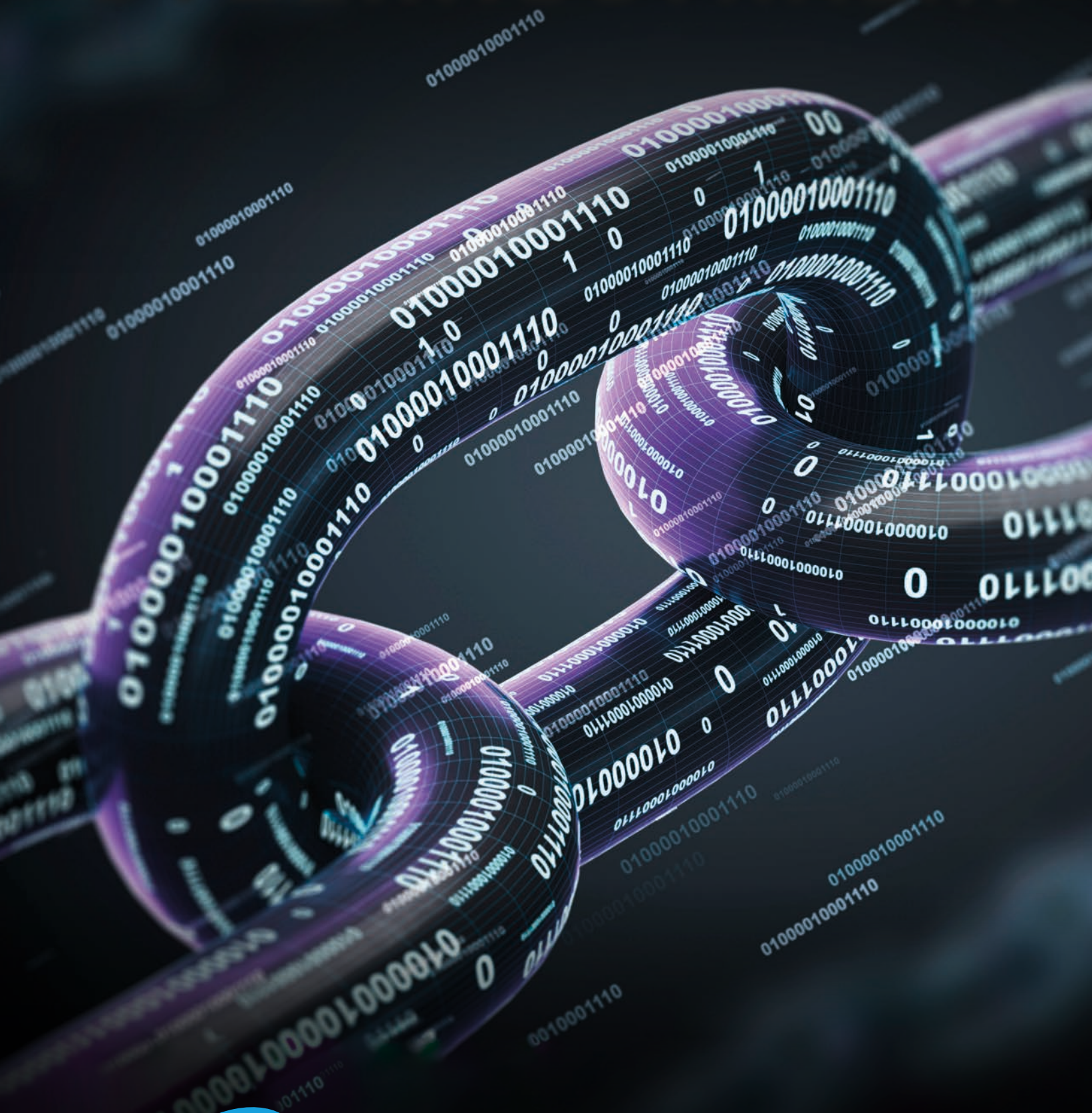


2024-2025

CYBERAUSTRALIA



Australian Cyber Conference



AUSCERT

Allies in Cyber Security

Ask us about our Table Top Exercises!

AUSCERT is proud to offer tabletop exercises (TTXs) as a component of our Governance, Risk, and Compliance (GRC) services. These simulations are designed to test your organisation's preparedness in managing and responding to a variety of incidents. We can design and deliver custom-created TTXs for organisations to suit their specific objectives. Through these exercises, you can identify critical gaps in your incident response plans, ensuring that your team is fully prepared to handle real-world crises.

Key Benefits

**Testing and Validation:**

Safely test and validate incident response plans in a controlled environment.

**Improved Coordination:**

Enhance team communication and role clarity during crises and help manage stress and stay effective in real incidents

**Stakeholder Engagement:**

Emotionally engage executives, driving stronger support for security initiatives.

**Continuous Learning & Development:**

Foster a culture of improvement by treating mistakes as learning opportunities.

**Compliance Readiness:**

Meet regulatory, contractual, and audit requirements.

**Better Decision-Making:**

Sharpen decision-making skills under pressure.

Contact us today for a quote!



+61 (0)7 3365 4417



grc@auscert.org.au



auscert.org.au

FOREWORD

Akash Mittal,
Chair,
Australian Information
Security Association



Akash Mittal

In today's hyper-connected, digital-first world, cyber security has evolved far beyond being merely a technical challenge. It is now a business imperative, a matter of national security, and a foundational requirement for societal trust. As Australia advances its national Cyber Security Strategy, aiming to become a global leader in cyber resilience, trust emerges as the cornerstone for building

a safer digital future. Cyber resilience is now central to business strategies, national policies, and ensuring that citizens can confidently use technology while safeguarding their identities and privacy.

As professionals in this field, our challenge is not only to keep pace with technological advancements, but to actively contribute to building and reinforcing this trust. We are responsible for fostering an environment where cyber security and privacy risks are understood, prioritised, and integrated into decision-making at every level – across government, industry, and the broader community. Achieving this requires strong leadership, ongoing innovation and collaboration. True leadership is demonstrated when we hold our leaders accountable, ensuring that they maintain high standards in their decision-making. As technology evolves, it is our duty to ensure that innovators remain transparent, helping users

understand both the risks and benefits of new developments. We must also, as a community of professionals and individuals, ask critical questions of our governments, organisations, and associations, while consciously reflecting on our own decisions. This approach fosters collaboration, ensures transparency and ultimately builds the trust needed for a more secure digital landscape.

As this edition of *Cyber Australia* explores, the need for collaboration between the public and private sectors, academia, and industry associations has never been greater. Initiatives that advance partnerships and promote knowledge-sharing between businesses, government agencies, and the academic community will be the backbone of our national defence against escalating cyberthreats. The Australian Information Security Association (AISA) remains dedicated to nurturing a collaborative cyber security community through its mission of connecting the industry. As we stand at the crossroads of innovation and security, the importance of collaboration and continuous learning has never been more critical. The Australian Cyber Conference will once again unite visionaries, experts and leaders to share insights, strategies, and advancements that will shape our digital future.

In this edition, you'll discover insights from thought leaders, experts, and practitioners on the front lines of cyber security. Whether you're a seasoned professional or new to the field, I hope these articles inspire you to think critically, innovate with integrity, and, above all, collaborate to strengthen Australia's cyber resilience. ●

CONTENTS

- 1 FOREWORD AKASH MITTAL**
- 4 CYBER SECURITY FOR THE FUTURE: A CALL FOR STRATEGIC BALANCE**
- 6 THE DAY THE EARTH STOOD STILL DAVID BRAUE**
- 10 THE HUMAN RISK MANAGEMENT PLATFORM**
- 12 THE CHALLENGES OF ATTAINING PCI DSS 4.0.1 COMPLIANCE SHANE TULLY**
- 16 THE CYBERTHREAT TO CRITICAL INFRASTRUCTURE JUST GOT WORSE DAVID BRAUE**
- 22 INFLUENTIAL THEMES FOR THE CYBER ARCHITECTURE OF 2030 JODA WALTER**
- 26 SECURITY MATURITY IS NOT A TECHNICAL-ONLY PROBLEM – INVEST IN YOUR PEOPLE**
- 28 EVOLVING TACTICS AND DIRECT PRESSURE STRATEGIES**
- 30 CAN THE GOVERNMENT MAINTAIN ITS CYBER SECURITY MOMENTUM? DAVID BRAUE**
- 34 COUNTDOWN TO QUANTUM**
- 36 INCIDENT RESPONSE FOR AUSTRALIAN COMPANIES – BETWEEN COMPLIANCE AND PRACTICAL CAPABILITIES**
- 38 THE INTERSECTION OF AI AND CYBER SECURITY: IMPLICATIONS FOR CYBER DEFENCE VANNESSA VAN BEEK**
- 41 WORLDS COLLIDE BENJAMIN RILES**
- 44 HOW PRIVILEGE ACCESS MANAGEMENT CAN REINFORCE YOUR CYBER SECURITY POSTURE**
- 46 HOW ANY ORGANISATION CAN GET STARTED WITH CYBERTHREAT INTELLIGENCE CHRIS HORSLEY**
- 48 HOW THREATLOCKER® CAN HELP YOU IMPLEMENT THE ESSENTIAL EIGHT**
- 50 BEYOND THE CONTRACT: THE SILENT KILLER OF YOUR BUSINESS ASRAR ISMAIL**
- 58 THE THREE ‘R’S YOU NEED ON YOUR CYBER SALES RADAR PAUL MALEY AND MEG TAPIA**
- 60 CYBER SECURITY FOR THE CLOUD ERA**
- 62 AGE RESTRICTIONS ON SOCIAL MEDIA KYLE WATERS**
- 64 SECURE AN INCOME WHILE YOU SECURE YOUR FUTURE IN CYBER SECURITY**
- 70 MONEY SEE, MONEY DO: WHY RANSOMWARE ISN’T GOING ANYWHERE DAVID BRAUE**
- 73 UNDERSTANDING AND NAVIGATING GLOBAL CYBER INSURANCE POLICIES AND REGULATIONS IFTEKHAR ALAM**
- 76 THE DIGITAL ID ACT 2024 IS GOOD NEWS FOR AUSTRALIANS!**

- 78 SHORT-TERM MAIL, LONG-TERM RISK**
JAMIESON O'REILLY
- 82 CUTTING THROUGH COMPLEXITY:
ELEVATING SECURITY AND
SIMPLIFYING COMPLIANCE**
- 84 FROM HOODIES TO NATION-STATES:
RETHINKING THE CYBERCRIME
PARADIGM** SABEEN MALIK
- 87 SILVER-TONGUED SWINDLERS USHER
IN A NEW EPOCH OF CYBERCRIME**
DARREN PAULI
- 89 AI SUCCESS RESTS ON SECURE
FOUNDATIONS** MICK DUNNE
- 92 AUSTRALIA'S DIGITAL BATTLEGROUND:
FACING THE SHADOWS OF
CYBER WARFARE**
- 94 AUSCERT NOW OFFERS
TABLETOP EXERCISES AS PART
OF ITS GOVERNANCE, RISK AND
COMPLIANCE SERVICES!**
- 96 TWO YEARS AFTER CHATGPT, THE
GENAI CYBER WARS ARE JUST GETTING
STARTED** DAVID BRAUE
- 99 CYBER SECURITY TRENDS ACROSS
AUSTRALIA** RIKI BLOK
- 101 RESILIENT LEADERSHIP IN
CYBER SECURITY** ROXANNE PASHAEI
- 104 SANS INSTITUTE AUSTRALIA: 25 YEARS
OF STRENGTHENING THE NATION'S
CYBER SECURITY CAPABILITIES**

PUBLISHED BY:



ABN 30 007 224 204

PO Box 256
North Melbourne VIC 3051

Tel: 03 9274 4200

Email: media@executivemedia.com.au
Web: www.executivemedia.com.au

PUBLISHER

David Haratsis
david.haratsis@executivemedia.com.au

EDITOR IN CHIEF

Giulia Heppell
giulia.heppell@executivemedia.com.au

CO-EDITOR

Craig Ford

JOURNALIST

David Braue

David Braue is an award-winning technology journalist who has covered the ICT industry for 25 years. He has written for major technology journals in Australia, the United States and the United Kingdom, and specialises in enterprise technology and its convergence with business strategy. Recent years have seen him nurturing a deep focus on cyber security, privacy, risk management and related issues. Braue earned a Master of Criminology degree from The University of Sydney, where he wrote his thesis on evolving computer crime laws.
www.braue.com

EDITORIAL AND DESIGN TEAM

Eden Cox, Sam Garland, Ruby O'Brien

The editor, publisher, printer and their staff and agents are not responsible for the accuracy or correctness of the text of contributions contained in this publication, or for the consequences of any use made of the products and information referred to in this publication. The editor, publisher, printer and their staff and agents expressly disclaim all liability of whatsoever nature for any consequences arising from any errors or omissions contained within this publication, whether caused to a purchaser of this publication or otherwise. The views expressed in the articles and other material published herein do not necessarily reflect the views of the editor and publisher or their staff or agents. The responsibility for the accuracy of information is that of the individual contributors, and neither the publisher nor editors can accept responsibility for the accuracy of information that is supplied by others. It is impossible for the publisher and editors to ensure that the advertisements and other material herein comply with the Competition and Consumer Act 2010 (Cth). Readers should make their own inquiries in making any decisions, and, where necessary, seek professional advice.

© 2024 Executive Media Pty Ltd. All rights reserved. Reproduction in whole or part without written permission is strictly prohibited.

All stock images sourced from iStock.com.

Vegetable-based inks and recyclable materials are used where possible.

