govtech review

GenAI
A PRAGMATIC APPROACH

FROM DATA TO INSIGHT
TRANSFORMING AUSTRALIA

SMART CITIES
THE ROLE OF WI-FI NETWORKS

Q3 2023
PP100021607

Q3 2023

INSIDE

FEATURES

Cover image: iStock.com/LightFieldStudios

Insider

Welcome to the Q3 issue of *GovTech Review* for 2023.

Our focus this edition is firmly on artificial intelligence. AI has made its mark in 2023, offering the perfect foil for organisations that continue to grapple with rising costs and skills shortages and look for new ways to improve efficiency, streamline operations and deliver a better customer experience. Rapidly developing technologies are being employed to various levels of effect across almost all sectors... government included.

The range of applications is broad, with some local governments using aerial mapping and AI technologies to gain better insights to better manage their natural and built environments, while researchers are turning to members of the public for data gathering. Using AI algorithms to detect and analyse seasonal changes and specific environmental events, scientists and academics can now quickly and accurately map ecological patterns that record the impacts of climate change — and develop strategies to mitigate or remove associated risks. Elsewhere, that same citizen-science approach is helping predict the probability, severity and burn area of potential bushfires, using images captured by the public to identify potential hotspots.

Of course, it's not all geospatial-related and boots-on-the-ground information sourcing. AI functionality is being progressively incorporated into software solutions and platforms, allowing organisations of all sizes to streamline operations, free up staff and elevate the customer experience through contact centre improvement.

While opportunity for improvement and heightened efficiency abounds, AI is not without its detractors — many of whom (somewhat worryingly) had a direct hand in the technology's development and advancement. The rapid rise and adoption of artificial intelligence has many commentators worried, and for good reason. While threat actors increasingly deploy AI functionality to improve efficiency in their more nefarious ambitions, there are also countless as-yet-undefined ethical, privacy and sovereignty implications in the rollout of these tools. As companies struggle to develop practical strategies to reduce risk, all eyes are on government for guidance — a difficult endeavour given broad-scale AI's relative newness and the corresponding lack of embedded expertise in both public and private sectors.

It's early days, so we'll have to see where the next 12 months take us, but there are repeated calls for a collaborative approach from industry and government. Working together pragmatically to understand the benefits and risks in the short term is seen as preferable to knee-jerk wide regulation that ignores the technology's rapid evolution — and therefore runs the risk of being ineffective before legislation is even enacted.

It's a thorny issue that will no doubt continue to stir up debate through the remainder of 2023 and well beyond. It will certainly make for an interesting ride, so hold on tight.

I hope you enjoy this issue of the magazine.

Dannielle Furness, Editor
editor@govtechreview.com.au

wfmedia
connecting industry

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

EDITOR
Dannielle Furness

gtr@wfmedia.com.au

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

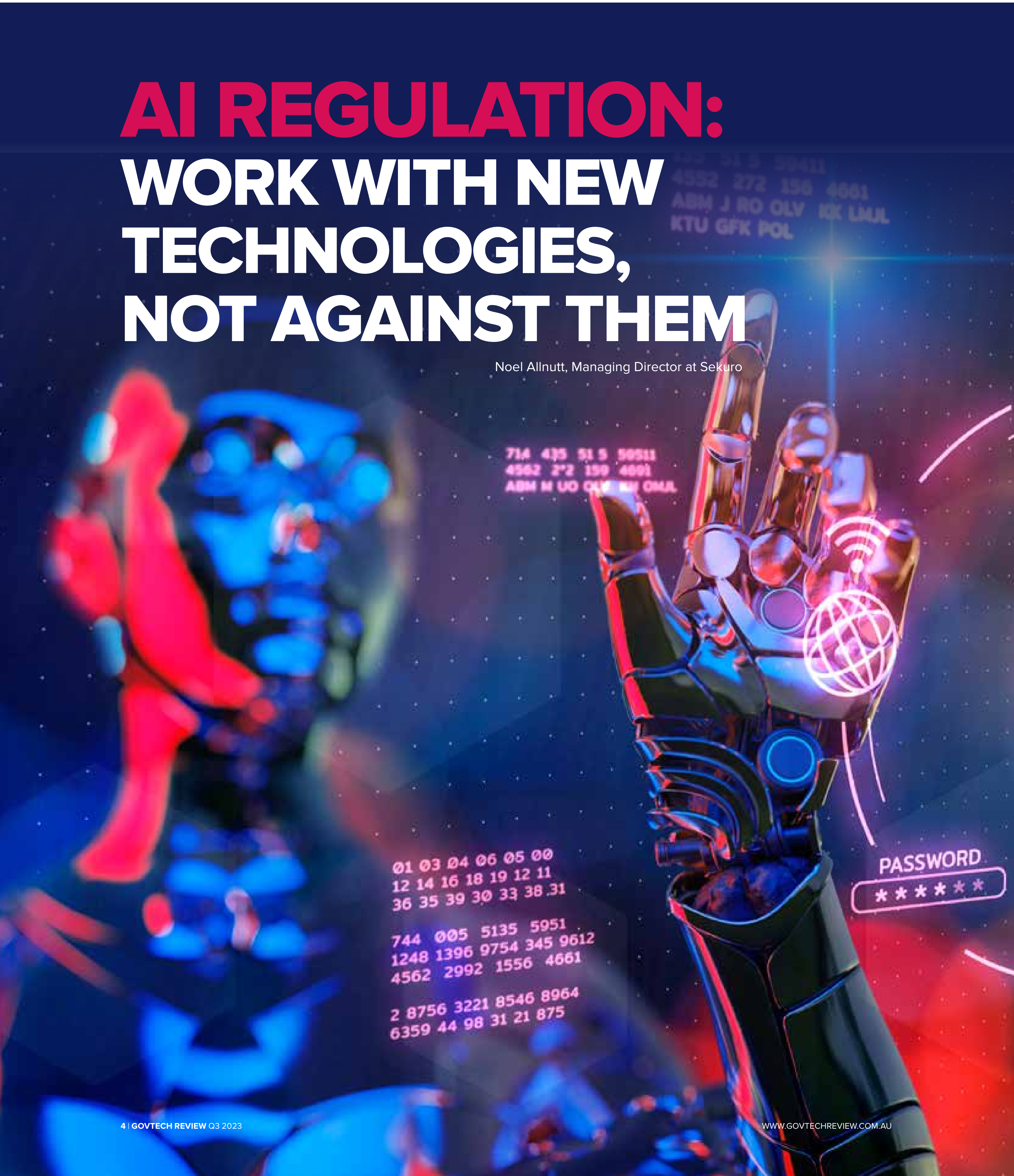
If you have any queries regarding our privacy policy please email privacy@wfmedia.com.au

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

AI REGULATION: WORK WITH NEW TECHNOLOGIES, NOT AGAINST THEM

Noel Allnutt, Managing Director at Sekuro



iStock.com/Thinkhubstudio

GENERATIVE AI IS CHANGING THE LANDSCAPE. HOW DO WE MITIGATE THE RISKS AND EFFECTIVELY REGULATE ITS USE?

We all knew generative AI tools like ChatGPT were fast approaching, yet what has been interesting to watch is the subsequent backstepping from the very people who created it. We all saw Geoffrey Hinton, dubbed one of the "Godfathers of AI", quit his job at Google just months after the launch of ChatGPT so he could speak out about the risks of AI. And we can't forget the more than 1000 high-profile industry executives — from Elon Musk to Steve Wozniak — who signed an open letter calling for a six-month pause on AI development to allow for regulation to catch up.

The hesitation from those behind the technology itself has served as a much-needed warning about blindly adopting a technology before understanding the consequences.

Minister for Industry and Science Ed Husic has already signalled intent to regulate 'high-risk' AI to curb threats like deep fakes and algorithmic biases. In response, Microsoft urged the government to assess risk based on the outcome of the tool itself, rather than banning AI technologies, particularly given the tools to measure potential AI harm are also still in development.

The thing is, we can't put generative AI back in the box it came in. It's here, and organisations, their employees and the general public are going to use it to find efficiencies, reduce human error and make more informed decisions. And whilst the AI waters are murky, it's clear that as a country, and even at a global level, we don't know enough about the risks to effectively regulate against it in a timely way.

So, if regulation is not the answer to mitigating AI risk in the short term, how can the government make sure that Australian organisations stay protected?

WHEN REGULATION IS NOT THE ANSWER

When it comes to legislating technologies, we've seen this same situation play out time and time again. Whether it be updating the Privacy Act or legislating data sovereignty, by the time the government has defined the problem, the entire issue has evolved so rapidly that any regulation is subsequently out of date.

The fact of the matter is that government legislation is not what we need to mitigate the immediate threats posed by AI. The legislative process is far too slow, and the adoption of AI is going to outpace any new policies before the ink is even dry. Instead, we'd be far better off with frameworks that can be drafted and then adapted quickly to evolve with the technology.

The other hurdle is that Australia doesn't currently have the talent to ensure effective regulation. But the truth is, nowhere does. There currently aren't enough people in Australia that know enough about generative AI and its consequences to create the right level of legislation. This is going to take time and collaboration with the private sector for governments around the world to better understand the risks and how to mitigate them.

Lastly, even if we were to regulate AI, it's all a waste of time if it's not enforced. Australia is the land of the slap on the wrist. Nobody has been fined 30% of their domestic revenue for breaching the Privacy Act despite it being written in law. The government needs a clear path for enforcement before starting down the road of regulating AI.

If it's not clear by now, my point is that protecting Australians against AI today will largely fall on the private sector. And what we need is a pragmatic approach outlined by the government that accepts AI as an integral part of the future of business whilst addressing the risks it poses.

A PRAGMATIC APPROACH TO RISK

There's a lot of confusion within organisations when it comes to AI adoption. We know effective regulation is a long way off, meaning the government needs to offer clear advice to establish a baseline for the private sector. Making sweeping statements threatening to ban AI is not going to stop adoption or reduce potential harm in the short term. The government needs to accept that we need to work with AI, not against it.

