATISFACTION

— HOW CAN COUNCILS GET IT?

Michael Craig, Harbour Software

In the 1970s, when much of the business world was introducing computers to free up employees from tedious routine tasks so they could pursue more strategic work, Australian local councils were quietly joining the fledgling IT revolution.

Not that much has changed today, with streamlining processes in the aim of efficiency still very much the goal. Councils are implementing software suites that continually improve productivity by automating a range of tasks from collecting rates to offering self-service dog registrations.

The difference now is that all these time-saving applications are expected to seamlessly work with each other, through the use of application programming interfaces (APIs).

Any disruption to the applications that run most council services is keenly felt, by council staff, residents and ratepayers. IT managers are at the coalface when it comes to disgruntled stakeholders. They, in turn, rely on their software vendors to respond quickly and effectively when operations are disrupted. But what happens when the vendor's help desk doesn't work properly and your customer service level agreement (SLA) doesn't materialise? SLAs vary depending on the arrangement between vendor and council. Adherence can be patchy and many questions remain unanswered: How much downtime is acceptable? How long can an outstanding ticket be left without a resolution?

To help understand better, three seasoned local government IT leaders shared their experiences and collective wisdom. They not only provide insight into why they believe some councils choose to stick it out with poor performing software vendors, but also offer a simple solution to one of the most frustrating parts of an IT manager's job.

WHAT DOES GOOD CUSTOMER SERVICE LOOK LIKE?

We all experience customer service every day — whether receiving or providing it. It is an area that is studied and promoted as a foundational element in retaining customers, with business gurus pushing terms like "customer centric focus" as must-have organisational attributes. Despite this, our understanding of what good customer service looks like — and what drives it — seems to vary wildly.

IT managers also have differing ideas when it comes to customer service, especially when it comes to vendor help desks, which they rely on heavily to keep mission-critical software running 24/7. With no best practice framework or standard to determine what lays outside the realm of 'reasonable', local councils are often in a vulnerable position.

AJ Jack is IT and GIS Coordinator at Oberon Council. With over 30 years' experience in IT, including managing a help desk in a previous role, he understands the importance of keeping on top of tickets and ensuring resolve times are minimised.

"My frustration with a previous software solution we used was endless," he said.

"I'd log a call and nothing would happen. Then I'd complain to my account manager, but he couldn't help either. New help desk managers would come and go and nothing would change in the help desk queue. One job remained active for two and half years, so I gave it a Happy Birthday greeting in the comments section when it turned two — thinking a comment like that would get people moving — but still, nothing."

Jack said his experience is not unusual, with a peer from another LGA once telling him about a four-year-old outstanding ticket of his own.

"I don't understand why some councils tolerate substandard customer service such as the council with the four-year-old outstanding ticket," he said.

"And what's even stranger, that same council re-signed with that vendor. I'm only half joking when I say this, but could it be some type of Stockholm Syndrome is keeping them from moving on?"

SUNK COST FALLACY

The more likely reason is a condition known as "sunk cost fallacy", where individuals and organisations feel they've invested too much to quit, justifying further investment and ongoing commitment.

Garry X has been working in IT for 25 years — including 15 as an IT leader in

local government in Queensland — and has seen sunk cost fallacy in action.

"I've seen this scenario many a time. You invest in a project for, say, a million dollars. It starts to go pear-shaped but — because it will cost two million dollars to start again — the organisation takes the risk and invests an additional $500,000 the vendor says will fix the issue. The money doesn't help, the project is still pear-shaped and even more investment is required — and it keeps going on and on."

He believes other factors influence this outcome, including a lack of binding SLA targets, along with what Gartner has termed the "Gartner Hype Cycle", a methodology that provides an objective map of risks and opportunities associated with emerging technologies.

"Predictably, at the beginning everyone is looking at the bright side looking forward to all the benefits a new technology will bring, so binding SLAs

iStock.com/gorodenkoff

> *Any disruption to the applications that run most council services is keenly felt, by council staff, residents and ratepayers.*

are not at the top of the list," he said.

"Then you get to the top, where the technology is at its peak. According to the Gartner Hype Cycle — which I think is accurate — it then swoops down to the 'Trough of Disillusionment', where you begin to discover problems with the technology. At this point, if the product is not well supported, there will be little help at hand to fix the issues. In my experience, some councils literally hit rock bottom and stay there until they look for another technology," he said.

PROCUREMENT PROCESSES

Some state governments have attempted to introduce more rigour around large investments, creating LG procurement processes designed to avoid the pitfalls associated with unresponsive software vendors, and, if implemented properly, taking them out of the equation altogether.

One such initiative is the Victorian Government's Rural Councils Transformation Project (RCTP), which aims to improve council services for rural communities by providing a framework for groups of councils to share procurement processes and services. RCTP already has several projects underway ranging from a couple of councils to collaborations of up to four or five.