Cyber security for the future: a call for strategic balance

BY SRUJAN TALAKOKKULA, MANAGING DIRECTOR – ANZ, TREND MICRO

IN TODAY'S RAPIDLY evolving digital landscape, cyber security has become both a necessity and a challenge. As businesses accelerate their digital transformation and adopt advanced technologies like artificial intelligence (AI), the need for robust yet balanced security measures has never been more critical. For more than three decades, Trend Micro has been at the forefront of this evolution as a key player in shaping the industry's approach to cyber security.

Cyber security has traditionally oscillated between extremes – either too rigid, stifling business operations, or too lenient, leaving organisations exposed to cyberthreats.

'[Cyber security is] the braking system of a racing car,' Trend Micro's CEO, Eva Chen, the longest-standing cyber security CEO, was quoted in *Forbes*.

This metaphor explains that like the braking system in a race car, where brakes allow a car to accelerate safely, effective cyber security serves as an enabler rather than a barrier, allowing businesses to innovate and grow with confidence.

The widespread adoption of AI and cloud technologies has created countless opportunities for businesses; but, in turn, also introduces new risks posed by the massive technological shifts that these advancements represent.

Trend Micro's recent collaboration with NVIDIA to secure AI-enabled data centres, as well as the development of AI-driven threat-detection tools, highlights the commitment to provide robust security without compromising the agility and innovation that AI brings to the enterprise landscape.

Within this, proactive measures that prioritise transparency, rapid response, and continuous improvement in security protocols are crucial to a robust cyber security strategy. Trend Micro's focus on AI security reflects this philosophy, ensuring that its security solutions remain effective and reliable, even as the technological landscape evolves.

While AI holds immense potential for cyber security as it can democratise access to advanced analytics and automation, it's essential that it is deployed

thoughtfully and securely. Rather than simply developing new models, Trend Micro helps businesses to operationalise their AI application operations by ensuring that their innovations are protected against emerging threats.

Looking to the future, cyber security will require continuous innovation, but it must also be grounded in fundamental principles. Cyber security should not hinder progress, but rather support it. As the industry moves forward, it is critical to rebalance security strategies so they are both robust and supportive of business operations – as Chen recommends, opting for the middle ground to avoid extremes.

By doing so, organisations can confidently navigate the threat landscape of today and tomorrow, ensuring that the core principles of cyber security remain defended as the foundation of digital transformation. ●



Srjuan Talakokkula





Imagine with AI **Secure with Trend**

Discover game-changing strategies for your AI transformation

Managing your cyber risk is fundamental to your business strategy and overall success. Let's help you achieve it. Our AI-powered cybersecurity platform, Trend Vision One™, is designed to help you better understand, communicate, and mitigate cyber risk across your enterprise.





THE DAY THE EARTH STOOD STILL

— BY DAVID BRAUE —

CrowdStrike's global outage was a harsh reminder of the importance of resilience.

It took three hours for the government's national cyber security protection experts to mobilise after CrowdStrike's own goal on 19 July, in which an avoidable mistake in a routine update snowballed into the world's worst-ever technology disaster – creating global chaos as airlines cancelled flights, supermarkets faced furious shoppers, and banks were paralysed.

It was the kind of attack that would normally earn cybercriminals bragging rights, but, in this case, the root cause was completely different. While CrowdStrike CEO George Kurtz was quick to broadcast a global mea culpa, telling people that no, they had not been hacked, fixing the problem proved far more complicated because the bug had rendered affected Windows systems unbootable.

That meant that fixing it was not just a matter of rolling out a new patch, as might otherwise have happened to little more than a few raised eyebrows. In this case, however, as IT teams around the world scrambled to recover, the threat of sustained outages escalated the bug's blast radius to the upper echelons of business and government.

Evaluating the rapidly changing situation was a key goal for the cyber security leaders that convened around a table after the government invoked its National Coordination Mechanism (NCM), an all-hands response plan that has conventionally been used during natural disasters.

In this case, however, the potential for the incident to disrupt Australia's economy warranted rapid action, with newly appointed Minister for Cyber Security Tony Burke telling Parliament that the NCM response – which aligned CrowdStrike representatives, industry leaders, Parliamentarians whose constituents were suffering service blackouts, and a raft of Australian cyber security experts led by newly appointed National Cyber Security Coordinator Lieutenant General Michelle McGuinness – 'brings in who is relevant to each crisis when it happens, gets them all together and starts working it through,

together, through the leadership of the government'. Burke also noted that the group held seven more meetings like this, as the issue played out over the next week or so.

As CISOs the world over activated their disaster response plans to ensure their businesses could continue operating until the problem was resolved, Burke says that the NCM panel 'found ways to deal with the long tail of consequences that stem from an outage of that scale'.

He continued, 'All the systems that had been put in place by my predecessor [Minister Clare O'Neil] were able to be tested, and showed that Australia is far better prepared for cyber attacks than comparable nations.'

PUTTING RESILIENCE TO THE TEST

Cyber security and risk management leaders have been pushing business executives to understand the magnitude of cyber security risk for years. Despite all their preparation – and well-intentioned business continuity and operational resilience plans – the instantaneous outage of more than 8.5 million endpoints posed the unusual opportunity to not only test those recovery mechanisms, but to also appreciate the reality that cybercriminals aren't the only thing that can bring IT infrastructure to its knees.

The problem – which CrowdStrike has detailed for technical and business leaders, and updated over time – occurred after a configuration update to CrowdStrike's Falcon AI endpoint security tool, which was intended to be the latest update to a new threat-sensing capability, known as Channel File 291 and first introduced in February, and which had been updated several times without incident.

Updates to Channel File 291 help it detect new cyber attacks, but the sensor expected that each update would have 20 input fields. Despite being developed and tested according to the standard software development processes, the company admitted that the update on 19 July was released with 21 input fields.

This caused Windows hosts to think that the software was trying to read information outside of its allowable memory space, and forcing them into an unrecoverable 'blue screen of death' crash that turned airport lounges, grocery store check-outs and company offices into a sea of azure.

While CrowdStrike quickly figured out what happened; developed a patch that, according to the company, means the scenario 'is now incapable of recurring'; and went on the front foot to help its customers recover – a process that, since affected Windows machines were unbootable, reportedly required IT staff to physically attend every affected machine in their business – it still took 10 days until around 99 per cent of affected systems were back online.

Despite the severe short-term consequences, many companies found that their well-rehearsed disaster recovery plans helped them get back online quickly;



however, the incident also exposed massive shortcomings in the resilience planning of others, who were caught flat-footed by the incident's scale and impact.

Delta Air Lines, for one, subsequently sued CrowdStrike and Microsoft, claiming that the outage had caused it more than \$750 million (US\$500 million) in lost business after 1.3 million customers were inconvenienced by the cancellation of around 7000 flights in the five days after the incident.

CrowdStrike and Microsoft, however, fought back, pointing out that none of Delta's rivals had needed to cancel even one-tenth as many flights – and suggesting the real reason that Delta was so intensely affected was not only because it had refused repeated offers of assistance from both companies, but that its IT infrastructure was so outdated that it could not readily fix the problem on its own.

LESSONS LEARNT ALL AROUND

Fallout from the incident will continue for some time, but CrowdStrike's assurances that its software development and testing processes are robust fell flat with shareholders – who filed a class action against the company two weeks after the breach. The class action alleges that those assurances were materially false and misleading, and that this had contributed to the 32 per cent fall in value, which wiped \$37 billion (US\$25 billion) from CrowdStrike's value in the 12 days.

Many affected companies went straight to their vendor contracts to see whether they could claim damages from CrowdStrike; however, Transworld Data President Mary E. Shacklett notes that many were disappointed because of fine print that excluded liability for vendors making 'best effort' attempts during disasters or outages – a small consolation since, she



says, only 10–20 per cent of affected companies would be covered by cyber insurance.

If the thought of explaining a service outage to angry shareholders, customers and business partners sends chills down your spine, take this incident as a reminder of the importance of not only implementing business resilience processes, but of also regularly testing and tweaking them.

That's just one of a flood of lessons learnt that cyber security experts have rolled out in the aftermath of the CrowdStrike incident, which, despite its magnitude, isn't the first time a software update caused material issues for companies – nor will it be the last.

Even routine software patches have a 75 per cent chance of breaking production applications, security firm Endor Labs found in its newly released 2024 Dependency Management Report. The report also found that minor software updates can potentially break a client application 94 per cent of the time, and that 95 per cent of version upgrades to software contain 'at least one breaking change'.

Managing these dependencies 'all comes down to effective prioritisation', the firm advises, warning that many companies' software development processes suffer from a 'superficial, or even inaccurate, understanding of how dependencies interact and impact the overall security of the software'.

Companies should also work to regularly check their systems, run comprehensive security reviews, document lingering issues, and evaluate their exposure to single-vendor technology capabilities, such as CrowdStrike's Falcon platform.

'We cannot predict black swan events, but we can very clearly anticipate the implications or consequences of black swan events,' Gartner Distinguished Vice President

and Analyst Leigh McMullen noted in a discussion, as the CrowdStrike incident moved from tactical response to introspection.

These consequences, according to McMullen, 'are fairly finite and fairly understandable, even in the most radical or unforeseeable black swan events – so this is an encouragement for CIOs, their boards, and their CEOs to go back and really take a look at some of the questions around their architecture.'

'While we're all on deck and very much focused on preventing threat actor activity, [the CrowdStrike outage] is just another example of how things can go wrong, with vast and unforeseeable consequences.'

Maryam Bechtel, CISO with electricity giant AGL, agrees, advising CISOs to 'never let a crisis go to waste', and encouraging them to engage closely with business stakeholders to document universally understood cyber security and resilience objectives.

'Agree on the joint goals and targets as an organisation,' she said during this year's Gartner Security & Risk Management Summit, urging CISOs to ask executives: 'What is our organisation's cyber strategy? What is an acceptable level of risk?'

'Agree on those targets together with those stakeholders, [so] you have joint goals, and joint growth, and executives feel like it's not being done to them, but that they're part of the journey.'

In organisations where leaders push back, she said: 'You can also generate your own crisis by doing a red teaming exercise – which, at least, generates a conversation and generates the sense of urgency that something has to be done.'

'Sometimes people just go into complete complacency mode and ask: "Why do we even have to change anything?" Do red teaming, and that will tell them why.' •

The human risk management platform

WHILE ALL USERS need security awareness training and should be mindful of potential cyber attacks, the fact remains that only eight per cent of users cause 80 per cent of security issues. Security teams must properly identify these users and be able to take action.

Organisations tend to invest in disconnected security point products. While some invest in security awareness training, many tend to unwittingly create an environment with security professionals who cannot differentiate risk across employees because they lack the right tools to do so, and frustrated end users who ignore continuous security warnings.

Employees have access to myriad collaboration tools and unlimited access to organisational data, making them prime targets for complex attacks, such as phishing and other forms of business email compromise. In addition, they are constantly multitasking and have multiple tools open at the same time. All of these factors make users more prone to errors, and

traditional security measures often fall short in addressing these human-centric risks.

Traditional security awareness-only measures simulate risk and training engagement, but don't measure real risk. Fortunately, at the time when it is needed most, an evolution of risk mitigation – the human risk management (HRM) platform – is poised to address many of these issues.

A connected HRM platform is built on a central risk engine, and is designed to prevent the evolving and sophisticated threats targeting human error within organisations. The HRM platform offers preventive controls and the ability to take direct actions that mitigate the risk associated with human behaviour, such as clicking a link that downloads malware, opening malicious attachments, or visiting a website with malicious content.

The HRM platform marks an important and eagerly anticipated milestone in advancement toward the next generation of cyber security. In response to customer and market demand for a more effective means of mitigating risk brought on by

human error, the HRM platform will provide unprecedented visibility into an organisation's risk profile, scoring users by risk and allowing CISOs to educate and protect the riskiest part of their employee base.