Whilst AI use in the workplace is likely to start off as a tool to help with relatively benign tasks like researching or writing presentations, it only takes one person to upload sensitive data into a third-party AI tool and before you know it, they've opened the company up to significant breaches of data privacy laws.

The government should be advocating for a collaborative, company-wide approach to implementing AI tools to properly access the risks and educate staff as to how to use them in a way that aligns with company policies and compliance requirements like data privacy and sovereignty. It sounds like an arduous task for IT teams, but this means reading terms of service to assess exactly how data is processed, stored and accessed. From there, organisations can create practical strategies to reduce the risks AI tools pose.

To go one step further, the government should be encouraging the private sector to establish formal working groups at an organisational level to investigate the benefits of each AI tool and develop a tailored action plan to roll out new technologies across the business. Having a working group will ensure that AI tools are providing actual value to the organisation, rather than a free-for-all based on individual needs. The working group will also be critical in making sure the adoption of AI is consistent across all functions and that it meets ethical, regulatory and compliance needs.

As AI evolves, so will our understanding of the benefits and risks it brings to organisations and society more broadly. As we wait for governments to catch up from a regulatory standpoint, the private sector needs the government to wake up to the realities of AI and provide clear advice based on the knowledge that the technology is already pervasive across Australian businesses. A pragmatic, outcomes-based approach to AI risk is required to protect Australian organisations and citizens whilst the government grapples with long-term regulation strategies.

"The other hurdle is that Australia doesn't currently have the talent to ensure effective regulation."

© Stock.Adobe.com/au/erhui1979

AUSTRALIA'S MOST PROGRESSIVE GOVT AGENCIES RECOGNISED

iStock.com/Parradee Kietsirikul

New South Wales (NSW) Department of Customer Service – Spatial Services (DCS Spatial Services) and the National Emergency Management Agency (NEMA) together with the Department of Home Affairs have been recognised with Special Achievement in GIS Awards for the Spatial Digital Twin (SDT) Program and National Joint Common Operating Picture (NJCOP) projects respectively, at the global Esri User Conference, hosting more than 100,000 delegates worldwide.

The programs align with the continued investment CIOs and other technology leaders are making to modernise their operations — to improve the access to digital government services.

In the case of DCS Spatial Services, its solution focuses on empowering the community to access information regarding the built and natural environment from the NSW Government's vast data networks. For NEMA, modernisation of its operation translates to a more timely response during times of impending disaster. In both cases, the application of geospatial technology combined with a citizen-centric focus has the agencies positioned as two of the most forward-thinking in the country.

DCS Spatial Services Surveyor-General and Executive Director Narelle Underwood said the GIS technology allowed for wider collaboration between agencies and improved how the community uses the digital twin.

"DCS Spatial Services is at the forefront of geospatial technology application; we have created a more collaborative environment that shares and visualises location information updated in near real time, with 4D models of the state to support improved decision-making," Underwood said.

Nineteen local government areas in Greater Sydney and regional NSW, representing about 37% of the population, have had data produced through the program so far, with 2D spatial datasets being upgraded to 3D/4D to support council planners and the community to interact with data in a user-friendly platform. Bathurst was the first regional city to be included in the NSW SDT Program, with four million square metres of CBD visualised.

As more data is integrated into the platform, the NSW SDT program is expected to provide significant opportunities for local councils and the NSW Government to realise benefits across the entire development and infrastructure lifecycle.

"Thanks to its ability to connect different data types and systems, the NSW Spatial Digital Twin program is enabling more efficient planning, prioritisation and delivery of infrastructure, and ultimately improved community engagement," Underwood said.

"By sharing data, organisations can come together to address mutual challenges — fostering public and private sector collaboration — that effectively accelerate the uptake of smart technologies across the state.

"We believe this model sets a strong foundation to facilitate delivery of information and datasets from local, state and federal agencies to the community."

SPONSORED CONTENT

5G in government: Enabling high performance, mission-critical services

Nathan McGregor, senior vice president Asia Pacific, Cradlepoint

iStock.com/Jian Fan

5G network slices increase the value and performance of mobile broadband, IoT, mission-critical communication, and more. Network slices are virtual networks that operate on top of shared 5G infrastructure. Available only on 5G networks with a standalone (SA) core,[1] each virtual network or "slice" is optimised for a defined organisational purpose by tailoring throughput, latency, speed, reliability, security, and more from end to end.

What does this mean for Australian government departments? Ericsson and BT predict that network slicing solutions will drive a 35% increase in value[2] for mission-critical IoT, thanks to a range of enhancements that include increased network flexibility and enhanced security for critical traffic.

Instead of best-effort, one-size-fits-all wireless services, government departments across various fields will be able to match their network needs and spending to desired or required service levels, improving use cases such as:

- Tele-operated driving and real-time situational awareness
- Remote medical emergency assessments and surgeries
- Remote video and real-time smart surveillance
- Remote drone control
- Virtual power grid monitoring and control
- Remote monitoring and control of machines and robots
- Ad-hoc or temporary mass events
- Augmented on-site experiences

Because 5G network slices are completely isolated, no slice can interfere with the traffic in another, making the user experience and security of each network slice the same as if it were operating on a physically separate network.

What other options do government departments have for secure, mission-critical connectivity?

Similar to a scaled-down version of a public cellular network, private 5G and LTE networks are dedicated cellular networks built to allow organisations to use licensed, shared, or unlicensed wireless spectrum to transmit data to wireless endpoints including smartphones, laptops, tablets, and routers. In big, sweeping areas where Wi-Fi isn't realistic and public cellular is either not available or too expensive for the sheer amount of data coming and going, private 5G and LTE combine the control of Wi-Fi with the benefits of cellular — like increased coverage, capacity, and security. Private network solutions from Cradlepoint and Ericsson offer the most flexibility, simplicity, and security to support any enterprise IT/OT organisation's mission critical applications and devices.

While there are some limitations in Australia due to spectrum availability, private cellular networks are coming and will offer government departments secure, reliable, cost-effective connectivity compared to public cellular and Wi-Fi solutions. Smart cities and municipalities for example, pose an interesting challenge and opportunity for Private 5G and LTE use cases. They are large, complex areas requiring reliable connectivity across an array of modern and legacy assets.

The key challenges smart cities face include surveillance cameras, smart lighting, intelligent traffic control, IoT technologies, public Wi-Fi access and EV charging stations. Private 5G networks are projected to overcome these difficulties to unlock the potential of IoT and become a driving force for the smart city and future investments.

Are government departments using 5G today?

Different regions around the world are at different stages of 5G maturity. While places like the US have the spectrum availability that enables private cellular, Australia is ahead when it comes to carriers offering network slicing. In the US, the Department of Defense has invested in growing the use of 5G, most recently through initiatives such as a 5G Challenge [3] and even within the last few years with its 5G to Future-G initiative.[4]

More specifically, the DoD has shown interest in how private 5G, and private cellular in general, can meet military needs. In fact, the DoD has recently been known as the organisation that spends the most on purchases related to private 5G.[5]

While Australian organisations wait for spectrum to become available and private cellular connectivity to become a viable option, governments can begin to plan their adoption of 5G SA, which offers significantly improved performance over 4G LTE. This makes it ideal for applications that require real-time communication and countless other opportunities for large organisations eager to capitalise on cellular networking.

Ultra-low latency

One of the most significant advantages of 5G standalone networks lies in their ultra-low latency. With latency reduced to milliseconds, real-time applications such as remote surgery, autonomous vehicles, and augmented reality (AR) have become viable and highly responsive. Ultra-low latency ensures virtually zero lag time in critical situations to enhance safety and reliability.

High reliability

SA networks operate on dedicated 5G spectrum bands, which reduces interference and congestion, making them more reliable and less prone to data outages. This reliability is especially crucial for critical applications such as emergency services or safety cameras in public spaces.

Enhanced security

Compared to its predecessors, 5G SA brings a wealth of security to the table. The technology boasts advanced encryption and authentication mechanisms, safeguarding sensitive data from potential cyber threats. Moreover — with features like end-to-end encryption and network slicing — 5G standalone networks are ideal for government departments that must protect sensitive data, such as citizen welfare or healthcare services. With robust security measures and dependable connections, 5G SA ensures a solid foundation for various sectors, including the public sector, to thrive, but it comes with its own set of challenges.

How 5G SA supports network slicing

SD-WAN enables traffic steering, where a software-defined router steers different sources of traffic to specific WAN links based on priority, use case, and the cloud-managed policies put into place by the IT team. The ultra-low latency of 5G networks and general improvements in broadband quality and capacity make cellular-optimised SD-WAN traffic steering highly valuable in government networks that may require secure links for classified or critical applications.

5G network slicing is a network architecture that enables virtualised networks to operate on the same physical network infrastructure. The basic idea of network slicing is to “slice” the original architecture into multiple logical and independent networks. These sliced networks can then be configured to effectively meet various application needs and service requirements. Each virtual slice aligns with the service categories of 5G — including eMBB, URLLC, and mMTC — and can also be customised to support public safety or other unique enterprise needs.

Looking ahead: controlling connectivity

One key benefit that comes with both network slicing and cellular networks is the control they give to the organisations that use them. With network slicing, IT departments can “slice” the original architecture into multiple logical and independent networks. These sliced networks can then be configured to effectively meet various application needs and service requirements.

In the case of private networks, operators have complete say in network traffic and network access. However, as the saying goes, ‘with more power comes more responsibility.’ Oftentimes, managing and establishing that private network comes with complexities. In some organisations, this could present somewhat of a hurdle, especially in departments where IT expertise and resources are limited.