These RCTP implementations provide a high level of transparency into how and why a particular software application is selected by a group within a fit-for-purpose framework. When working through the procurement process, councils are able to openly discuss the merits of different software solutions, including customer service.

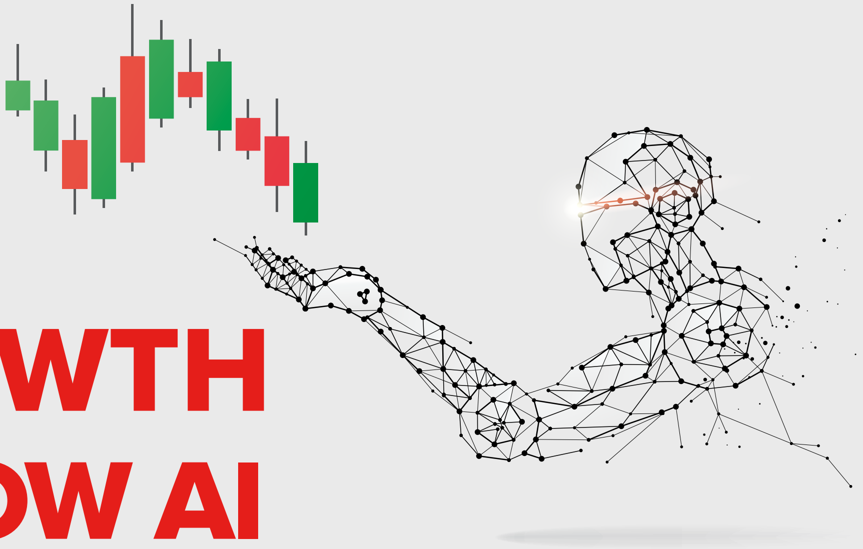
Our last IT professional is Vaughan Williams, Director Corporate and Community Services at North Grampians Shire Council (NGSC). NGSC is part of an RCTP initiative involving Northern Grampians, Southern Grampians and Queenscliff Shire Councils. Williams has another take on the issue.

"The problem starts when councils see themselves as unique and become resistant to any change in their entrenched processes," he said.

"In reality, all councils fulfil very similar functions for their local communities. We don't ask for Excel to be customised — we all have the same version and it works really well just as it is, regardless of your business processes."

When it comes to software in general, Williams has some sage advice.

"Councils need to stop being afraid of change — if we don't change our software when it's not working properly, how else are we going to encourage innovation and keep them (software vendors) honest?" he said.



iStock.com/Tuadesk

THE GROWTH OF SHADOW AI

IN THE WORKPLACE

A NEW AI STUDY HAS FOUND THAT 63% OF RESPONDENTS ACTIVELY USE AI IN THE WORKPLACE, BUT ONLY 36% OF ORGANISATIONS EXPRESSLY PERMIT IT.

Nearly two-thirds of employees in Australia and New Zealand (63%) are using AI in the workplace, despite only 11% of organisations having a formal policy in place permitting its use, research suggests.

The results of a survey published by ISACA, the professional association for IT governance, show that employees in the two countries are already using AI to create written content (51%), increase productivity (37%), automate repetitive tasks (37%), improve decision-making (29%) and provide customer service (20%).

But only 36% of ANZ organisations expressly permit the use of generative AI, only 11% have a formal comprehensive policy in place and 21% say their organisations have no plans to introduce such a policy.

Likewise, only 4% of respondents' organisations are providing training to all staff on AI, with 57% saying that no AI training is provided at all, even to teams directly impacted by the technology.

Such findings mirror concerns over shadow IT, or the use of IT-related hardware and software by employees without the knowledge of the IT department of security group.

ISACA Oceania ambassador Jo Stewart-Rattray said such a situation could be putting organisations at risk.

"As employees across the nation increasingly explore AI in the workplace — some initially out of curiosity — organisations must prioritise policies and governance frameworks addressing ethical, privacy and security concerns, to name a few," she said. "There is an urgent need to address the inevitable risks AI will generate, without stunting innovation and the benefits this technology brings."

Rather than seeking to prevent the use of AI in the workplace, organisations should be seeking to put guardrails around the use of the technology to ensure the security of corporate data and to ensure there are formal governance guidelines in place, Stewart-Rattray said.

"Employees are not waiting for permission to explore and leverage generative AI to bring value to their work, and it is clear that their organisations need to catch up in providing policies, guidance and training to ensure the technology is used appropriately and ethically," said Jason Lau, ISACA board director and CISO at Crypto.com. "With greater alignment between employers and their staff around generative AI, organisations will be able to drive increased understanding of the technology among their teams, gain further benefit from AI and better protect themselves from related risk."

The survey also found that 40% of employees believe that a significant number of jobs will be eliminated due to AI.

Despite such fears, 76% of respondents believe AI will have a positive or neutral impact on their industry, 79% believe it will have a positive or neutral impact on their organisations and 85% believe it will have a positive or neutral impact on their careers.