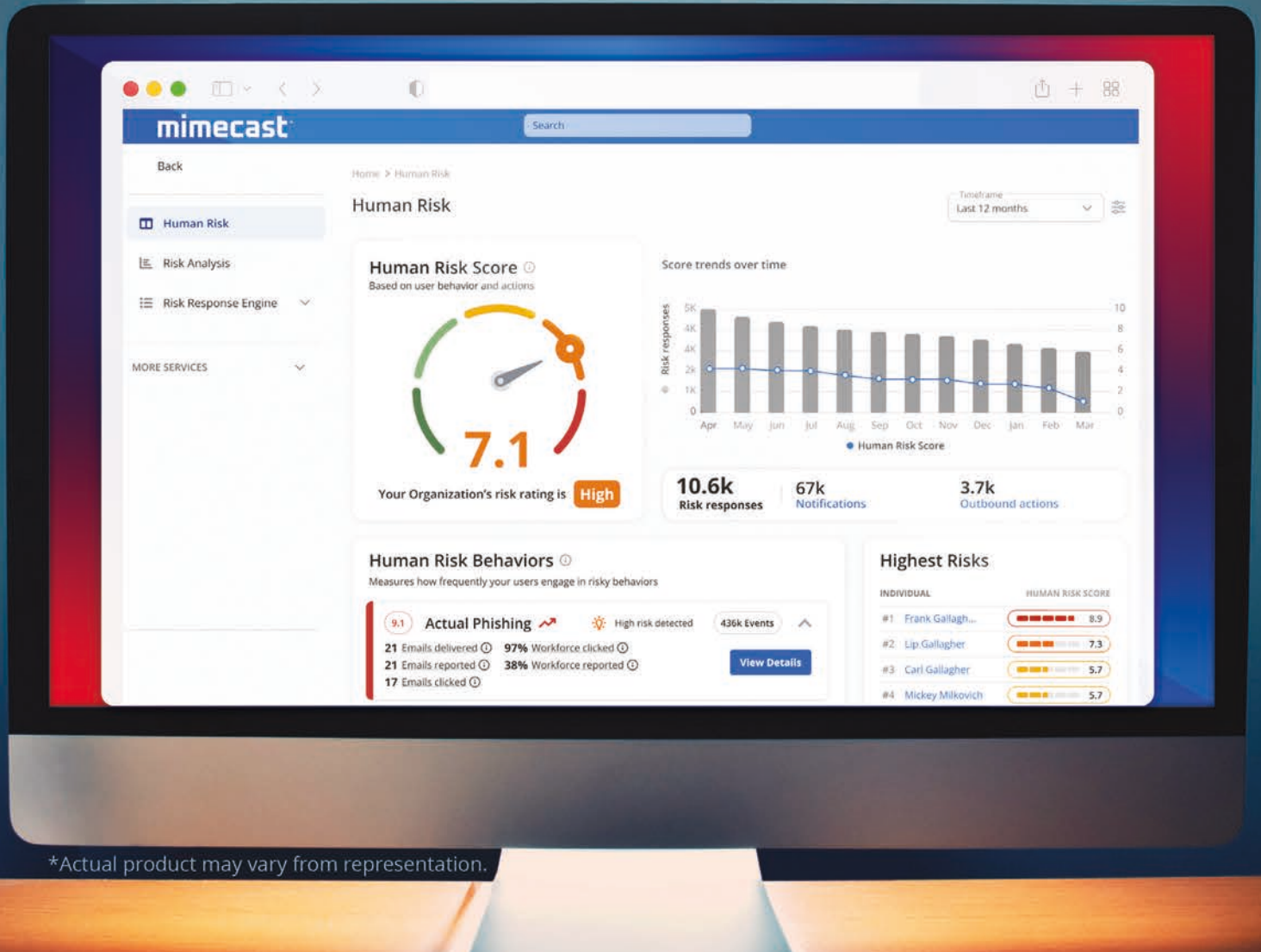
With an HRM platform, security teams can surface and centralise risk signals in the form of a human risk dashboard. This provides security teams with human risk scoring and visibility based on event data from both native metrics, as well as data from third-party tools. A key function of the HRM platform and the human risk dashboard is to integrate findings into an organisation's security awareness training program. This redefines how security leaders can manage human risk.

The HRM platform, the human risk dashboard, and the integration of both with the latest in security awareness products will revolutionise how organisations manage human risk. ●

Visit <https://www.mimecast.com/products/mimecast-engage-awareness-training/> to learn more.



Mimecast is Pioneering Human Risk Management.



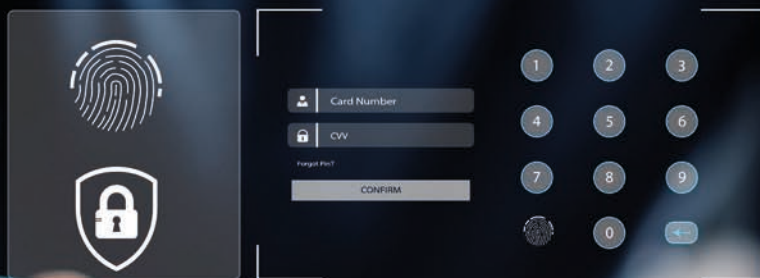
*Actual product may vary from representation.

The Mimecast Human Risk Management Platform and Mimecast Engage technology are the latest innovations in our mission to advance cybersecurity and transform the way organisations manage and mitigate risk.

mimecast[®]

The Connected Human Risk Management Platform

[LEARN MORE AT MIMECAST.COM](https://www.mimecast.com)



The challenges of attaining PCI DSS 4.0.1 compliance

— BY SHANE TULLY, GLOBAL CISO, A24 —

Navigating the transition from Payment Card Industry Data Security Standard 3.2.1.



Shane Tully

The Payment Card Industry Data Security Standard (PCI DSS) is a critical framework designed to protect cardholder data and maintain secure payment environments. Since its inception, PCI DSS has evolved to address emerging threats and technological advancements. The latest version, PCI DSS 4.0.1,

introduces new requirements and updates to the standard, challenging organisations that handle or process payments to reassess and enhance their security postures so that customers have an embedded assurance of trust in the organisation's payments ecosystem.

This article explores the key challenges in transitioning from PCI DSS 3.2.1 to PCI DSS 4.0.1, the risks for organisations that delay compliance, insights into the new requirements, potential pitfalls, and the steps needed to achieve PCI DSS 4.0.1 certification.

THE TRANSITION FROM PCI DSS 3.2.1 TO PCI DSS 4.0.1: A COMPLEX UNDERTAKING

Transitioning from PCI DSS 3.2.1 to 4.0.1 is more than just an upgrade; it requires a comprehensive evaluation of an organisation's entire payment-processing environment. The following factors make this transition particularly challenging.

Increased flexibility and complexity

PCI DSS 4.0.1 introduces a more flexible approach to achieving compliance, allowing organisations to tailor their security controls to better fit their specific

environments. This shift, while beneficial, also adds complexity, as organisations must now demonstrate that their custom controls meet the intent of the standard. For many, this means developing a deep understanding of the security objectives behind each requirement, and providing detailed documentation to support their chosen implementations.

Expanded scope and stringent requirements

The scope of PCI DSS 4.0.1 has expanded to include a broader range of security considerations. For instance, the new version emphasises the importance of continuous security monitoring and the use of encryption across all channels. These additions mean that organisations must reassess their entire payment ecosystem, potentially bringing more systems, processes and third-party vendors under the compliance umbrella.

Organisational readiness

Many organisations have established compliance processes based on PCI DSS 3.2.1. The transition to 4.0.1 requires not just technical adjustments, but also changes to governance, risk management and compliance frameworks. Organisations need to invest time and resources in retraining their staff, updating policies and procedures, and ensuring that all stakeholders understand the new requirements.

THE RISKS OF NONCOMPLIANCE: WHAT'S AT STAKE?

Failing to achieve PCI DSS 4.0.1 compliance exposes organisations to a range of risks, each with potentially severe consequences.

Data breaches and financial loss

Noncompliance with PCI DSS can result in significant security vulnerabilities, making organisations prime targets for cyber attacks. Data breaches involving payment card information can lead to massive financial losses, including fines, penalties and the costs associated with breach remediation. Additionally, compromised organisations may face costly lawsuits and lose revenue due to damaged customer trust.

Reputational damage

In today's digital age, consumers are increasingly concerned about data privacy and security. A failure to comply with PCI DSS 4.0.1 can result in reputational damage that is difficult to repair. Customers and partners may lose confidence in an organisation's ability to protect sensitive data, leading to lost business opportunities and long-term harm to brand reputation.

Legal and regulatory consequences

PCI DSS is a mandatory standard for organisations that process, store or transmit payment card data. Noncompliance can lead to significant legal and regulatory consequences, including fines from payment card networks, increased scrutiny from regulatory bodies, and potential loss of the ability to process payment cards. In some cases, organisations may be required to undergo more frequent and invasive audits, further straining resources.

INSIGHTS ON PCI DSS 4.0.1 REQUIREMENTS: WHAT'S NEW?

Understanding the new PCI DSS 4.0.1 requirements is essential for achieving compliance. Some of the most notable changes include:

Emphasis on risk-based approaches

PCI DSS 4.0.1 introduces a greater emphasis on risk-based approaches to security. Organisations are now encouraged to assess their unique risk profiles, and implement controls that address specific threats and vulnerabilities. This shift allows for more customised security strategies, but also requires organisations to conduct thorough risk assessments and justify their control decisions.

Enhanced authentication requirements

The new version places a stronger focus on authentication, including multi-factor authentication (MFA) for all access to the cardholder data environment (CDE). This enhancement aims to mitigate the risk of unauthorised access by ensuring that only verified users can interact with sensitive data. Organisations must evaluate their current authentication mechanisms and upgrade to MFA where necessary.

Continuous monitoring and testing

PCI DSS 4.0.1 highlights the importance of continuous security monitoring and regular testing of security controls. This includes the implementation of security information and event management systems, real-time monitoring of network traffic, and frequent penetration testing. These requirements are designed to ensure that organisations can detect and respond to security incidents promptly.

Encryption and data protection

Encryption requirements have been strengthened in PCI DSS 4.0.1, with a focus on encrypting data across all transmission channels, not just within the CDE. Organisations must ensure that encryption is applied consistently, and that encryption keys are managed securely. This change aims to protect cardholder data throughout its life cycle, reducing the risk of data breaches.

Vendor management and third-party risk

Third-party risk management is a critical aspect of PCI DSS 4.0.1. The new version requires organisations to assess and manage the security practices of their vendors, particularly those that handle payment card data. This includes ensuring that third parties comply with PCI DSS requirements, and that any risks associated with outsourcing are adequately mitigated.

PITFALLS TO AVOID IN THE COMPLIANCE JOURNEY

Achieving PCI DSS 4.0.1 compliance is a complex and challenging process. Organisations must be aware of common pitfalls that can derail their efforts, such as:

Underestimating the scope of the changes

One of the biggest mistakes that organisations can make is underestimating the scope of changes required to achieve PCI DSS 4.0.1 compliance. The new version introduces several new requirements and expands the scope of existing ones, making it essential for organisations to conduct a thorough gap analysis. Failing to identify all areas that need updating can lead to incomplete compliance efforts and potential security gaps.

Inadequate planning and resource allocation

Compliance with PCI DSS 4.0.1 requires significant planning and resource allocation. Organisations that fail to allocate sufficient time, budget and personnel to the compliance effort risk falling behind schedule or missing critical requirements. A lack of proper planning can also lead to rushed implementations, increasing the likelihood of errors and vulnerabilities.

Over-reliance on automation

While automation can streamline many aspects of compliance, over-reliance on automated tools can be

a pitfall. Compliance with PCI DSS 4.0.1 involves not just technical controls, but it also involves policy updates, staff training and ongoing risk management. Organisations that rely too heavily on automation may overlook the need for human oversight, leading to gaps in compliance.

Neglecting third-party risks

Third-party vendors play a crucial role in many organisations' payment processing ecosystems; however, failing to adequately assess and manage third-party risks can undermine compliance efforts. Organisations must ensure that all third-party vendors handling payment card data comply with PCI DSS 4.0.1, and that they have robust security controls in place.

Inconsistent documentation and evidence collection

Documentation and evidence collection are critical components of PCI DSS 4.0.1 compliance.

Organisations that do not consistently document their processes and collect evidence of compliance risk facing challenges during audits. Incomplete or inaccurate documentation can result in audit failures and the need for costly remediation efforts.

PREPARING FOR PCI DSS 4.0.1 CERTIFICATION: A STEP-BY-STEP APPROACH

Achieving PCI DSS 4.0.1 certification requires a methodical approach, involving several key steps.

1. Conduct a gap analysis

The first step in preparing for PCI DSS 4.0.1 certification is to conduct a comprehensive gap analysis. This involves comparing your current security posture against the new requirements of PCI DSS 4.0.1 and identifying areas where your organisation falls short. A gap analysis provides a road map for the changes that need to be made, and helps prioritise compliance efforts.

2. Update policies and procedures

Based on the findings of the gap analysis, organisations should update their policies and procedures to align with PCI DSS 4.0.1. This includes revising access control policies, incident response plans, and data protection procedures. Ensuring that policies are up to date and reflect the latest requirements is crucial for achieving compliance.

3. Implement technical controls

Technical controls play a vital role in PCI DSS 4.0.1 compliance. Organisations must ensure that all systems within the scope of the standard are properly secured. This includes implementing MFA, encryption, continuous monitoring, and other required security measures. Testing these controls regularly is essential to ensure that they are functioning as intended.

4. Engage stakeholders and provide training

Achieving PCI DSS 4.0.1 compliance is not only the responsibility of the IT or security teams; it also requires the involvement of all relevant stakeholders. Organisations should engage their employees, management and third-party vendors in the compliance process. Providing training on the new requirements and the importance of PCI DSS compliance helps to ensure that everyone is aligned and aware of their roles and responsibilities.

5. Conduct internal assessments

Before undergoing a formal PCI DSS 4.0.1 audit, organisations should conduct internal assessments to evaluate their compliance status. Internal assessments help to identify any remaining gaps, and provide an opportunity to address issues before the formal audit. These assessments should be thorough and involve a review of all policies, procedures, and technical controls.

6. Select a qualified security assessor

When the organisation is ready for certification, selecting a qualified security assessor (QSA) is a critical step. The QSA will conduct the formal audit and determine whether the organisation meets the requirements of PCI DSS 4.0.1. Choosing a QSA with experience and expertise in the payments industry is essential for a smooth and successful audit process.