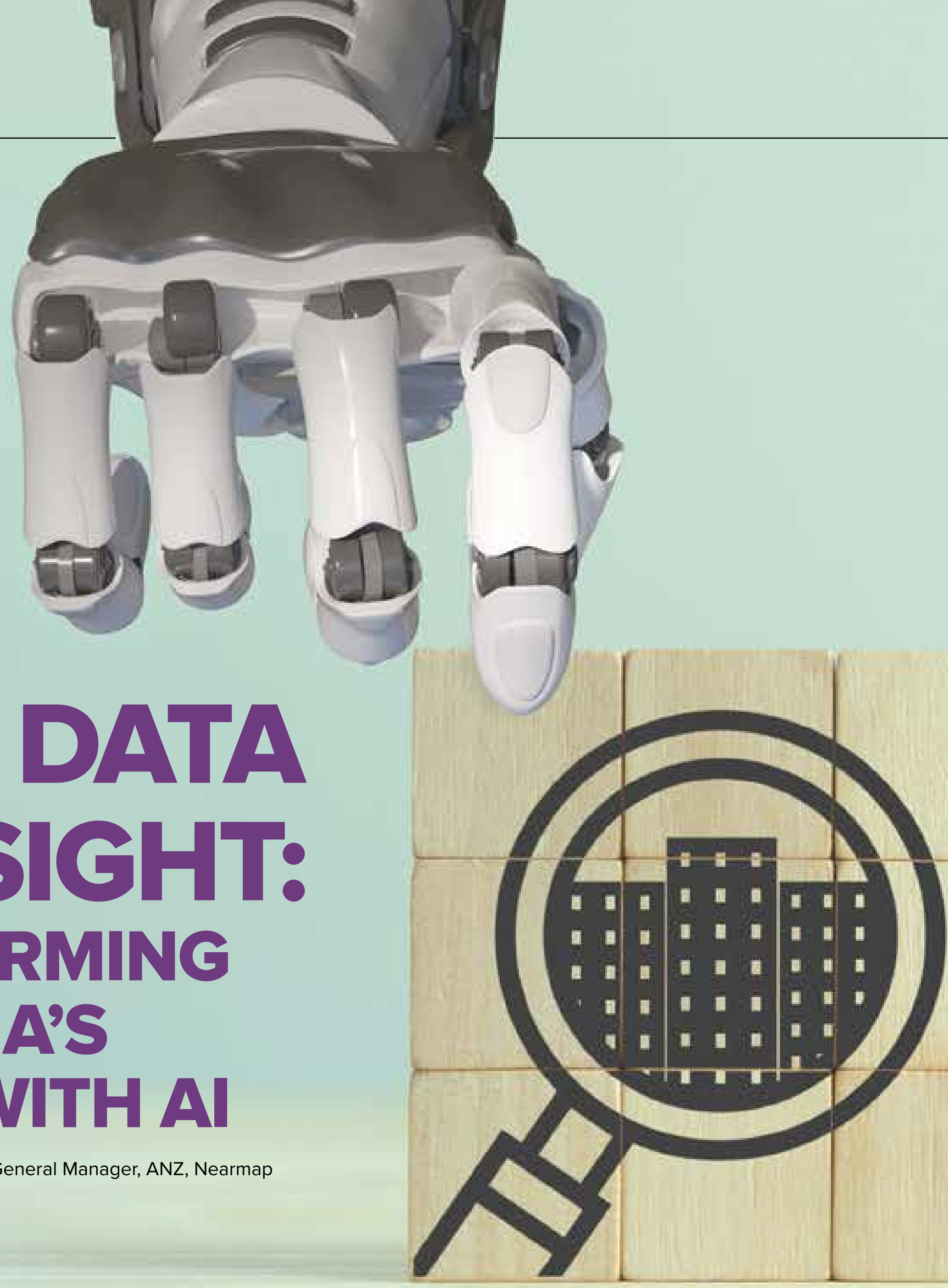
This is why organisations need to find a solution that makes both curating and maintaining 5G SA networks — and in the near future, private networks — as simple as possible. With the right 5G solution, setting up a network could take minutes, but would not compromise on the control, flexibility and security that will be necessary to streamline operations in government organisations.

1. *Standalone 5G vs. Non-Standalone 5G*, RCR Wireless, 7 Sep 2021
2. Ericsson Executive Guide: Scalable Network Opportunities
3. *DOD and the National Telecommunications and Information Administration Launch 2023 5G Challenge for Open RAN with an Eye Toward Future Base Modernization*, US Department of Defense, 2 Feb 2023
4. *DOD Establishes 5G and Future Generation Wireless Cross-Functional Team*, US Department of Defense, 9 Mar 2022
5. *DoD is the largest private 5G network deployer*, Fierce Wireless, 6 Oct 2021

cradlepoint

PART OF ERICSSON

Cradlepoint Australia Pty Ltd
www.cradlepoint.com/au



FROM DATA TO INSIGHT:

TRANSFORMING AUSTRALIA'S FUTURE WITH AI

Dan Paull, Executive Vice President & General Manager, ANZ, Nearmap

As Australia navigates an uncertain landscape, due to economic and environmental factors, embracing technologies like artificial intelligence (AI) becomes increasingly vital. By leveraging cutting-edge technology, organisations can navigate the challenges of an ever-changing world more effectively, drive growth, foster resilience and ultimately contribute to the betterment of communities nationwide.

With rising costs and skilled talent shortage, Australian organisations are increasingly seeking ways to drive efficiencies, improve operations and reduce expenses. Embracing technology has become an imperative for companies looking to stay competitive and resilient. At the same time, Australia has faced the impacts of El Niño and La Niña climate patterns for the third consecutive year, with many communities across the country still reeling from the devastating impact of bushfires, droughts and floods.

Efficiently evaluating, managing and responding to different risks and challenges requires Australia to leverage powerful data, insights and tools like never before. This is where the transformative potential of AI technology

iStock.com/Parradee Kietsirikul

comes into play. By harnessing AI, organisations can unlock a wealth of information and derive meaningful insights from a wide range of sources, helping them make better-informed decisions and take proactive measures.

CONVERGENCE OF DATA AND AI

The world is creating a staggering amount of data today. In 2010, we created just two zettabytes but, in 2023, it is expected to grow by more than 60 times to 120 zettabytes and hit 181 zettabytes by 2025. However, an excess of data is difficult to manage effectively, analyse thoroughly and use in its entirety. An IDC study found that less than 10% of data created each year is structured, meaning an overwhelming amount of data cannot be processed and analysed with conventional methods. This includes audio and video files, images and social media content.

Aerial imagery and location intelligence are pillars of geospatial information and knowledge within the mega data landscape that drives business decisions. Today, with even more comprehensive information, the focus is now on how organisations and communities can use pertinent data to enhance and strengthen their capabilities, optimising for the future.

The difference lies in the ability of AI to transform location data into location intelligence.

TECH-DRIVEN DECISION-MAKING

Organisations across various industries, from construction to real estate and the public sector, can harness the power of AI to gain valuable insights from geospatial data. With insights shaped by data and technology, organisations can make more informed decisions that drive growth and efficiency while positively impacting communities. The possibilities are vast.

Today, there are a multitude of challenges that organisations face in Australia — from rising costs to skill shortages. However, data-driven decisions can help increase productivity and enable cost savings.

For example, governments and councils are benefiting from greater situational awareness regarding the built and natural environment, gaining more accurate property insights at a commercial and residential scale, and analysing vegetation to better analyse and plan green space.

The City of Ryde in New South Wales also turned to aerial mapping and AI to help manage and protect its green spaces. By 2041, the city's population is expected to grow by almost 30% and green spaces are a vital part of any city — they improve air quality, reduce the urban heat island effect and can also improve residents' physical and mental health. As such, the leafy local government area (LGA) wants to ensure that its more than 200 parks and open spaces are conserved. However, as green spaces are often measured in anecdotal terms, the city needed a quantifiable approach to accurately measure the success of its conservation programs.

Using historical Nearmap geospatial data, combined with a tailored AI program and the latest machine learning technology, the city mapped tree canopy cover of the entire LGA. Armed with this critical data, it formed a baseline against which all future tree-planting programs would be measured.

The City of Ryde in April 2022, with an AI layer that maps canopy cover in the city.

Furthermore, in the public sector, technology plays a crucial role in disaster response and recovery efforts. From the Black Summer fires of 2019 to the country's worst floods in history, these natural disasters devastated communities across the country and most are still recovering from the impact. However, by utilising AI-powered aerial imagery, authorities can more efficiently assess the impact of disasters, prioritise resources and expedite recovery processes. Timely and accurate information derived from aerial imagery can make a significant difference in saving lives, restoring infrastructure and rebuilding communities. Insurance companies are also making use of this data to help assess damage and expedite the claims process.

In today's digital era, data is one of the most precious assets that organisations must leverage. The crucial piece of the puzzle lies in the ability to transform raw data and take advantage of the zettabytes of data at our fingertips to create an intelligent, insight-driven strategy. Moreover, at the pace that AI is developing, organisations now can filter through what is noise versus critical information within minutes, instead of weeks or months.

If organisations, both private and public, can harness the power of AI-related big data, their teams will achieve a deeper situational understanding than ever before, guiding decisions that will deliver the most beneficial impacts.

SPONSORED CONTENT

iStockphoto.com/matejmo

The cyber battleground

Unveiling emerging threats and the opportunity for change

The cyber landscape is constantly changing. With a seemingly endless parade of new attack methods and other security concerns, it can be difficult to stay on top of emerging threats and opportunities. To learn about the latest global and regional developments, we spoke with Jake King, Director of Threat Intelligence at Elastic.

One of the downsides of an increasingly connected world is the speed and efficiency with which cybercriminals can take advantage of new risks and vulnerabilities — something that organisations of all sizes in both private and public sectors now face daily.

It's no longer enough for enterprises, government agencies and vendors to practise a passive 'wait-and-see' approach when dealing with cyber threats. The constantly adapting and evolving environment calls for more pre-emptive strategies and action that is borne out of up-to-date analysis of the major threat tools, tactics and procedures currently employed.

According to Director of Threat Intelligence at Elastic, Jake King, and the rest of the team at Elastic — the company behind Elasticsearch® — true change means transforming the threat landscape from reactive to proactive. That means weaponising defensive technologies and creating an environment that is inherently hostile to threats. It might seem easier said than done, but King says the path forward is clear.