7. Prepare for continuous compliance

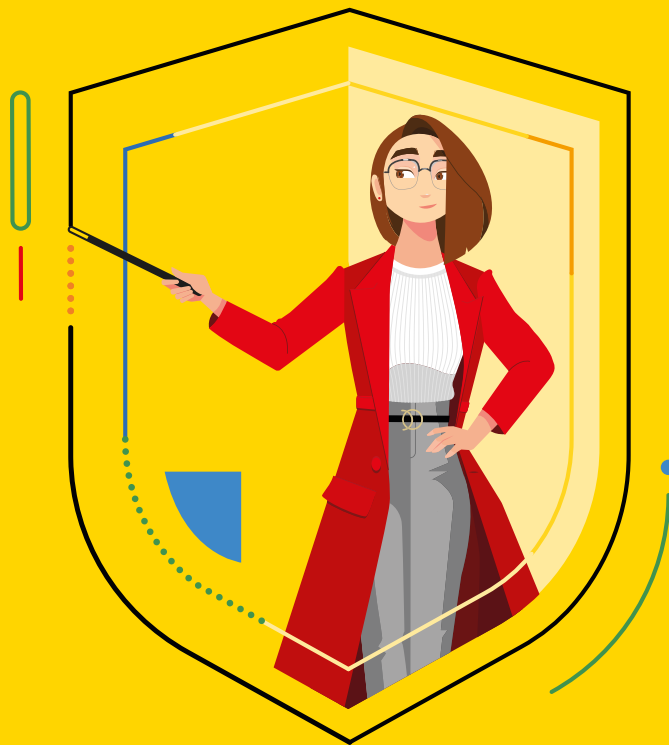
PCI DSS compliance is not a one-time achievement; it requires ongoing effort. After achieving PCI DSS 4.0.1 certification, organisations must maintain their compliance posture by continuously monitoring and testing their security controls, updating policies and procedures as needed, and staying informed about any changes to the standard. Continuous compliance ensures that the organisation remains secure and avoids the risks associated with noncompliance.

OBSERVATIONS AND CONCLUSION

The transition from PCI DSS 3.2.1 to PCI DSS 4.0.1 presents significant challenges, but it is also an opportunity for organisations to enhance their security postures and protect sensitive payment card data. By understanding the new requirements, avoiding common pitfalls and taking a methodical approach to compliance, organisations can successfully achieve PCI DSS 4.0.1 certification. Starting the compliance journey early and engaging all stakeholders in the process is key to navigating the complexities of this transition and ensuring long-term success in a rapidly evolving threat landscape. ●

Cybersecurity solutions for your digital enterprise

Protect your business from internal and external threats with ManageEngine's IT security solutions.



ManageEngine

Our solutions

Cloud security for enterprise IT | Endpoint security | Network security | Identity and access management | Data security | Security information and event management
Privileged access management

cybersecurity.manageengine.com

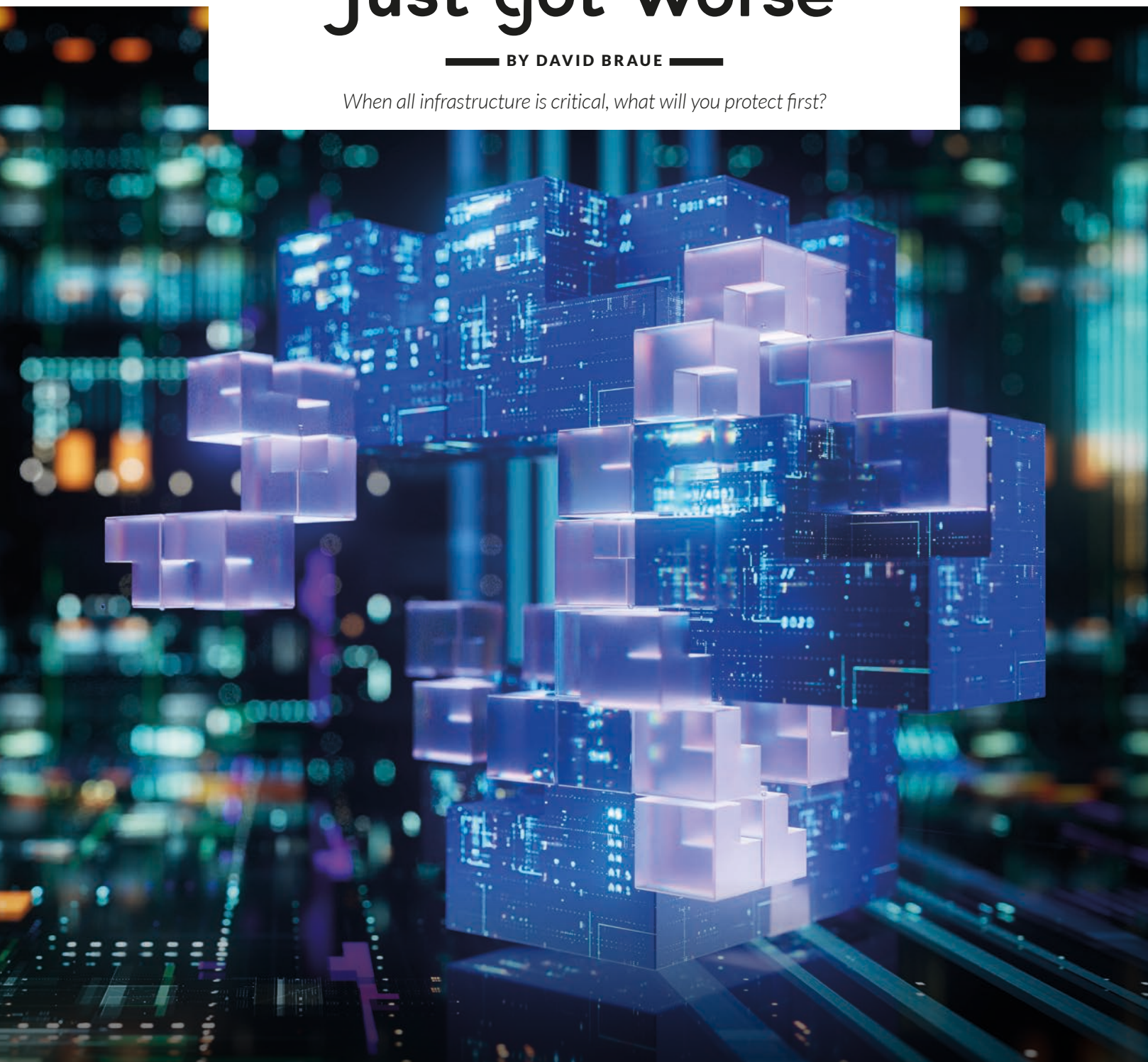
Find ManageEngine at booth 147

ManageEngine is a division of Zoho Corp.

The cyberthreat to critical infrastructure just got worse

— BY DAVID BRAUE —

When all infrastructure is critical, what will you protect first?



As if CISOs' jobs weren't already hard enough, dealing with the idiosyncrasies of legacy security technologies – or, in the case of many critical infrastructure industrial control systems (ICS), no security technologies at all – calls to implement newly finalised post-quantum computing (PQC) encryption standards have added yet another layer of urgency.

In progress since 2016 and released in their final form by the US National Institute of Standards and Technology (NIST) in August, the three new standards – ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) – replace widely used public-key cryptography standards that will – mathematicians have proven and security specialists readily admit – be rendered useless once powerful enough quantum computers are available.

Engineers once believed that point was still decades away, but given the recent signing of contracts to build commercial-scale cryptographically relevant quantum computers (CRQCs) in the next few years – PsiQuantum, for one, has been engaged to deliver fault-tolerant, one-million-qubit machines in Brisbane by 2027 and Chicago the year after – timeframes have moved up considerably.

Once the massively parallel computing power of CRQCs are readily available, as the Australian Signals Directorate has previously warned, the systems 'will render most contemporary public-key cryptography insecure' because they will be able to brute-force the encryption keys – whose security is based on the massive amount of time needed for contemporary computers to find prime factors of extremely large numbers – in hours rather than millennia.

With the long-discussed arrival of 'Q-Day' will come a very real problem for every security executive: if the security of your data – or of the systems managing the critical infrastructure you rely on – relies on today's public-key encryption, the fundamental security controls of your business will be blown right open.

Little wonder, then, that PQC Standardization Project Head and NIST Mathematician Dustin Moody advised systems administrators to start integrating the new encryption standards 'immediately, because full integration will take time'.

CRITICAL INFRASTRUCTURE SECURITY IS ALREADY CRITICAL

For systems administrators that have waved away the vague threat of Q-Day – or, worse still, hadn't considered it at all – the looming timeline is sure to be an unwelcome reminder that data and systems security has never been more important.

The average number of weekly cyber attacks against utility providers has quadrupled since 2020 and doubled

during 2023 alone, according to a KnowBe4's recent Phishing By Industry Benchmarking Report, which observed a 30 per cent increase – to 420 million attacks last year alone – against critical infrastructure targets.

Despite this surge, KnowBe4 warned that the number of vulnerable points in United States power grids is still growing by around 60 per day – from 21,000 in 2022 to nearly 24,000 today – as increasingly interconnected businesses increase their exposure.

With Internet of Things (IoT) security specialist Claroty recently warning that 38 per cent of cyber-physical systems are overlooked by traditional management tools that leave 'blind spots', businesses are vulnerable to exploits they often didn't even know they had. In July, for example, security firm Dragos uncovered new malware called FrostyGoop, which exploits the widely used Modbus protocol that's common in ICS environments to send disruptive commands that can bring systems in those environments to their knees.

FrostyGoop, which Dragos says is the ninth ICS-specific malware uncovered to date, has been blamed for a recent attack on a Ukrainian energy company that caused over 600 apartment buildings to lose heating for two days when the malware was used to send Modbus commands that caused inaccurate measurements and system malfunctions.

'The adversary exploited unsecured network points and inadequately protected systems,' the security firm noted, warning that 'given the ubiquity of the Modbus protocol in industrial environments, this malware can potentially cause disruptions across all industrial sectors by interacting with legacy and modern systems'.

Indeed, the ongoing Ukraine–Russia conflict has proven to be a turning point in critical infrastructure attacks, with both sides' offensive cyber security teams working to take down enemy infrastructure.

Russia, in particular, has notched up success after success through attacks like the one in April, when its intelligence-linked 'Sandworm' group, also known as APT44, triggered rolling blackouts in Ukraine after it targeted 20 energy facilities' control systems with malware like Kapeka, GOSSIPFLOW, KnuckleTouch, ICYWELL and Wrongsens, as well as previously unseen derivatives like LOADGRIP and BIASBOAT.

The cybercriminals used the compromised ICS systems 'for horizontal movement and development of cyber attacks in relation to corporate networks of enterprises', the Computer Emergency Response Team of Ukraine (CERT-UA) reported in its analysis of the attacks, in which it said at least three supply chains had been compromised.

CERT-UA's analysis noted a range of factors that enabled the critical infrastructure to be targeted – including 'incorrect segmentation' that left critical control systems insecurely connected to the internet, and 'negligent attitude of suppliers to the security of software

provided to consumers’, including ‘banal’ remote code execution vulnerabilities.

AUSTRALIA PUTS CRITICAL INFRASTRUCTURE OPERATORS ON NOTICE

The ongoing cyber war between Ukraine and Russia has been a vindication for security experts who were already warning about the risks of poor critical infrastructure security when the Stuxnet worm was discovered manipulating Iran’s nuclear fuel enrichment equipment in 2010.

Authorities in Australia – who stopped alluding to cyberthreats from unnamed overseas governments years ago, and now openly names China and PRC-backed groups as threats to Australia’s critical infrastructure – have been ramping up their engagement with a broad range of local businesses as they seek to harden domestic water, electricity, gas, data centres, transportation, financial services, and other types of infrastructure.

As well as passing laws expanding the definition of ‘critical infrastructure’ to 11 industries from four, and imposing requirements such as a 12-hour reporting mandate when attacks are discovered, the government has run outreach to the sectors through programs like the Australian Cyber Security Centre’s Critical Infrastructure Uplift, part of its nearly \$10-billion REDSPICE cyber security investment.

As the ongoing exposure of ICS infrastructure has demonstrated, cybercriminal groups will leverage any foothold they can gain in target organisations’ IT systems – even the network equipment itself, as was demonstrated all too clearly when the FBI recently led a global take-down of a 260,000-strong botnet managed by Chinese cybercriminal group Flax Typhoon.

It was the second take-down of a Chinese Government-sponsored botnet this year – the other being a Volt Typhoon botnet that was disrupted in January – and this one had reportedly compromised 2400 IoT devices in Australia alone, using a complex and distributed command and control infrastructure to force them to participate in data exfiltration, distributed denial of service attacks, and more.

Botnets have become a major problem for businesses, with a recent Imperva report finding that Australian businesses are losing an estimated \$2.94 billion annually to automated attacks and insecure application programming interfaces, with 24 per cent of all attacks found to be bot related.

One victim of the Flax Typhoon botnet ‘suffered an all-hands-on-deck cyber security incident that ... took swathes of the organisation offline and caused a significant financial loss’, FBI Director Christopher

Wray said, illustrating that such compromises pose a significant risk to all companies.

‘Cybercriminals and nation-state hackers alike have demonstrated that they’re not only willing, but more and more able to hit the services people really cannot live without, like hospitals and schools,’ Wray said at the recent 2024 Aspen Cyber Summit, admitting that ‘given the ubiquity and the severity of the cyberthreat, it can sometimes seem like the odds are stacked against us’.

Over the past three years, he said, 15 of the United States’ 16 declared critical infrastructure sectors had been hit by ransomware. ‘Criminals and hackers backed by nation-states know they can store big,’ he explained, ‘by 1) locking up your data until you pay an outrageous ransom; 2) conducting double extortion [by] stealing your data and then threatening to release it or sell it to the highest bidder; and 3) conducting triple extortion by preventing access to your website through denial of service attacks’.

That’s a well-worn playbook – and one that continues to help cybercriminals extort billions of dollars annually from a who’s who of businesses – and it should, experience has shown, send shivers down your spine.

Whether your company carries formal cyber security obligations under recent legislation or not, the experience of the many unlucky companies to date is a reminder that you can’t be too progressive, or too worried, about working to shore up your defences.