GovTech Review: The last few years have really created the perfect storm, generating a rapidly expanding threat attack surface. The pandemic gave us digital transformation acceleration, hybrid working, increased mobility and more reliance on cloud services. Combined with sustained development in IoT, AI and machine learning, along with some significant geopolitical events, it's been a boon for cybercriminals. What has this meant specifically for government?

Jake King: The pandemic changed things for the government. The scale of investment into cyber — infrastructure, programs to get people connected, healthcare responses and integrations — was more aggressive than we had seen in a long time. It transformed the public sector and allowed departments and agencies to extensively fund areas that were probably lacking prior to that. The opportunity now is to realise further dividends on that investment. Establishing these expert teams and utilising cutting-edge technology has made the public sector an attractive option for workers. Now is the time to level up those teams with training and skills development in key areas and new technologies — like generative AI — that will help the sector expertly address the challenges posed by an increasingly complex threat landscape.

GTR: How are those changes driving global threat trends, are they likely to impact our region and what should government agencies do to prepare?

JK: This is an interesting topic — on one hand, threats are borderless so there is effectively no real distinction. On the other, there are definite contrasts in defence and capability across different geographic regions when it comes to specific areas of security focus. We have observed strength in network-based security in some regions, including Australia, whereas other parts of the world, like the US, lean more heavily on endpoint detection methodologies.

Those divergent approaches mean response capability differs. Across APAC, where we have maturity at the network level, we can respond and react at the periphery, though that maturity hasn't extended to automation upon detection in all cases just yet. It has, however, led to cross effort on the part of threat actors. Where five or ten years ago, we had hours or days to respond, threat actors are now observing and moving very quickly using automation and sophisticated tools. We've done deep analysis on specific attack groups, their processes and responses, and we see new threats and capabilities quickly fill the niche of those that preceded them.

The thing to remember is that there are multiple threat groups operating globally. Australia is on the radar — as recent attacks have shown us — but adversarial groups aren't being drawn by geography, they're looking for opportunity. They target nations and organisations they believe offer greater potential for financial gain – it's usually that simple.

GTR: What are some specific insights gleaned from the latest Elastic Threat Labs report that you can share?

JK: One of the key things is the prevalence of business email compromise and the simplicity of many of these attacks. It is incredibly common to see a stolen password being leveraged to gain access to critical systems. We all tend to think of these large breaches as being complex or sophisticated operations when they are really just simple phishing or credential theft attacks — a tactic that is repeated globally.

What has changed, however, is that connected systems are making access available remotely. We now see more instances moving from business systems to infrastructure systems and, most recently, to the cloud. Cloud hosted applications and systems have historically been a bit of a blind spot for organisations, with many failing to recognise them as part of their own enterprise.

Things are speeding up on both sides. Our observation shows that threats of all kinds have adopted new capabilities and methods while increasing their cadence of activity. As organisations have tracked decreasing mean-time to detect (MTTD) and mean-time to remediate (MTTR) metrics, threats continue to act with even greater speed to undermine those efforts.

GTR: What does that mean for government agencies specifically — do their security and defence needs differ from private enterprise?

JK: The intricacies of many government systems — we're talking large data sets and interaction with multi-faceted services — make security an inherently complex exercise. If it were a private industry, the organisation would hire highly skilled individuals who would be very open in the way they use technology to achieve the optimum security stance. This is not necessarily the current public sector approach in many cases, often due to skills shortages.

We know from our observation that some aspects of the threat landscape cannot be addressed using technology — the right visibility, capability, and expertise are integral to success. This makes it critical for governments at every level to understand their specific attack surface, which means examining threats outside of the public sector, as well as in. Cybercriminals don't delineate between private enterprise and public, so efforts to understand the threat environment shouldn't either. It makes sense to look beyond government attack trends and investigate industry sectors that share similar conditions — the Department of Health could benefit more from an analysis of threats in the private healthcare vertical than the Department of Education, for example.

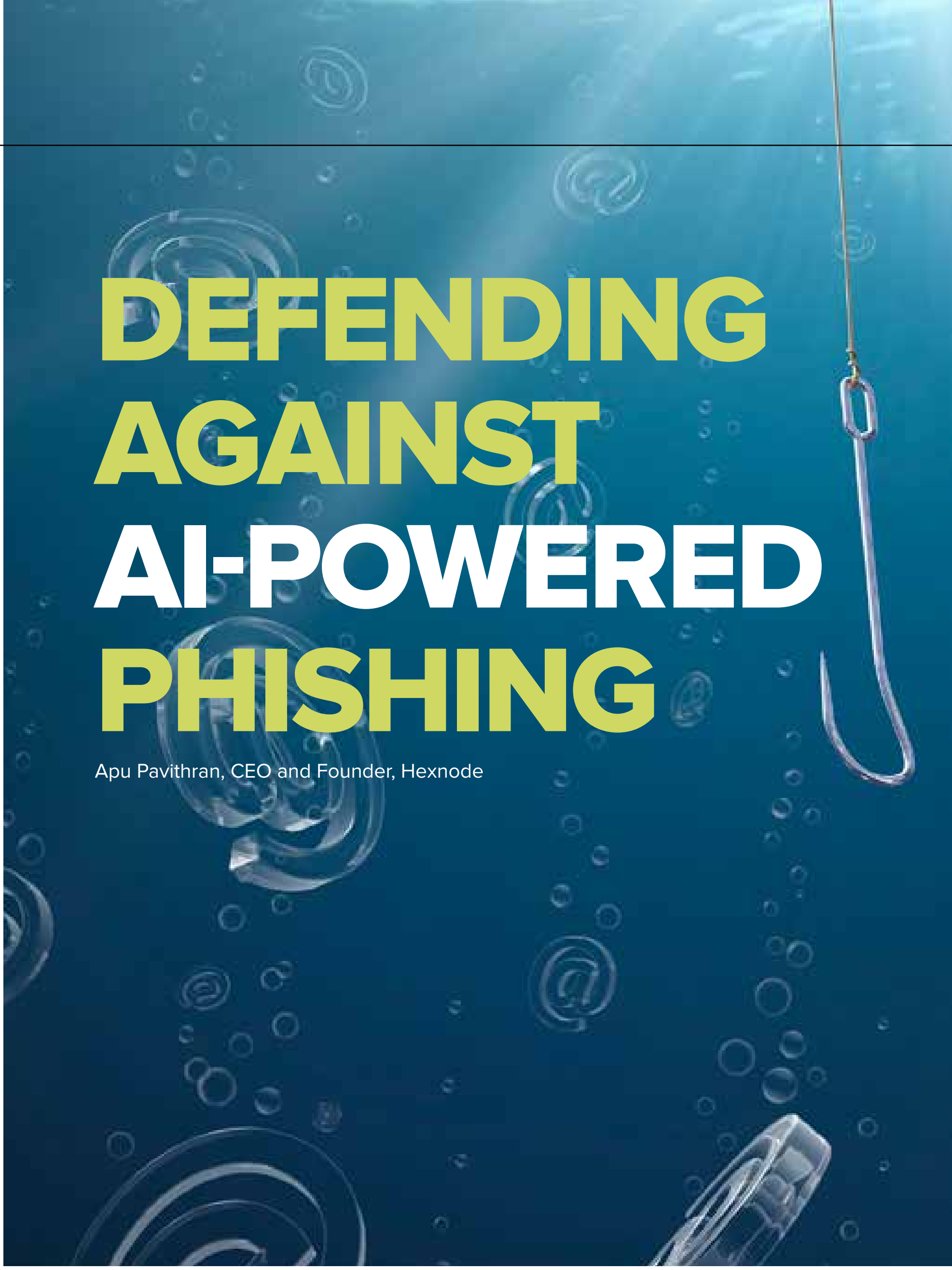
It also means having the right expertise embedded internally. Without it, organisations rely on vendors and service providers to set up, manage and operate security infrastructure. We've seen how this has left targeted entities at a disadvantage, whether the threat was a newly announced vulnerability, a threat group determined to extort, or collateral from a geopolitical event.

GTR: Where should we be headed with security approaches and defence strategies?

JK: We know that a significant percentage of all threats achieve a degree of success against technical, procedural and human mitigations, so something has to change. We can't keep operating in an endless cycle of vulnerability, exploitation, compromise and theft. The key to changing our collective response is to adopt a more open approach to security intelligence. Investments in data collection and our sensory apparatus indicate that visibility is the first step toward comprehension, and comprehension empowers us to act. There is no doubt our understanding of the global threat landscape is as open to change as the landscape itself, but we need to start somewhere. We know that through visibility, capability and expertise, we can create environments that are hostile to threats — allowing us to find them once, in one place, and interfere with them everywhere, all at once. That's a powerful outcome made possible through the open security approach we are committed to fostering across sectors with our Security Lab activities and research.

elastic

Elastic
www.elastic.co



DEFENDING AGAINST AI-POWERED PHISHING

Apu Pavithran, CEO and Founder, Hexnode

PHISHING ATTACKS ARE EVOLVING, THANKS TO THE INTRODUCTION OF AI. IN THIS ARTICLE, WE EXPLORE THIS POTENT COMBINATION AND PROVIDE STRATEGIES TO FORTIFY DEFENCES AND STAY AHEAD OF THE CURVE.

In today's world, where technology permeates every facet of our lives, the convenience and efficiency brought about by digital transformation are undeniable. One remarkable subset of this transformation that has quickly become a global sensation is generative AI. From content generation to writing code to generating images, videos and much more, the possibilities are limitless. However, this transformation has also opened Pandora's box, giving rise to a new breed of cyber threats — AI-based phishing attacks.

THE EVOLUTION OF PHISHING ATTACKS

The term “phishing” may evoke images of crude emails filled with misspellings and dubious claims, but the landscape has transformed dramatically over the years. From the early days of generic mass emails, cybercriminals have honed their tactics to create messages that prey on psychological triggers and exploit human vulnerabilities.

In the nascent stages of phishing attacks, cybercriminals cast wide nets, sending out thousands of emails hoping that a fraction of recipients would take the bait. These emails often contained glaring errors, making them easier to spot. However, the attackers adapted as people became more aware of these tactics.