The SANS Institute’s Five ICS Cybersecurity Critical Controls guidelines offer a framework for companies seeking to audit and reduce their exposure – with core capabilities including ICS incident response, defensible architectures, ICS network visibility monitoring, secure remote access, and risk-based vulnerability management.

Just how hard it is to meet these ideals will depend on how mature your environment is and what resources you have available. But as you work through the process, remember that cybercriminals aren’t working in a vacuum either – just as they have rapidly embraced generative artificial intelligence to improve their cyber attacks, the coming quantum computing technology will once again prove game changing, particularly as it becomes available to all on an as-a-service basis.

And if you’re not ready when it comes, whatever protections you’ve put on your critical infrastructure will be for naught.

‘Quantum computing technology could become a force for solving many of society’s most intractable problems,’ NIST Director Laurie E. Locascio said, calling the new standards ‘the capstone of NIST’s efforts to safeguard our confidential electronic information ... ensuring it will not simultaneously disrupt our security’. ●



PROUD SPONSORS OF CYBERCON

TAKE COMMAND OF YOUR ATTACK SURFACE FROM ENDPOINT TO CLOUD

Visit us at
**BOOTH
79**

Ask for a demo

Ask for a live demo and witness the power of Rapid7 in action.
Our experts can showcase the following:



MDR with Unlimited Incident Response

Gain 24/7 XDR monitoring, remediation
and DFIR from SOC experts



Vulnerability Management

Understand risks across hybrid
environments



Next-Gen SIEM

Pinpoint threats where they start with
cloud-first detection and response



Threat Intelligence

Discover and remediate
external threats



Cloud Security

Secure multi-cloud environments with
complete visibility



Exposure Management

Get continuous assessment and
validation of your attack surface

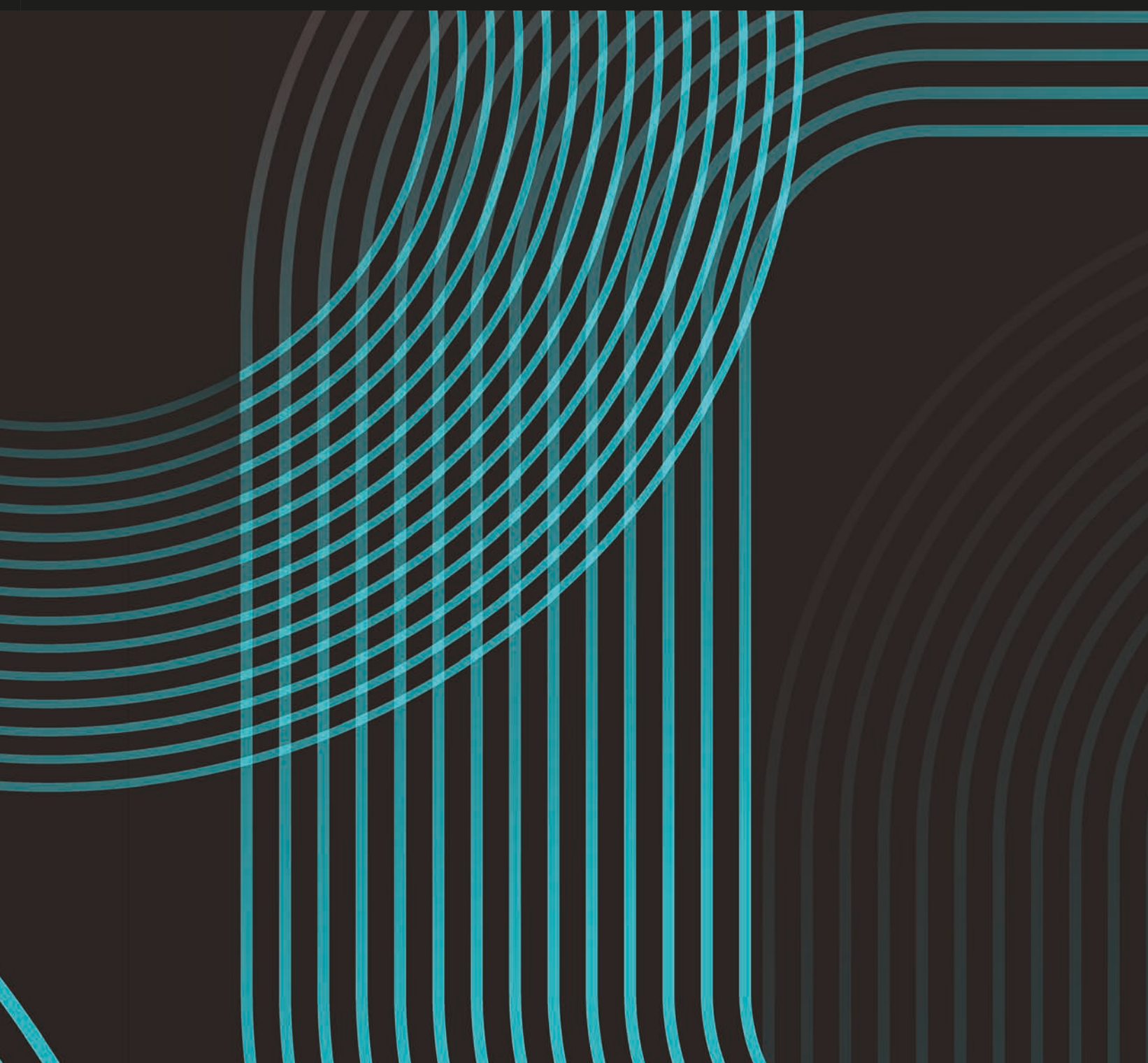
THE FUTURE IS CALLING...

IS YOUR INTELLECTUAL PROPERTY

QUANTUM SAFE?

Following NIST's publication of the first standards for Post-Quantum Cryptographic (PQC) Algorithms, the race is on for Australian organisations to migrate to a quantum-safe stance ahead of Y2Q.

Visit senetas.com to start preparing a comprehensive solution for this essential quantum shift.



INFLUENTIAL THEMES FOR THE CYBER ARCHITECTURE OF 2030

— BY JODA WALTER, SENIOR EXECUTIVE AND CYBER SPECIALIST —

The world of the future will be very different.

The proliferation of generative artificial intelligence (AI) has ushered in a wave of new investments, propelling the world's leading governments and technology companies into an AI arms race. The key to success in this domain lies in computational power and mathematical prowess. As of now, the H100 NVIDIA Graphics Processing Unit stands as the market leader, priced at \$25,000 per unit – if one can even secure a purchase.

META is at the forefront of the physical hardware race, boasting the equivalent of 600,000 units. Concurrently, global internet speeds are rapidly increasing due to advancements in fibre-optic cable infrastructure, laser technology optimisations, and the proliferation of low-Earth-orbit satellites. These developments enable systems like Starlink to provide wireless internet access virtually anywhere on Earth.

Cloud data centres are expanding, with a new category emerging, known as the 'AI factory'. These centres are hubs of large AI processing capacity, optimised for the infrastructure-as-a-service, platform-as-a-service and software-as-a-service models of the future.

The next large change in the world's computing environment will be the advent of quantum computing, which is just on the horizon.

Estimates suggest that approximately 2000–5000^{1,2} quantum computers will exist by 2030, primarily in the hands of top tech companies and governments. While the first quantum computing killer app has yet to be developed, it is known that the computer architecture will be immensely powerful for solving two complex mathematical problems that underpin modern asymmetric encryption: integer factorisation and discrete logarithms (clock arithmetic).

Unfortunately, this means that quantum computers will excel at using the Shor's and Grover's algorithms to break any asymmetric encryption relying on these processes. Consequently, current transport layer security (TLS) and public-key infrastructure (PKI) implementations will no longer be fit for purpose unless we replace their asymmetric cryptography components with post-quantum-resistant ones (PQR algorithms). This includes RSA encryption, Diffie–Hellman key exchange and elliptic-curve cryptography.

Combined, these technology changes present some opportunities, complications and challenges for the future of technology design thinking.

Let's focus on the quantum computing component. The first quantum 'killer app' may be an app killer.

Any application running non-quantum-resistant encryption that stores personally identifiable information will experience a mass exodus of users and/or encounter legal issues, as it will be unable to meet its obligations under various global data privacy laws. This could mean that we see large clusters of app store offerings taken

offline en masse. Future apps will therefore need to be designed with PQR algorithms protecting them and their infrastructure.

Furthermore, our non-repudiation methods, which are designed to eliminate doubt or denial surrounding an individual's or entity's participation in a transaction or communication, will no longer be effective with current technology. A multitude of security packages and frameworks will need to be modified and upgraded to resolve this.



Joda Walter

Estimates suggest that approximately 2000–5000, quantum computers will exist by 2030, primarily in the hands of top tech companies and governments. While the first quantum computing killer app has yet to be developed, it is known that the computer architecture will be immensely powerful for solving two complex mathematical problems that underpin modern asymmetric encryption...

If you're thinking that you can simply increase the bit size on your digital certificates and that this will act as a temporary countermeasure, you would be incorrect. The certificate protocols will start to fail as the computer chips in your hardware struggle with the computational power required to process the instructions. Even if you could increase it, the additional protection is insignificant compared to the outlay in time, money and personnel.

This means transitioning to encryption that quantum computers cannot easily crack will likely necessitate substantial software and, in many cases, hardware upgrades across enterprise computing environments.

This raises the following questions:

- › Will this extend to personal and smart devices?
- › Will export restrictions on arms limit proprietary implementations or PQR algorithms to certain parts of the world and, consequently, rearchitect the internet?
- › Will this lead to a Balkanisation of the internet, with a poorly encrypted section alongside an appropriately encrypted arterial component with compartmentalised segments?

- › Will international internet gateways only terminate PQR traffic from known proprietary technology in geo-restricted locations, and not accept traffic from untrusted zones? Untrusted zones may not be provided with the technology to connect with a PQR gateway (at least initially).

In any case, it is evident that the physical infrastructure of enterprise and global computing is undergoing a transformation at scale. This evolution presents new challenges and opportunities for security and intelligence professionals.

Enormous AI computing power will be capable of tailoring a virtual reality around us in real time in staggering high definition. In the wrong hands, this has large implications for disinformation, misinformation, deepfakes and social engineering attacks

Enormous AI computing power will be capable of tailoring a virtual reality around us in real time in staggering high definition. In the wrong hands, this has large implications for disinformation, misinformation, deepfakes and social engineering attacks.

Quantum computing will be able to simulate, trial and synthesise medicine, materials and crack encryption like the cyber equivalent of a hypersonic missile on the modern battlefield.

It is important to note that just because the first application is the application killer, it does not mean we will be aware of it.

The first corporation or government to achieve this breakthrough does not need to announce that it has tapped or acquired restricted encrypted data. Instead, it can decrypt the data in a separate computing environment and integrate it into any models with utility for the dataset.

Will we see new, large data honey pots deployed as standard countermeasures to stifle the decryption and AI learning of our adversaries or competitors?

With these combined technologies, complex digital transactions could possibly be cloned or faked in new ways. This raises another critical question: If current non-repudiation technologies, asymmetric encryption and AI-driven information interfaces are at risk, will this undermine the utility of online systems?

The answer is no, but it does imply that cyber security will need to evolve to remain effective. Perhaps it will need to become more cyber physical. Cyber-physical systems are integrations of computation with physical processes.

Some modern smartphones have incorporated light detection and ranging (LiDAR) technology, which can create 3D renders of objects in near real time. If a digital transaction can be faked with AI and quantum computing, then a smartphone with a PQR-resistant signature comprising metadata and a real-time LiDAR scan of the person making it may be a viable defence. This would be a cyber-physical representation of the real-world action protected with quantum-resistant encryption.

If traditional TLS standards are easily cracked by quantum computers (we now know that PQR algorithms will need to replace them), will different physical silicon processing chips be required to handle the performance requirements in a range of systems? Perhaps.

If PKI systems, internet gateway, wide-area network and local area network infrastructure need to handle PQR algorithms, will their performance and security be adequate without physical changes to upgrade their processing chips? I have doubts in many cases.

The good news is that the US National Institute of Standards and Technology has published standards on the first set of PQR algorithms³, and the Australian Cyber Security Centre has guidance on how organisations can plan for post-quantum computing cryptography⁴.

Whatever the solutions may be, an enormous effort will be required across the cyber and technology industry to upgrade the systems we rely on, and a new set of design thinking will be required to maintain the cyber-enabled systems we all love. If we are to maintain the confidentiality, integrity and availability of the modern digital world, we need to mobilise – and fast.

In the words of Winston Churchill: ‘The era of procrastination, of half-measures, of soothing and baffling expedients, of delays is coming to its close. In its place, we are entering a period of consequences.’ ●

Joda Walter is a recognised cyber security expert with extensive experience in large organisational settings. He specialises in leadership, strategy, program management, emerging technology, governance, risk and compliance, enterprise security architecture, policy, AI security, and ICT auditing. Walter has sponsored or played leading roles in numerous high-profile ICT programs with large cyber focuses, including cyber programs, data centre and internet gateway migrations, big data AI and machine learning cloud platform deployments, and Microsoft 365 and ServiceNow service integration and management implementations.

References

1. *Quantum computing: What leaders need to know now* | MIT Sloan
2. *A game plan for quantum computing* | McKinsey
3. <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>
4. *Planning for Post-Quantum Cryptography* | Cyber.gov.au

UNLOCK YOUR CYBERSECURITY POTENTIAL



Map your journey to increased maturity with the ultimate integrated security management platform



Ready to move the needle?
BOOK A DEMO



go.myciso.co/cyberaus

Security maturity is not a technical-only problem – invest in your people

BY JEREMY DALY, CYBER SECURITY LEAD; LOUIS CREMEN, LEAD CYBER SECURITY INSTRUCTOR; AND CHRIS EVANS, CYBER SECURITY INSTRUCTOR, LUMIFY WORK, FORMERLY DDLS

BY DEVELOPING THE skills of your people, you can significantly elevate how your organisation approaches security – not only to manage current changes, but to also anticipate and adapt to the future in the ever-evolving landscape of cyber security.

With technology constantly changing, cyberthreats are becoming increasingly sophisticated; they no longer distinguish target organisations by size and industry.

Cyber security and cyber security maturity are not technical-only problems. We need people who can improve cyber security maturity from the top down. We need people who can develop, build and deliver a cyber security strategy that meets the objectives of an organisation.

We need security professionals who can successfully liaise with different business units, and communicate threat and risk impacts in a way that the business understands. This ensures that suitable mitigation measures are in place. To do this effectively, companies must elevate their cyber security maturity to stay one step ahead. The best way to start

is to invest and train your people in the key skills outlined below.

RISK MANAGEMENT

Measuring the efficiency and effectiveness of the current cyber security strategy is often performed from a risk perspective. There needs to be an executive decision to accept, avoid, transfer, or (as a best practice) reduce or mitigate the deemed risk. Professionals must then learn to identify, assess and prioritise potential threats based on their impact and probability. They should know how to create and implement strategies to mitigate identified risks and efficiently allocate resources to protect critical assets.

SECURITY ARCHITECTURE AND DESIGN

Designing robust security architecture is fundamental to a proactive cyber security strategy. Professionals need a deep understanding of how to integrate security controls into networks and systems. They must be skilled in implementing measures like firewalls,

intrusion-detection systems and encryption protocols.

THREAT INTELLIGENCE ANALYSIS

Staying ahead of cyberthreats requires continuous monitoring and analysis. Skills in threat intelligence involve gathering and interpreting data on emerging threats and vulnerabilities. Analysts use these to anticipate and prepare for potential attacks, so it's essential to know the latest attack vectors, tactics and trends.

COMPLIANCE AND GOVERNANCE

Adherence to relevant regulations is crucial. Professionals must be well-versed in Australian legal requirements, industry standards and best practice to ensure that the company meets obligations under local laws. Through internal policies and tools for endpoint detection and response, businesses can maintain compliance, safeguard against regulatory risks, and enhance their overall cyber security posture.

SECURITY AWARENESS TRAINING

Human error remains one of the leading causes of security breaches. The 17th annual Data Breach Investigations Report by Verizon Business found that 68 per cent of breaches involve a non-malicious human element. Organisations need to invest in educating employees about cyberthreats, safe practices, and how to recognise phishing attempts or other malicious activities.

Ultimately, every organisation will differ in its security maturity; however, what remains true is that an over-reliance on technology solutions to fix people and process problems will continue when there is little to no value placed on the education and training of people. •

Jeremy Daly





Formerly known as DDLs

Elevate your Organisation's Cyber Security Maturity

Access training designed with leading associations and delivered with the latest official course materials by award-winning local trainers.



Exclusive Offer

Get 20% off our Cyber Security courses*. **Scan here!**



GOLD PARTNER

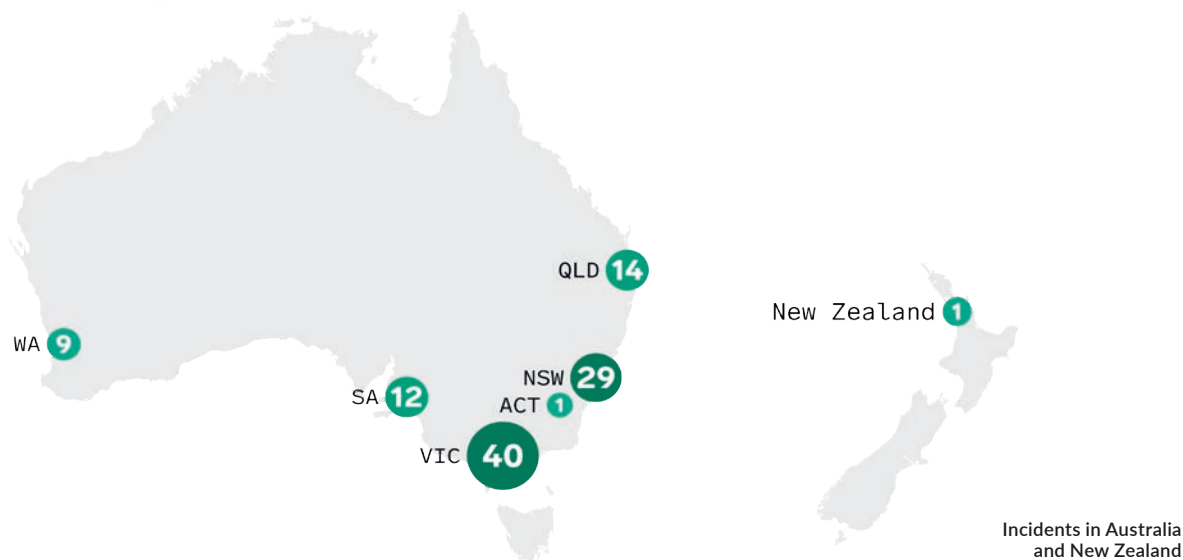


Terms and Conditions

*Offer valid for new bookings made prior to 31 Jan 2025. Not applicable in conjunction with any other Lumify Work special offers or packages. The discount is only applicable for our publicly scheduled instructor-led courses for ISC2, ISACA, CompTIA, EC-Council and PECB certifications. The discount cannot be applied to the purchase of exams, Self-paced/eLearning courses or any promotional bundles with a discount already applied. All other standard Lumify Work Terms and Conditions apply.

Evolving tactics and direct pressure strategies

The 2023–24 financial year was marked by numerous high-profile cyber attacks that earned significant attention from Australia’s media; however, for every large-scale attack reported in the media, numerous others go unreported, highlighting the pervasive nature of cyberthreats.



TRISKELE LABS'S LATEST report covers statistics and information gathered from Digital Forensics and Incident Response (DFIR) investigations conducted during the 2023–24 financial year across all Australian states and New Zealand.

KEY FINDINGS AND INCIDENT TYPES

Business email compromise

Business email compromise (BEC) incidents were the most frequent. BEC typically involves attackers gaining unauthorised access to business email accounts, often through phishing schemes, and then using these accounts to attempt payment redirection fraud.

Phishing continues to be the primary method that threat actors use to gain initial access to cloud accounts during BEC attacks. Still, tactics and techniques vary widely in their sophistication and delivery methods.

'Modern' credential harvesters use advanced defence-evasion techniques, such as traffic redirects from known data centres.

Some phishing schemes involve multiple redirects, making it more challenging for users and automated systems to identify the final malicious

landing page, which increases the complexity of the attack and the difficulty of detection.

Another method, captcha implementation on phishing sites, is adding another layer of legitimacy and can thwart automated security tools from detecting fraudulent activity.

Ransomware

Ransomware incidents were also significant. The encryption of data and demands for ransom payments to restore access severely impacts organisations, disrupting business operations, and leading to potential data and financial losses.

In addition to the technical aspects of ransomware attacks, Triskele Labs observed an increase in engagements where threat actors employed direct tactics to pressure victim organisations into paying ransomware.

These direct and aggressive pressure strategies are designed to create a sense of urgency and fear, aiming to force organisations into swift compliance with ransom demands.

Other types of incidents

In addition to ransomware and BEC incidents, the DFIR team also investigated a mix of malware infections, unauthorised access

attempts, insider threats, and data breaches that did not fall into the specific categories of ransomware or BEC.

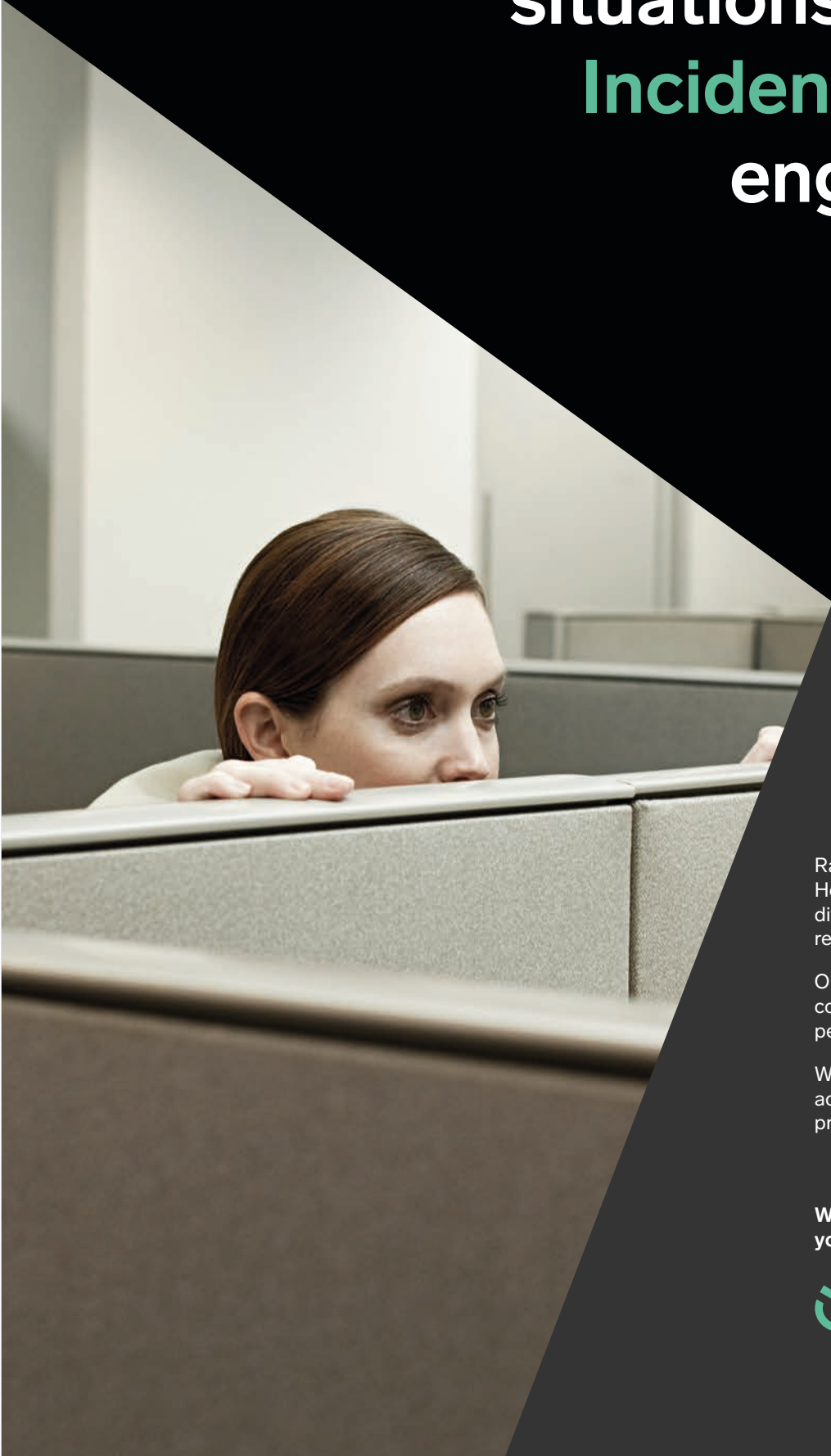
DATA EXFILTRATION
OCCURRED IN
65 PER CENT OF CASES,
WITH AN AVERAGE
OF 406 GIGABYTES
EXFILTRATED DURING
RANSOMWARE ATTACKS

INDUSTRY VERTICALS

The data again confirms that any industry can be impacted by a cyber incident, with finance and health care being the most affected. The broad distribution of incidents across various sectors underscores the opportunistic nature of threat actors, who do not necessarily target specific organisations, but exploit vulnerabilities wherever they find them.

They reflect a broader trend of cybercriminals diversifying their methods to maximise their chances of success. ●

Access the full report at www.triskelelabs.com



We find clients in the most awkward situations during our **Incident Response** engagements.

Ransomware can happen to anyone.
However, your preparedness will make the
difference between a significant financial and
reputational loss and a manageable situation.

Organisations can mitigate the risk of cyber
compromise by focusing on three key areas:
people, processes, and technologies.

We can help you identify the immediate
actions you need to take, making you feel
proactive and in control.

We are the only Cyber Security experts
you'll ever need to talk to.

 **Triskele Labs**

CAN THE GOVERNMENT MAINTAIN ITS CYBER SECURITY MOMENTUM?

— BY DAVID BRAUE —

The Australian Cyber Security Strategy has laid out a national agenda through 2030.

The major reshuffling of the Albanese Government's ministerial portfolios in July marked a dramatic change for the cyber security ministry, which was created in 2022 and forged under pressure as Clare O'Neil was soon faced with a series of major cyber attacks that informed last year's release of the Australian Cyber Security Strategy (ACSS) 2023–2030.

O'Neil often stated that her goal by 2030 was to make Australia the most cyber-secure country in the world – and it would happen through a strategic ACSS built around six 'shields', including strong businesses and citizens; safe technology; world-class threat sharing and blocking; protected critical infrastructure; sovereign capabilities; and a resilient region and global leadership.