Realising that personalised messages were more likely to succeed, attackers began to use social engineering techniques, tailoring their messages to exploit personal information gleaned from social media and other online sources. This evolution made it increasingly difficult for individuals to discern legitimate emails from malicious ones.

Now, in the age of intelligent machine learning algorithms, the infusion of AI into phishing attacks has been a game changer.

A POTENT DUO: AI AND PHISHING

Artificial intelligence is a double-edged sword, offering immense benefits while simultaneously amplifying the capabilities of malicious actors. In the realm of phishing attacks, AI provides

iStock.com/JanWillemKunnen

cybercriminals with powerful tools to create, adapt and launch attacks with unprecedented precision.

These AI-generated emails often mimic the writing style of colleagues, friends or family members, making them virtually indistinguishable from authentic communication. As a result, the human element in detecting phishing attacks has become less reliable, rendering traditional defence mechanisms inadequate.

Every AI chatbot relies on large language models, whether it's OpenAI's ChatGPT, Google's Bard or Microsoft's AI-powered Bing. Access to such large datasets dramatically speeds up information access and content generation. Phishing attacks targeting specific individuals or organisations have become alarmingly accurate thanks to the contextual knowledge available through these chatbots. By analysing publicly available data and scraping information from social media profiles, attackers can craft emails that reference recent events, projects or even personal interests. The result? An email that appears to come from a trusted source, weaving a seamless tapestry of deception.

Researchers from cybersecurity firm SlashNext recently found a tool called WormGPT being sold on a hacker forum. This 'black-hat alternative' to ChatGPT was designed specifically for malicious activities. While tools like ChatGPT have rules in place to try to prevent users from abusing it, WormGPT bars no such convictions and offers limitless attack possibilities.

Unfortunately, AI isn't just about crafting convincing emails. Every day, scammers are on the hunt for fresh ways to fool users into disclosing their personal information. With the development of deepfake technology, it is becoming more and more obvious that phishing schemes may use this potent tool in the future. Deepfake audio recordings may be used by cybercriminals to make voicemails that seem authentic and can direct the receiver to offer private or confidential data.

STRATEGIES FOR BUSINESSES: FORTIFYING AGAINST AI-BASED PHISHING

The convergence of AI and phishing requires a holistic and multifaceted approach to cybersecurity. However, every strong security posture necessitates strong fundamentals.

Endpoints and users are ground zero in the cyber warzone, and finding the right tools to protect them is essential. Employing a unified endpoint management (UEM) solution provides the capabilities to monitor and manage every endpoint. UEMs can enforce restrictions on managed devices to block untrustworthy applications and malicious websites or prevent the use of weak passwords. Furthermore, they can remotely set firewalls and filter out emails so that only authorised communication can pass through.

“Realising that personalised messages were more likely to succeed, attackers began to use social engineering techniques.”

Zero trust network access (ZTNA) and identity and access management (IAM) are two other critical solutions — the former encrypts sensitive data and ensures that every user is authenticated continuously to gain access, while the latter supplements ZTNA by assigning a consistent identity for each user which can be actively monitored. All three solutions lay the groundwork for implementing a zero-trust architecture. Deploying an architecture that involves multifactor authentication, segmentation of networks and continuous endpoint monitoring limits the potential damage even if a breach occurs.

With the basics covered, the next step is to fight fire with fire. The human instinct for detecting deception remains invaluable, but AI can amplify its efficacy. Owing to the rapid increase in AI-powered attacks, it has become challenging to employ enough human security experts to combat this exponentially rising problem. In order to stay toe to toe with them, intelligent automation is essential. By integrating AI-driven email analysis tools into communication platforms, businesses can automatically flag emails with suspicious patterns.

Behavioural analytics is another critical technology in the fight against modern-day phishing. It leverages AI to establish baseline patterns of user behaviour. By swiftly scanning through files and web pages to ascertain the legitimacy of their sources, it provides added visibility for the security operation. When deviations occur, such as an employee clicking on an unusual link, the system can trigger alerts or automatically quarantine suspicious emails. Additionally, by teaching it to quickly identify the precise designs and colour palettes of trademarked websites, it can automatically block any impostor sites that do not adhere to a particular site’s requirements. This approach minimises reliance on recognising known attack patterns and adapts to emerging threats.

Similarly, using natural language processing tools offers helpful context for identifying certain phrasing styles, accents and other verbal components. This would significantly help identify phishing calls that employ deep-fake technologies to sound almost exactly like a company’s C-level executive. If it is unable to find variations from a person’s typical pattern, the system can immediately issue an alert about a possible assault.

Even with all the bases covered and solutions implemented, your employees are still the first bastion to fortify your security architecture. Employees need to be well versed in the evolving tactics of AI-based phishing attacks. Moreover, regular training sessions highlighting the importance of not clicking unknown links or not using personal mail apps on work devices might seem trivial but are paramount. Finally, simulated phishing campaigns, infused with AI techniques, can provide a safe environment for employees to experience real-life scenarios and learn to distinguish genuine communications from malicious ones.

The era of AI-based phishing attacks requires a paradigm shift in our approach to cybersecurity. As these attacks become increasingly sophisticated, businesses must adopt equally sophisticated strategies to counter them. By fostering a culture of continuous learning, integrating AI tools and prioritising a resilient cybersecurity practice, organisations can build a robust defence against AI-based phishing attacks. The essence of the battle lies in leveraging human intuition, supported by AI, to safeguard our digital future in a world of rapid technological advancement.

AI-POWERED IMAGES TO HELP PREDICT AUSTRALIAN BUSHFIRES

A new citizen science initiative will help predict bushfires in the summer ahead, according to the University of the Sunshine Coast (UniSC).

The National Bushfire Resilience Network (NOBURN) project empowers people to use their mobile phones for information collection to help predict bushfire hotspots and minimise their impact, said Chief Investigator Dr Sam Van Holsbeeck.

“Fire season is approaching. After some very wet years with everything growing nicely, there’s a lot of fuel available,” Van Holsbeeck said.

“The NOBURN app encourages people out and about in their local forests to take photos and tell us more about the forest and fuels. That data is processed by artificial intelligence to help predict the probability, severity and burn area of potential bushfires.

“So what we want people to do is to go into the forest, snap a pic and help predict.”

The project is the culmination of two years’ research through an alliance of world-renowned researchers in artificial intelligence, forestry, human factors and science communication at the University of the Sunshine Coast and University of Adelaide’s Australian Institute for Machine Learning (AIML), in partnership with Noosa Shire Council and funded through the Federal Department of Industry, Science and Resources.

Professor Javen Qinfeng Shi from AIML said the AI developed for NOBURN is cutting edge.

“We are developing AI models to spot potential bushfire hazards and assess bushfire fuel load from the images captured by the NOBURN app. The algorithms behind these AI models are based on AIML’s world-leading expertise in computer vision, and machine learning,” Shi said.

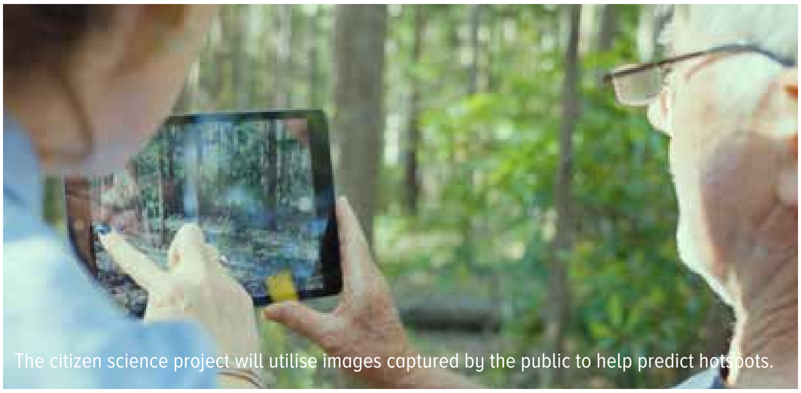
NOBURN was developed in the wake of the 2019–20 bushfires that burned more than 10 million hectares of forest, destroyed 2000 homes and claimed dozens of lives.

Professor Mark Brown from UniSC’s Forest Research Institute said the app will help predict future disasters of that scale.