Backed by \$586.9 million in funding through 2030, the strategy was a 'generational shift' that encapsulated the ambition of a government that was, O'Neil said when the ACSS was released last November, 'determined to act decisively and do what is necessary to protect Australians from the fastest-growing threat that we face as a nation'.

'Our strategy will make every Australian citizen, business, government agency and organisation a harder target,' she said, adding that 'it will enable us to bounce back faster from attacks that we cannot prevent'.

She continued, 'We will put cybercriminals on notice, and we will fight back against the threat.'

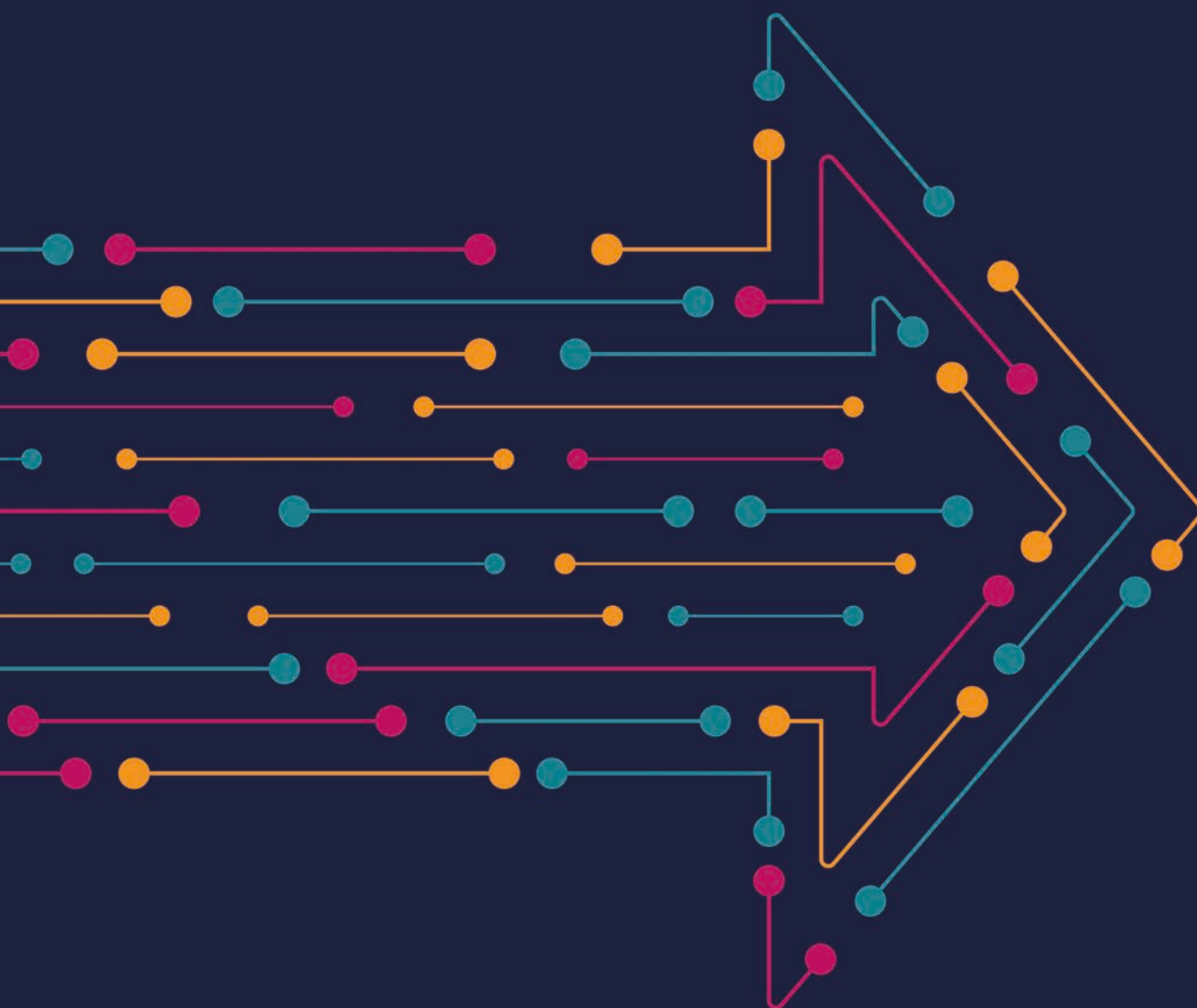
As a complement to strategies such as the Ransomware Action Plan and an education campaign built around three core, relatable ways of maintaining security online – the use of multi-factor authentication, installation of regular software updates, and the use of strong, unique passphrases that are over 14 characters long and use four or more random words – the significant update to the ACSS offered O'Neil a way to consolidate the lessons of the

massive breaches of Optus, Medibank, Latitude Financial Services, and the myriad other cybercrime victims.

Many of those breaches – which have led to hundreds of millions of dollars in losses and fines, as well as class action lawsuits – were ultimately attributed to 'rookie errors' that could have been avoided had the companies been more focused on finding and addressing latent security exposures.

The magnitude of those breaches fuelled a series of policy changes as a visibly angry O'Neil, bent on exacting revenge on the cybercriminals – the 'scumbags', she said, that had compromised sensitive information relating to more than half of Australia's population – pushed through policy changes, including raising the fines on companies whose inaction led to major breaches of personally identifiable information, an ongoing debate about potential liability for company boards and executives, and a mandatory reporting overhaul that saw operators of critical infrastructure required to report critical cyber security incidents within 12 hours.

O'Neil oversaw the appointment of the National Cyber Security Coordinator role, and facilitated



the launch of the government's National Anti-Scam Centre 'fusion cell', whose proactive and collaborative approach to scams enforcement saw it and similar organisations cautiously proclaiming that they had turned the tide on scammers and cybercriminals in May.

CHANGING OF THE GUARD

O'Neil's two-year tenure saw a dramatic reshaping of the government's attitude towards cyber security, which was treated in the two previous cyber security strategies as being more the responsibility of private industry than what O'Neil described in the strategy document as 'an urgent national problem ... [that] touches the lives of every Australian'.

The ACSS crystallised the idea that cyber security has become fundamentally important to the operation of businesses, and its structure reflects the intense period of learnings and introspection that characterised O'Neil's tumultuous first year, when she was learning on the hop and developing policy as quickly as her emerging nationwide expert apparatus could advise her.

'We are living in the new cyber normal,' Professor Matthew Warren, Director of the RMIT Centre for Cyber Security Research and Innovation, noted upon the release of a strategy that he called 'a key step in helping to protect Australia in the future against the wide range of cyber threats that Australia faces'.

'Unlike previous national cyber security strategies, this strategy clearly defines what success looks like and the three phases of implementation needed to get to a successful outcome,' he added.

Albanese's decision to hand the portfolio to new minister Tony Burke, however, has repositioned cyber security yet again – and not necessarily for the better, as it became arguably the smallest of four high-profile ministries managed simultaneously by Burke. He is also the Minister for Home Affairs, the Arts, and Immigration and Multicultural Affairs, as well as serving as Leader of the House.

This change of focus was reflected in Burke's official statement on his new portfolios, where he touched on the myriad aspects of a new portfolio that he promised to approach 'with a deep sense of responsibility and resolve'.

And while ‘keeping Australians safe’ was a central part of his philosophy, Burke’s only mention of his new role as cyber security policy head was to say that he ‘look[s] forward to continuing Clare O’Neil’s important work in protecting the nation from cyberthreats’.

That proved to be prescient days later, when Burke – who was sworn into the role just days after a CrowdStrike configuration error took down millions of computers worldwide and disrupted businesses of all sizes – was asked about the government’s response.

‘All the systems that had been put in place by my predecessor were able to be tested and showed that Australia is far better prepared for cyber attacks than comparable nations,’ he said.

Whether Burke is truly committed to advancing the cyber security agenda in the proactive way that O’Neil was – or whether he sees it as a peripheral responsibility that can be left largely on autopilot thanks to the clarity of vision elucidated in the ACSS – remains to be seen, and Burke’s response to the inevitable next big breach will be enlightening.

Industry, however, has high hopes that he can maintain the pace of the policy work that O’Neil set: AvePoint Industry Engagement and Strategy Lead Janine Morris, for one, recently noted that ‘the industry’s expectations are high for Minister Burke’ to continue building on the ‘commendable strides’ of his predecessor in building ‘a comprehensive approach that can uplift national cyber capabilities through the NCSS’.

Four key activities, Morris said, will be crucial – including ‘regular and secure’ backups to mitigate the damage from ransomware breaches; the use of ‘crucial’ tools and policies to provide real-time visibility into security posture and compliance status; effective data life cycle management to reduce an organisation’s attack surface; and comprehensive and ongoing training for users that form the ‘human firewall’ that every organisation needs.

AN ACTION PLAN FOR EVERY AUSTRALIAN BUSINESS

Those four key focus areas are subsumed within the broader scope of the ACSS, which includes a range of specific actions grouped within its six ‘shields’.

These include, for example, small business support through the delivery of free cyber security maturity assessments to help small businesses get ahead of their vulnerabilities, and a Small Business Cyber Resilience Service to help them recover when cybercriminals beat them to it.

Authorities will double-down on threat sharing, working with government and industry leaders to improve the flow of threat- and breach-related information, as well as a Cyber Incident Review Board – modelled after the US Cyber Safety Review Board and

the Australian Transport Safety Bureau – that will offer no-fault incident reviews, and whose findings will be shared with the business community, threat intelligence bodies, and other initiatives.

The government has also promised cyber security guidance and a single cyber incident reporting portal for businesses, as well as national cyber awareness campaigns for the public, and a community grants program to deliver tailored cyber awareness campaigns to diverse groups.

The ACSS also unifies law enforcement and offensive cyber security capabilities being developed, here and across the region, under the auspices of initiatives such as the Australian Signals Directorate’s (ASD’s) Project REDSPICE, and the Australian Federal Police and ASD-led Operation Aquila, which has been working with some success to disrupt criminal syndicates both in Australia and outside of it.

ACSS initiatives will guide the government’s increased focus on protecting critical national infrastructure and the data storage systems supporting that infrastructure, with initiatives such as the Systems of National Significance framework and the Critical Infrastructure Uplift Program helping critical entities ‘better manage the consequences of cyber incidents’.

Other aspects of the far-reaching ACSS include a focus on building a government-backed digital ID framework; funding for support of identity theft victims; and a review of the government’s data holdings, data-brokerage ecosystem, and data-retention requirements backed by the development of a voluntary data-classification model.

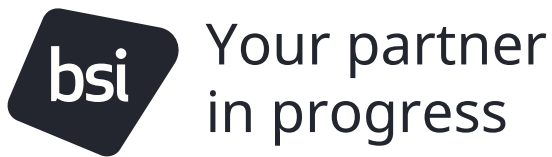
The new ACSS is a long read, filled with initiatives and action items based on keeping Australia, its citizens, its businesses and its infrastructure safe from cyber security compromise.

Keeping its agenda on track is enough to keep a minister busy on a full-time basis – but if Burke can successfully juggle the ACSS’s vision with his other responsibilities while maintaining the momentum that O’Neil built, analysts agree that the strategy could be just what Australia needs to achieve her 2030 vision.

‘The Australian Government realises that genuine behavioural change will take time, and aims to address this by delivering awareness-raising programs in the long term,’ Forrester Vice President and Principal Analyst Jinan Budge said when the new ACSS was released, adding that ‘the government’s in-principle focus on instilling culture is admirable’.

‘While the last decade has seen significant increased attention on cyber security, the proposed solutions, capabilities and skills have largely centred around technology,’ she said.

‘The strategy recognises that cyber is no longer a technical topic, but a whole-of-nation effort ... If Australia realises the strategy’s vision and intent, it’s a great time to work in cyber.’ ●



Advance your career and build trust in AI with BSI training

To effectively leverage AI, organizations must build understanding, establish governance, manage risks, and ensure legal compliance. BSI AI professional qualifications are designed to accelerate progress through structured learning pathways, combining selected courses with rigorous assessments to ensure relevance. Our training equips you with essential knowledge for implementing and auditing AI management systems.