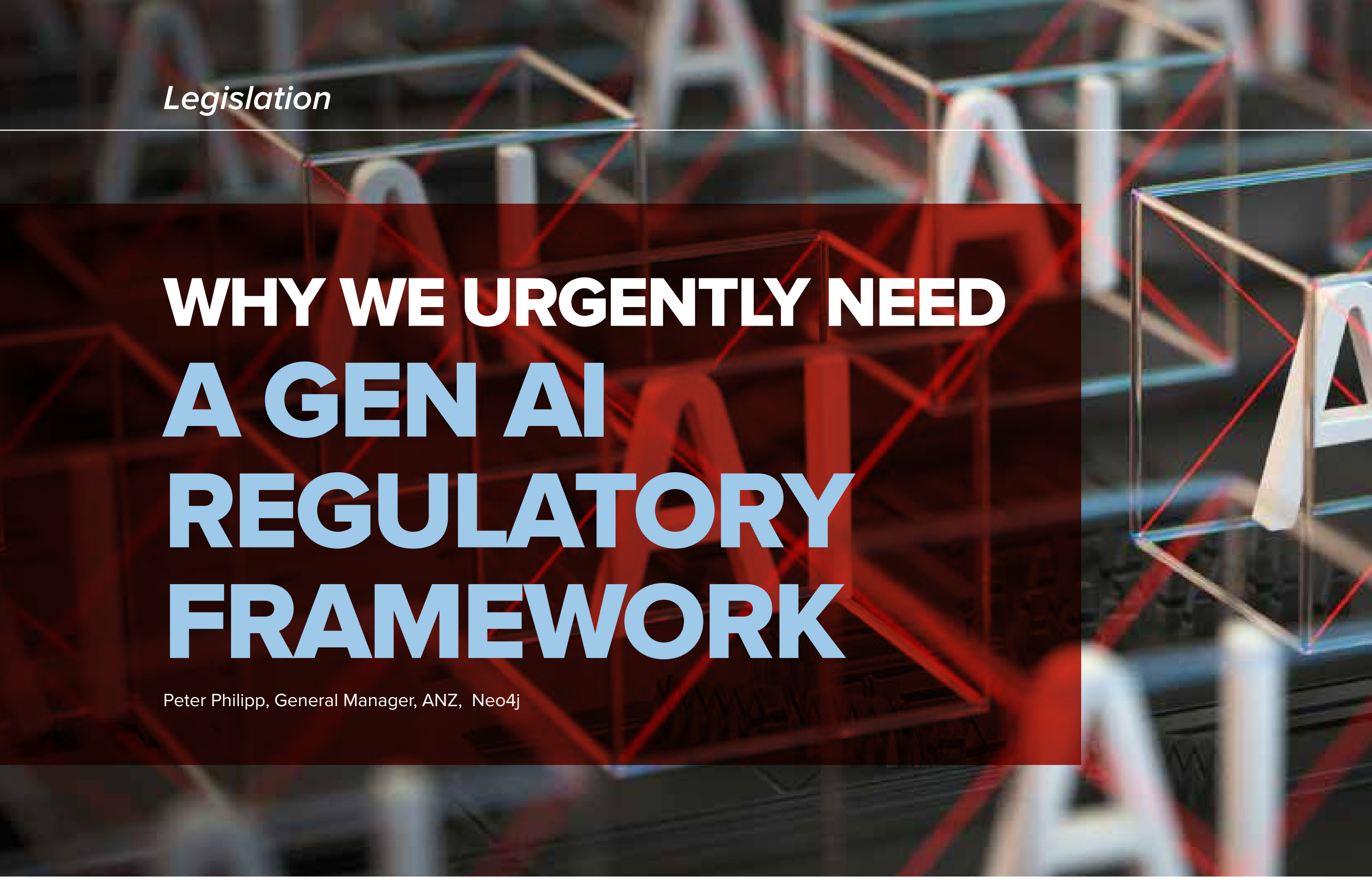
“While naturally occurring bushfires cannot be avoided, there is an opportunity with this project to predict their likelihood and implement strategies to minimise their impact on the environment, property and life,” Brown said.

Van Holsbeeck believes NOBURN will generate not only better-informed science about the risk of bushfires in Australia, but also better-informed communities.

“The NOBURN project is a unique opportunity to engage the community to collect nationwide forest fuel data while creating more awareness on the risk associated with fuels in our forests. It's a great way to learn how to be better prepared for any potential disasters or extreme bushfire events if they were to happen,” Van Holsbeeck said.



The citizen science project will utilise images captured by the public to help predict hotspots.



WHY WE URGENTLY NEED A GEN AI REGULATORY FRAMEWORK

Peter Philipp, General Manager, ANZ, Neo4j

From writing code to composing essays and answering questions to assisting with tasks, generative artificial intelligence (GenAI) is transforming the way people work, study and find information. This technology is poised to drive the next wave of disruption across nearly every industry, despite current limitations, including ‘hallucinations’, misinformation, bias and a lack of explainability.

REGULATORY MOVES SO FAR

Due to these concerns, there’s a growing consensus in Australia that GenAI needs a regulatory framework to ensure its safe and responsible development and deployment.

The Albanese government has released two papers to ensure the safe and responsible use of AI. The Safe and Responsible AI in Australia discussion paper investigates existing regulatory and governance responses here and overseas to identify potential gaps and recommend options to strengthen the framework. The National Science and Technology Council’s Rapid Response Report: Generative AI paper also assesses the potential risks and opportunities related to AI, delivering a scientific basis for discussions about the way forward.

Via a call for industry submission from the federal government, Google has urged we look at the greater picture. The organisation suggests copyright laws should be relaxed, thereby allowing AI systems to be trained. The company believes talent and opportunity are at risk, saying “the lack of such copyright flexibilities means that investment in and development of AI and machine-learning technologies is happening and will continue to happen overseas”. In addition, it says that there is a need for greater flexibility in sending sensitive data offshore and that companies should not have to deal with overly cumbersome requirements to justify how AI derives at its decisions.

The federal government has issued eight voluntary AI Ethics Principles and called for public submissions on the matter, the results of which are expected to drive decisions on potential regulatory changes.

Some other nations have also taken steps towards this. The European Union has developed legislation that would require companies that create GenAI platforms such as ChatGPT to publicise copyrighted content used by these technology platforms to create content of any kind. The United States Department of Justice (DOJ) and other US agencies have also issued a joint statement on Enforcement Efforts Against Discrimination and Bias in Automated Systems.

iStock.com/Just_Super

INDUSTRIES THAT REQUIRE REGULATION

The education sector is hugely impacted by generative AI. There have been instances where ChatGPT has been used to exploit the system, enabling students to pass exams ranging from high school graduation to legal and medical board exams. In response, educators have rushed out tools to try to detect AI-generated essays and 'cheating'.

There is considerable debate around whether such technology should be allowed at all. Curtailing GenAI in education may not be the answer, as it seems inevitable that students will continue to use it and find ways to circumvent bans.

Beyond the classroom, there is a need for regulation in industries where compliance and safety are crucial to ensure accountability, mitigate risks and safeguard the public welfare. The benefits of boosting productivity and facilitating data analysis by applying AI models should be combined with human oversight, which may involve incorporating additional checks and validation processes to verify compliance.

Establishing clear guidelines and validation processes will ensure AI systems align with regulatory requirements, maintaining standards for safety and compliance.

As exciting as these applications are, GenAI is intended to support and assist human workers, not replace them. The more powerful and widely used GenAI becomes, the greater its potential for negative influence. It will require a careful and responsible approach to ensure trustworthiness and transparency.

While AI requires regulation, technology providers cannot just outsource the 'how' to regulators, as there is a need to make the technology inherent to the solution itself. This is where graph technology comes in — by helping to solve issues on both the innovation and regulation fronts, making AI more productive and ethical in the process.

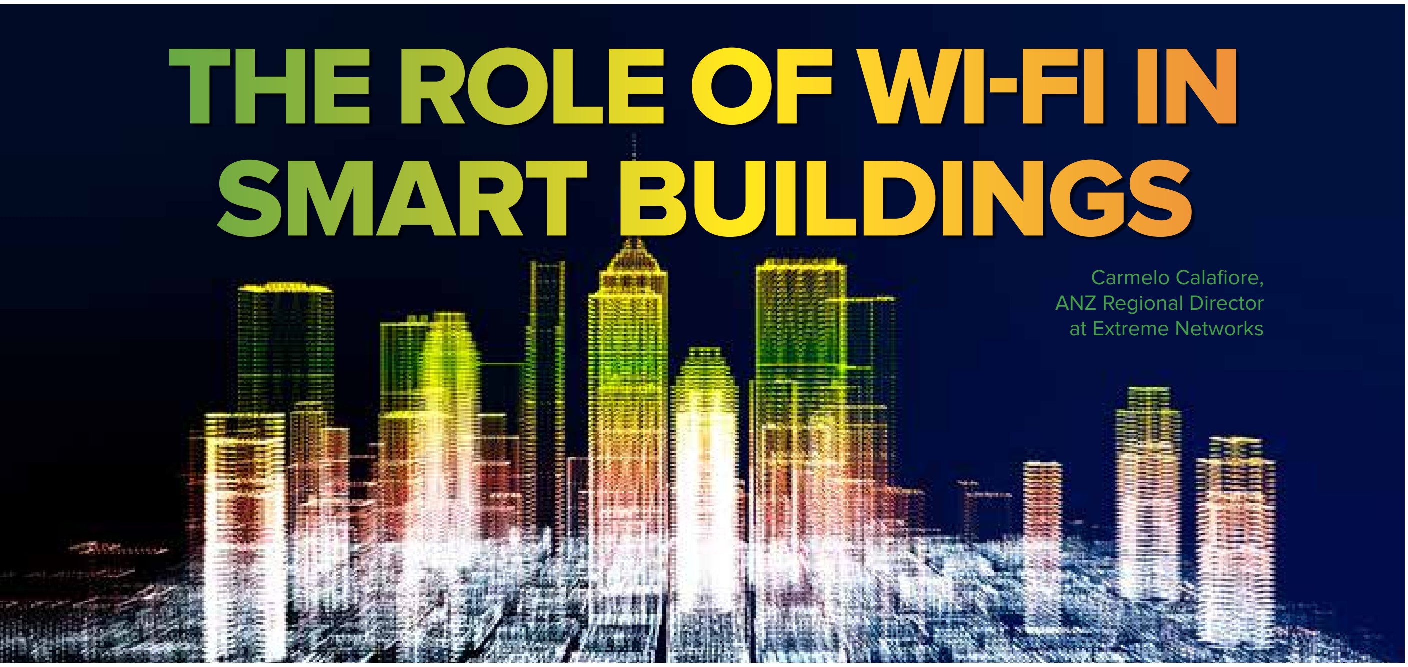
GenAI algorithms can inherit or amplify biases from training data, leading to discriminatory outcomes that reinforce existing inequalities. For example, if training data used to create a hiring algorithm is biased towards specific demographics, the algorithm may discriminate against other groups.

However, if IT leaders look at the technology that powers GenAI, namely large language models (LLMs), the potential of LLMs presents opportunities to overcome these challenges.

Enabling LLMs to ingest large volumes of text and make sense of it using knowledge graphs and graph data science algorithms will significantly reduce the risk of errors. Training LLMs on curated, high-quality structured data will help GenAI achieve accuracy, explainability, compliance and reproducibility.

For technologies where compliance or safety are important, creating a policy environment that helps inform the use of that technology is ideal. Our best response is to blend the best of GenAI with other tools to ensure that safety, rigour and transparency are adhered to and can truly be a benefit to organisations, businesses and society at large. The data and AI investment decisions made today will determine the leaders of the future.

THE ROLE OF WI-FI IN SMART BUILDINGS



Carmelo Calafiore,
ANZ Regional Director
at Extreme Networks

iStock.com/Thinkhubstudio

While the capabilities of smart buildings vary from one to the next, all share one key element: a robust Wi-Fi network. They are essential to smart building functionality as they allow diverse devices – including keypads, sensors, cameras, thermostats and lighting arrays – to connect and share data. Once interconnected and configured via Wi-Fi, they work together to create a seamless, smart environment. These networks also provide real-time data, enabling building managers to monitor and analyse building functions. Data capture and analysis of HVAC, lighting and security can significantly improve efficiency, allows real-time energy usage monitoring and can also generate building maintenance alerts. These functions will be enhanced as more smart buildings are equipped with Wi-Fi 6E networks, allowing operational IoT devices to be shifted to the 6 GHz frequency band, delivering faster speeds and lower latency. It will also remove some of the burden from existing 2.4 and 5 GHz networks and improve their performance.

REMOTE ACCESS

Strong Wi-Fi connections deliver other benefits as well. Building managers can remotely access and control multiple building systems from a central location, allowing for more efficient operation and maintenance. Wi-Fi-enabled sensors can detect when a room is unoccupied and adjust the temperature or lighting accordingly, saving energy and reducing costs. Wi-Fi also supports the rapidly increasing number of available IoT devices, further enhancing building management and operation. IoT builds on the rich history of monitoring, telemetry, sensor-based computing and automation that has been a part of many industries for decades. Because IoT devices are based on Internet Protocol (IP) networking, the majority are instantly compatible with existing building wireless and wired networks.

WI-FI AND SECURITY

As well as boosting building efficiency and convenience, a strong Wi-Fi connection is essential for the safety and security of occupants. A robust Wi-Fi network allows integration of sophisticated security systems that provide real-time alerts and monitoring, enhancing overall safety levels. Smart building Wi-Fi networks can also help to prevent potential accidents or incidents. For example, a building manager could use Wi-Fi-enabled sensors to monitor and detect hazards such as gas leaks or faulty electrical systems. This allows remediation steps to be taken before the situation escalates. Occupant safety in smart buildings is also enhanced by Wi-Fi. For example, building managers can use Wi-Fi-enabled systems to communicate real-time safety instructions and evacuation procedures to occupants in the event of an emergency. It can also support the deployment of location-based services, providing real-time information about safety hazards, emergency exits and evacuation routes. In the future, it's highly likely that most commercial and residential buildings will become smart, as the benefits become more widely understood. An even broader range of devices that further enhance the environment for occupants will be utilised. As the inevitable march towards truly smart cities continues, these facilities form the building blocks, and central to success is connectivity via a robust and secure Wi-Fi network.

iStock.com/metamorworks

HOW TO USE AI TO REACH OPERATIONAL MATURITY

Kelly Brough, Data and AI lead, Accenture ANZ

Just like the Industrial Revolution or the dot-com boom, AI is shaping the future of how we work and what we do. The massive shifts we are witnessing in technology, consumer preferences and climate change are redefining how the world operates. We are only just beginning to see the full potential of AI and its unique value to each industry, including the public sector. As this technology evolves at pace, government agencies and the public sector need to move quickly, but also with caution, to develop an AI strategy or they risk falling behind and not delivering to citizen expectations. Such extraordinary times call for an unprecedented response and a reinvention of the way the sector operates. But while some organisations in the public sector are rising to this challenge, we're witnessing a widening gap between AI adoption and effective utilisation.

ADDRESSING THE GAP OF OPERATIONAL RESILIENCE

AI operational maturity is the evolution and development of an organisation's capabilities and processes to effectively integrate and utilise artificial intelligence in day-to-day operations. This could involve stages or levels of maturity that organisations progress through, and we can split this across six capability measures: data, analytics and automation; artificial intelligence; leading practices; business-tech collaboration; talent strategies; and stakeholder experience.

The benefits of lifting AI operational resilience across these six capabilities include outcomes such as being 34% better at reducing energy consumption and greenhouse gas emissions and 25% more effective at delivering equality of opportunity, as well as in the private sector, delivering 2.2x the shareholder return.

The issue is, while many organisations in Australia's public and private sectors are already using AI to bolster their operational resilience, only 2% are using it effectively. And with AI counting as a business digital investment priority, the biggest challenge leaders face today is optimising output.

Juggling these demands means keeping the big picture in mind — and not just focusing on financial measures. Enterprises, government agencies and vendors need to take a fresh approach to unlocking their internal talent and committing to business goals. Sustained growth is rooted in strategic transformation and AI maturity comes from mastering a more balanced approach across integrating the six capability measures — not only in data and AI, but also in organisational strategy, talent and culture.

Decision-making needs to be driven from the top, backed by senior leadership. By clearly outlining the organisation's goals and objectives for adopting AI, operational reinventors ensure that AI execution aligns with overall business strategy. Reinventors invest in their workforce, to educate and train them about AI technologies, benefits and potential use cases. An organisation is only as good as its people; therefore, they must be empowered with the knowledge and skills needed to effectively use AI tools, which would then foster a willingness to embrace AI-driven solutions across all levels.

> *To embark on the path toward AI adoption, it's crucial to start with a strong foundation.*

This landscape is fast-paced and highly competitive, and each facet of daily operations must be transformed, with new ways of working and engaging with the public and new opportunities for growth. By connecting people and assets to the appropriate technologies, the synergy between human expertise and AI capabilities can lead to exponential growth in operational efficiency. But is this just easier said than done?

LAYING THE GROUNDWORK FOR SUSTAINED SUCCESS

To embark on the path towards AI adoption, it's crucial to start with a strong foundation. This entails a comprehensive assessment of capabilities, technology infrastructure and data readiness. Areas need to be pinpointed where AI can make a meaningful impact, and those areas need to align with the government department or agency's overall strategy. A clear understanding of the starting point is necessary to create a roadmap that ensures a seamless integration of AI initiatives into existing operations.

Effective adoption and utilisation of AI at scale across an organisation is an ongoing process that requires continuous learning, adaptation and refinement. It is necessary to regularly assess the performance of AI models, monitor their impact and make adjustments. It's essential for governments and the public sector to align AI initiatives with their unique context and long-term growth strategy.

While the public sector has different rules and regulations to adhere to, it can also take insights from the experiences of private companies to improve and transform its own operations and growth strategy. A great example is a large Australian telco that deployed AI to quantify the effectiveness of its individual marketing initiatives. The organisation was able to accurately and rapidly measure thousands of different marketing metrics to create a world-class marketing performance insights capability that can be applied across the business. These insights enabled them to optimise the allocation of marketing spend, messaging and media, resulting in quick, easy gains. Once the foundations are in place, the ability to scale across the business is far more attainable.

AI ISN'T JUST A BUZZWORD...

It's a strategic imperative that will drive profound shifts in how government entities operate and deliver value. And in this current landscape, it's certainly one that forward-thinking public service leaders cannot afford to overlook. By seamlessly integrating AI-driven insights into decision-making, the public sector can unlock unprecedented efficiencies, harness untapped opportunities, and elevate customer experiences, with a resounding impact on profitability and sustainable growth.

AI-POWERED PHONE ASSISTANCE DEFLECTS 43% OF INBOUND CALLS

iStock.com/AndreyPopov

The UK's Derby City Council and council-owned Derby Homes — an organisation created to manage and mantain the council's housing stock — have supplemented their main switchboard with phone-based AI assistance to deal with inbound resident calls.

As Director of Digital & Physical Infrastructure and Customer Engagement at Derby City Council, Andy Brammall said embracing the power of AI for digital self-service was a logical move.

"It quickly became clear that AI had the potential to dramatically streamline our customer service operation. We started first with an AI-powered website assistant and followed by supplementing our main switchboard with phone-based AI," he said.

Inbound phone calls represent 60%+ of resident contact with the council, and therefore are the cornerstone of Derby City Council's self-service strategy.

"Trained in over 1000 council services, it has exceeded our deflection target of 21%, handling over 62,000 calls and achieving an incredible 43% deflection. This success has allowed us to maintain our service levels while streamlining operations," Brammall said.

The new AI assistants, Darcie, servicing the council's customer service centre, and Ali, serving Derby Homes, are currently answering over 1000 questions each day, directly handling up to 45% of inbound calls. Beyond answering citizen queries, they can also direct calls to over 40 different departments.

The new AI system employs advanced natural language processing, providing a user-friendly, 24/7 service in natural language to simplify interactions.

"Our new AI assistants not only allow citizens access to a range of council services and information around the clock and across multiple channels, but by automating routine tasks they also free up time for our colleagues to focus on more complex queries which require human conversation. This ultimately aims to provide a more personalised service for our residents, improving service delivery and achieving higher levels of resident satisfaction," Brammall said.

The council partnered with ICS.AI and leveraged its SMART AI platform for this transformation. This development sets a benchmark for using AI to streamline public services and enhance citizen engagement.

"We chose the SMART AI platform from ICS.AI for several reasons. Their strong reputation and proven experience in the local government sector reassured us of their capabilities. They offered a 'human parity' council AI language model trained in over 1000 council topics, which could be rapidly deployed, and we were confident in their performance and their proven commitment to innovation in the phone channel. Above all, what really appealed to us was ICS.AI's genuine interest in working as a true collaborative partner," Brammall said.

The council is committed to further exploring the potential of AI technology across additional contact channels and service areas to further improve customer service and increase efficiency.

OAIC RELEASES ATTITUDES SURVEY RESULTS

The Office of the Australian Information Commissioner (OAIC) has released results from a major survey into privacy attitudes and experiences.

The 'Australian Community Attitudes to Privacy Survey (ACAPS) 2023' uncovered a sharp increase in the number of Australians who feel data breaches are the greatest privacy risk they face. The survey tested attitudes on topics such as data practices, privacy legislation, data breaches, biometrics, artificial intelligence and children's privacy.

"Our survey shows privacy is a significant concern for Australians, especially in areas that have seen recent developments like artificial intelligence and biometrics," said Australian Information Commissioner and Privacy Commissioner Angelene Falk.

"Australians see data breaches as the biggest privacy risk today, which is not surprising with almost half of those surveyed saying they were affected by a data breach in the prior year.

"There is a strong desire for organisations to do more to advance privacy rights, including minimising the amount of information they collect, taking extra steps to protect it and deleting it when no longer required."

Among the key themes of the survey are:

- **Australians care about their privacy.** Nine in 10 Australians have a clear understanding of why they should protect their personal information, and 62% see the protection of their personal information as a major concern in their life.
- **Australians don't feel in control of their privacy and don't know what to do about it.** Only 32% feel in control of their privacy, and half believe if they want to use a service, they have no choice but to accept what the service does with their data. Three in five care about their data privacy, but don't know what to do about it.

iStock.com/xxxxxx

- **Most Australians have had a negative privacy experience.** 47% were told by an organisation that their personal information was involved in a data breach in the year prior, and three-quarters said they experienced harm because of a data breach.
- **Australians have strong feelings about certain data practices.** Nine in 10 are concerned about organisations sending customers' information overseas. 96% want conditions in place before artificial intelligence is used to make decisions that might affect them.
- **There are high levels of distrust.** Only four sectors (health, federal government, finance and education) are more trusted than not by Australians to handle their personal information. Less than half of people trust organisations to only collect the information they need, use and share information as they say they will, store information securely, give individuals access to their information and delete information when no longer needed.
- **Australians want more to be done to protect privacy.** 84% want more control and choice over the collection and use of their information. Around nine in 10 Australians would like businesses and government agencies to do more to protect their personal information.

Commissioner Falk said the survey has important signposts for organisations.

"The findings point to several areas where organisations can do more to build trust in the community," she said.

"Not only is good privacy practice the right thing to do and what the community expects, it's a precondition for the success of innovations that rely on personal information."

The survey findings also show there is strong support for privacy law reform.

"We are at a pivotal moment for privacy in Australia, where we can seize the opportunity to ensure laws and practices uphold our fundamental human right to privacy," Falk said.

"This is an opportunity to ensure the protections the community expects are reflected in the law.

"The OAIC will use the findings to inform our ongoing input into the review of the Privacy Act and to target our activities at areas of high concern among the community."

The full report is available on the OAIC website: oaic.gov.au/acaps.

KEY FINDINGS

- Three-quarters of Australians feel data breaches are one of the biggest privacy risks they face today. This has increased 13 percentage points since 2020.
- Seventy per cent of Australians place a high level of importance on their privacy when choosing a product or service. After quality and price, data privacy is the third most important factor when choosing a product or service.
- Australians trust health service providers the most and social media companies the least when it comes to the protection and use of their personal information.
- Only 42% of Australians feel most organisations they deal with are transparent about the way they use their personal information, and three in five don't understand what organisations do with the information they collect.
- Over half of Australians consider having to share some personal information if they want to use a service fair enough. However, they generally only consider it fair and reasonable to provide their name (81%) and email address (77%) to organisations and, to a lesser extent, their phone number (68%), date of birth (62%) and physical address (61%).
- Protecting their child's personal information is a major concern for 79% of parents. However, only half feel they are in control of their child's data privacy. 85% of parents believe children must be empowered to use the internet and online services, but their data privacy must be protected.

DATA SECURITY AND SOVEREIGNTY IN THE AGE OF VULNERABILITY

Terry Miaolo, VP & GM, APAC, OVHcloud

In recent years, the world has witnessed new emerging technological innovations that have maximised business potential, such as the cloud and the transformation of digital data storage. Although these rapid developments are exciting, they come with new questions and challenges that businesses must conquer to ensure customer safety.

Australia has seen various high-profile cyber attacks that not only prove the need for significant reviews to data protection laws, but also for cloud providers and other technological bodies to consider what forms of regulation businesses should adhere to in order to combat the growing threat of cyber breaches.

The number of Australians who are actively concerned about the security of their data has grown significantly over time. Almost two-thirds of Australians (64%) lack confidence in the ability of large organisations to keep their personal data safe, while 83% are concerned about the security of information held by their service providers.

Essential for the future use of new technologies, both businesses and governments alike must also consider key challenges to maintain their duty of care whilst delivering innovative technologies to their customers.

THE STATE OF PRIVACY ACTS

As the world continues to become more connected than ever, so does the transferring of personal data globally. However, processing data through new solutions like the cloud often risks exposing sensitive information, with personal data quickly becoming a commodity for hackers.

Following the high-profile Australian cyber attacks of 2022, the Attorney General's office released a review of the 1988 Privacy Act. As part of its review, the office emphasised the outdatedness of the Act as well as the urgent need to focus on the vulnerability of individuals' information in the new digital age. The Attorney General's office specifically highlighted just how at-risk millions of Australians are to privacy risks such as identity theft, reputational damage and blackmail.

The review concluded that Australia's regulation on data privacy needs updating, citing the modernised approach of the European Union's General Data Protection Regulation (GDPR), which applies to any person or company who handles personal

full transparency about data location and regulations is critical in retaining control of data in the cloud.

HOW CAN AUSTRALIA APPLY THIS?

Drafted in 1988, the Privacy Act requires urgent changes to meet the standards of today's demands and new technologies. By ignoring the threats that are cyber attacks and the exposure of personal information, regulators run the risk of hurting trust and uptake in new technology needed to deliver digital services. Australia should look to bodies like the EU that have responded to these technological advances in personal data handling. By doing so, Australia can position itself as a trust partner and reap the economic benefits for local business and the economy.

Australia should consider applying transparency laws to business to ensure that breaches and data location are made aware to customers. Amendments should also look to ensure individual control over personal information.

Adopting a more protective regulation on data protection would also offer Australian companies a wider playing field as data could flow more easily between Australia, the EU and Canada.

The future is cloud, and there are opportunities for organisations to improve security systems and processes and better manage data collection and retention. Australian businesses and governments alike must come together to combat new threats to personal data by placing data protection and compliance at the forefront of data regulation.

information of a citizen. By following this type of regulation, businesses can better keep personal information safe regardless of where in the world it is stored.

On the flip side, complex data laws can leave companies lost in how regulation is enforced differently in different parts of the world, hindering local customers in taking advantage of cloud services. In fact, faced with changing regulations, compliance is a top cloud challenge according to 76% of organisations.

A recent survey from ISACA also found that 54% of businesses experienced a large skills gap with frameworks and/or controls and 46% with understanding the laws and regulations that an enterprise is subject to.

The question becomes, how do we overcome these data protection and security hurdles to provide clear pathways for cloud providers and customer protection alike?

Questions you should be asking your cloud service provider should include:

- Where is my data stored?
- What laws apply to my data and who could access it?
- Does my cloud provider follow best practices in terms of security and data protection?

HONESTY IS THE BEST POLICY

As part of the journey towards adopting cloud, customers and providers should ensure compliance with various data protection laws both locally and globally. Doing so not only means that organisations are fulfilling their duty of care, but also protecting themselves from the risk of imposed fines and infringements. Coming to the table with

FIXING THE NDIS

Mark Woodland, Co-founder & CEO, Kismet

iStock.com/Nils Versemann

The National Disability Scheme (NDIS) is one of Australia's most critical social services for those in need. In its current state, running the NDIS is growing exponentially in cost and that is set to double to $108 billion by 2034. On top of the cost, the scheme currently offers support to about 590,000 people with permanent and significant disabilities — but this is only 13% of the 4.48 million people living with a disability in Australia.

In October, an independent panel will share recommendations for the NDIS which is set to 'reboot' the scheme. But if the last 10 years of the NDIS's existence is anything to go by, it may not be the kind of reboot we need.

INEFFICIENCY ONE OF THE MAIN ISSUES

Both NDIS and the healthcare system it is built within are riddled with inefficiencies. Many health providers still use legacy systems, relying on pen and paper, which slows down simple things such as invoicing, reimbursements and even general reporting.

Meanwhile, the current shrinkage of the healthcare workforce means that NDIS participants stay on waitlists for months on end. This has a flow-on effect, such as their NDIS funding being cut due to underutilisation and families end up paying from their own pockets to support their needs. This is even more concerning as the government has pledged an 8% annual growth cap and is currently working on reforms that will result in a forecasted 27,000 fewer people joining the NDIS over the next four years.

Now more than ever, we need to find more effective and efficient ways to support our community.

THE ROLE TECHNOLOGY CAN PLAY

There are simple technology-powered tools and solutions that already exist and that could solve myriad problems when it comes to our disability scheme, and can support those living with disabilities.

For instance, mandatory digital check-ins could ensure that participants are only charged for the consultations they actually attended or only pay for the cleaning services that were really provided to them. It will also ensure that invoices are reimbursed quickly, in the 2–3 business days window the government is promising.

Digital wallets would also allow better transparency for participants when it comes to their plans, and give them an accurate picture of the remaining allocation for sub-budgets, allowing them and their careers to better manage their plan. They will also allow family members to have better oversight of their loved ones' plans, potentially spotting fraud more easily.

MORE IS BETTER: HOW A CO-CONTRIBUTION MODEL CAN HELP

Recent modelling by Kismet revealed that optimising expenditure by only 5% would allow up to 273,000 additional people access to the NDIS by 2032, while means-tested co-payments would address ongoing cost management.

High-income households would no longer receive full NDIS subsidies, which would free up resources and enable a broader distribution of benefits for more people. The idea is to ensure that the financial resources of the NDIS are allocated in a manner that prioritises those who need them the most, while still providing some level of support to higher-income households.

While it's been 10 years of the NDIS, we can't let another 10 go by without change. We believe that better use of technology combined with the application of a co-contribution model will be a game changer for everyone touched by the NDIS, from participants to providers.

FREE

for government and industry professionals

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

wfmedia
connecting industry

Lab+Life SCIENTIST
safety solutions
what's new in Food technology
critical comms
HOSPITAL AND HEALTHCARE
PROCESS TECHNOLOGY
Electrical Comms Data ECD
what's new in electronics
SM sustainability matters
agedhealth

www.WFMedia.com.au/subscribe