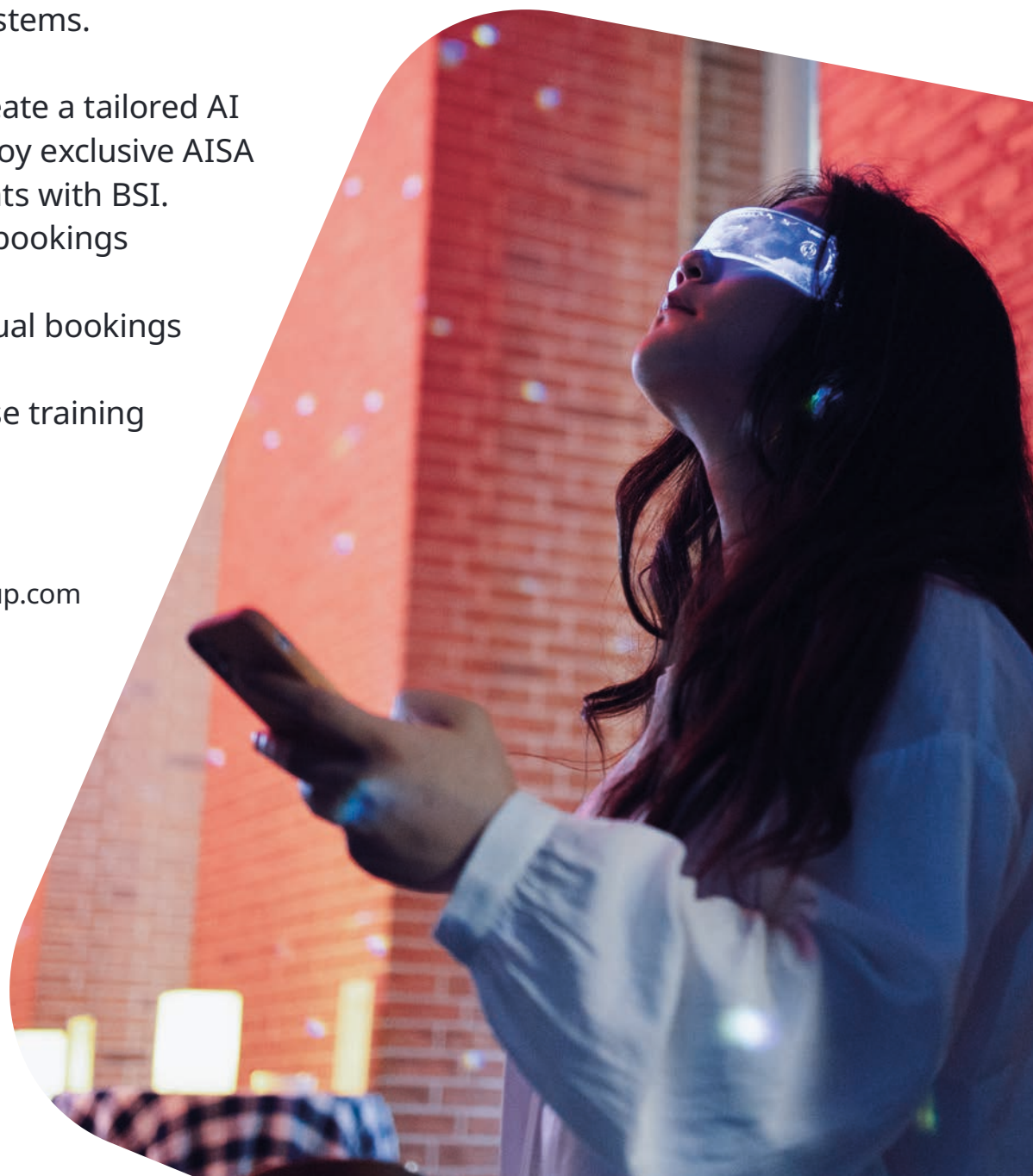
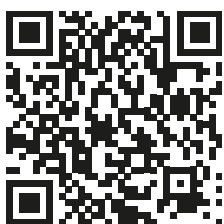
Contact us to create a tailored AI pathway and enjoy exclusive AISA member discounts with BSI.

- 30% off group bookings (code: AISA30)
- 20% off individual bookings (code: AISA20)
- 10% off in-house training (code: AISA10)

P: 1300 730 134

E: info.aus@bsigroup.com

**Download our
AI brochure**



Countdown to quantum

FOLLOWING THE UNITED STATES National Institute of Standards and Technology's (NIST's) publication of the first standards for post-quantum cryptographic (PQC) algorithms, the race is on for Australian organisations to migrate to a quantum-safe stance ahead of Y2Q.

On 13 August 2024, NIST announced the availability of its first three finalised PQC algorithms. This was a significant milestone in a journey that began over eight years ago, when NIST first sent out the call to solicit, evaluate and standardise quantum-resistant, public-key cryptographic algorithms.

WHY DO WE NEED PQC?

The dawn of the quantum computing era is viewed with equal parts optimism and scepticism. There are

undeniable benefits to the exponential growth in computing power that a quantum processor represents. Experts eagerly anticipate advances in areas as diverse as drug discovery and genomics, financial risk assessment and fraud detection, materials science, climate modelling, network optimisation, and more; however, the problem-solving capacity of a quantum computer also represents a significant threat to the public-key cryptographic infrastructure we currently rely on for secure data transmission, web browsing and communications.

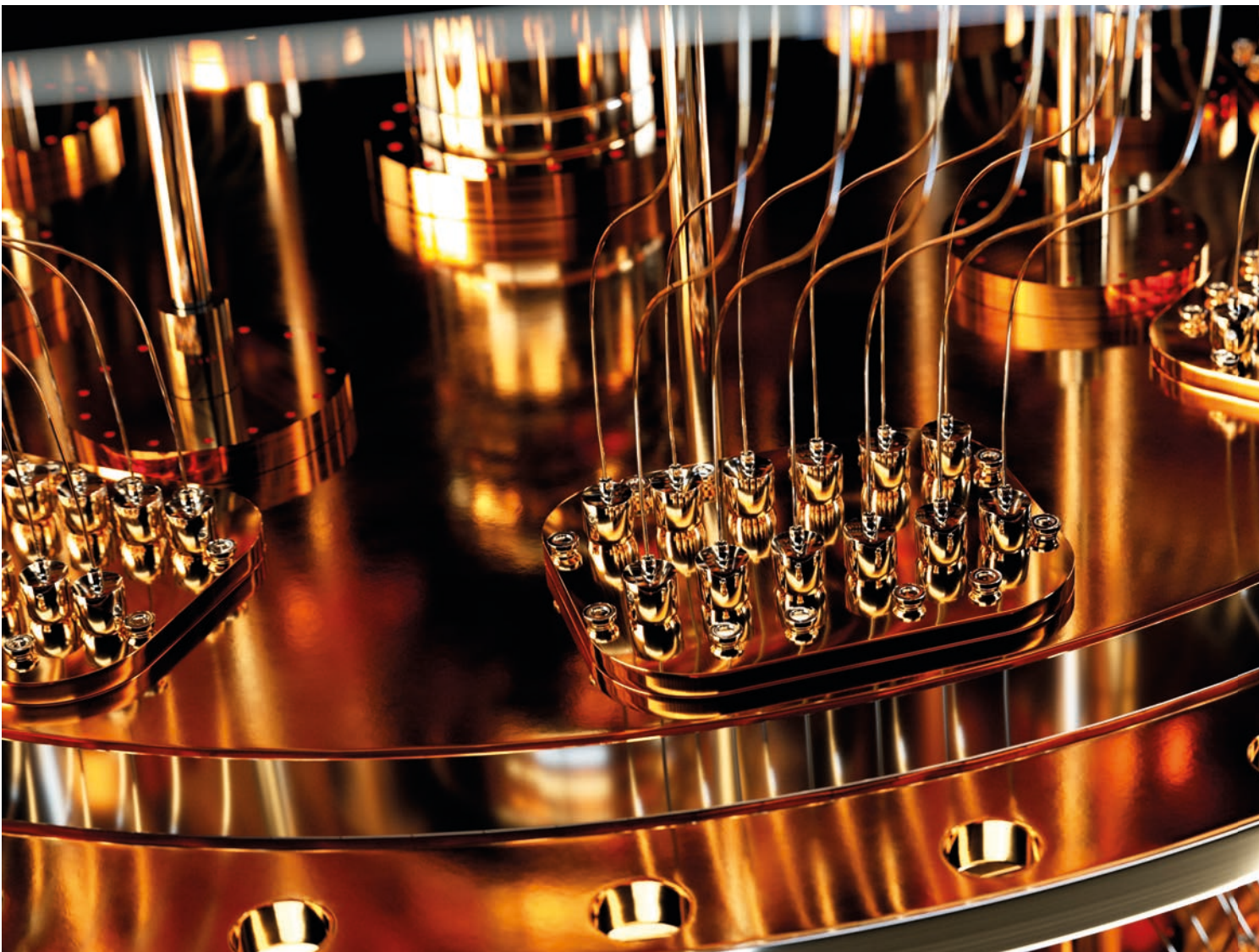
Today's cryptographic security is based on the principle that math is hard. In fact, the math is so hard that it's estimated that an array of classical supercomputers would need 1500 years to crack an RSA 1024-bit key. The problem is that quantum

computers are really good at math. A sufficiently error-corrected quantum computer running Shor's algorithm could achieve the same task in a matter of hours.

PQC is designed to be resistant to both classic and quantum computing attacks. It will replace vulnerable cryptographic elements such as RSA encryption, elliptic-curve cryptography and Diffie-Hellman key exchange over time. Quantum-resistant algorithms, key exchange and digital signatures will be used to provide long-term data protection, and to futureproof the security of critical infrastructure and the Internet of Things.

THE CORRIDOR OF UNCERTAINTY

Although progress towards a commercially viable quantum



computer has been slow, governments and private sector organisations are investing vast amounts of time and effort into developing quantum assets. Private sector investment in 2023 exceeded US\$1 billion, and governments worldwide have already committed more than \$40 billion in public funding over the next decade. The benefits of being first past the post in this race are significant!

When it comes to quantum succession planning, timing is everything. Industry experts, including IBM and the Cloud Security Alliance, agree that the quantum horizon is the end of the decade. The Cloud Security Alliance started its countdown to Y2Q in 2022, with D-day being 14 April 2030. Five years may seem like enough time to get your house in order, but history will tell you something different. The last project of a similar scale, the rollout of RSA encryption,

took almost 20 years from invention to adoption.

You don't need to have the mathematical ability of a quantum computer to see that these numbers just don't work out. Granted, we're probably looking at a best-case scenario for quantum computers, and a worst-case scenario for quantum cryptography; however, there is a corridor of uncertainty during which a quantum computer will be available, and systems will still be vulnerable.

FORWARD SECRECY

Whatever timeline you believe in, there is a more immediate concern. Much of the private and commercially sensitive data that exists today has a long life – meaning that it retains its value, relevance and sensitivity over an extended period. Personal identification information, financial records, medical records, intellectual property and a wide

range of other data can retain its value for decades – well beyond the most pessimistic of quantum horizons. All this data is vulnerable to what is known as 'harvest now, decrypt later' attacks, where threat actors intercept encrypted data today and store it until a time when a quantum computer can efficiently decrypt it.

If this all sounds a little apocalyptic, it doesn't need to be. The release of the first standards for PQC means that cyber security professionals now have access to technology that can ensure long-term data protection in a post-quantum world. Forward-thinking solution providers practice what is known as crypto agility, and there are systems available today that provide hybrid encryption with the capacity to use both classic and quantum algorithms.

MIGRATION TO QUANTUM-SAFE SECURITY

For most, the migration to a quantum-safe infrastructure is likely to be a lengthy process, so it is important to start your journey as soon as possible. As such, Senetas advocates a five-step process:

- audit
- assess
- plan
- evaluate
- implement.

Step one is to carry out a comprehensive audit of your current cryptographic use – what is being encrypted, how and where. Step two is to carry out a risk assessment of all your cryptographic systems to identify which will be potentially vulnerable to quantum attack. Having established what is at risk, step three is to devise a mitigation plan that establishes whether the risk is acceptable (low-value data), and if current systems will need to be upgraded or replaced. Step four is to evaluate the quantum-safe options available, and step five is to agree on a road map for implementation of your chosen solutions.

There may have been a time when it was tempting to dismiss the quantum threat as pure science fiction, but the reality is that quantum is coming. It's up to you to be ready for it when it gets here. •



Incident response for Australian companies – between compliance and practical capabilities

IN AUSTRALIA, BOTH businesses and regulators increasingly understand that not every security incident can be prevented. Developing and implementing a cyber incident response plan has become a common theme across most Australian cyber regulations. This requirement is highlighted in the Australian Cyber Security Strategy, recommendations and checklists from the Australian Signals Directorate, and even in the latest Audit Office of New South Wales report on local government cyber security.

These publications consistently urge Australian organisations to ‘develop, implement and test a cyber incident response plan’.¹

As practical experience shows, this compliance-focused approach to incident response planning has significant shortcomings. An incident response plan can only be effective if decision-making can be supported by technology.

During a breach, businesses frequently face the harsh reality that their technical capabilities – whether security information and event management, extended detection and response, network detection and response, or other systems – tend

to provide only partial data about the breach. This data often lacks the detailed insights needed to pinpoint the initial point of compromise. As a result, businesses find it challenging to quickly assess the extent of the damage, confirm whether the attacker has been fully contained, or determine if it is safe to commence recovery.

Your success in responding to a cyber security incident depends on answering these key questions about the breach:

- Who is the patient zero?
- How long had the attacker been in our system?
- Are there any other systems that are breached?
- Has our data been exfiltrated? If so, what exactly?
- How can we be 100 per cent confident that the attacker has not left any backdoors open, and will not return?

These questions will naturally arise during the response process. If you can answer them confidently, you will be able to recover and move forward. If not, you will find yourself in murky waters, relying on guesses instead of informed decisions.

In such scenarios, there’s a risk of making statements like, ‘We likely covered all bases’, ‘We’ve done as much as possible’, or ‘We haven’t found any evidence of further intrusion.’

In Australia, there have been numerous instances where companies were unable to answer these critical questions and resorted to guessing. Here are two well-known examples:

- After Medibank’s data breach in October 2022, Medibank’s official statement said: ‘We have still found no evidence that customer data has been accessed.’
- After Service NSW’s data breach in April 2020, Service NSW’s official statement said: ‘There is no evidence that Service NSW databases were compromised, and the network and systems of record that store licence information are not affected by this breach.’

Notably, both incidents resulted in extensive data breaches involving millions of records.

In a world where cyber security attacks are becoming increasingly sophisticated, organisations must strengthen their security operations to conduct thorough investigations with greater scale, speed and efficiency. Building capabilities focused on gathering and analysing evidence is crucial for effective incident response. These core capabilities are essential for ensuring a strong, evidence-driven approach to handling cyber security incidents. •

¹ *Audit Office of New South Wales, Cyber Security in Local Government, March 2024*



threatdefence_

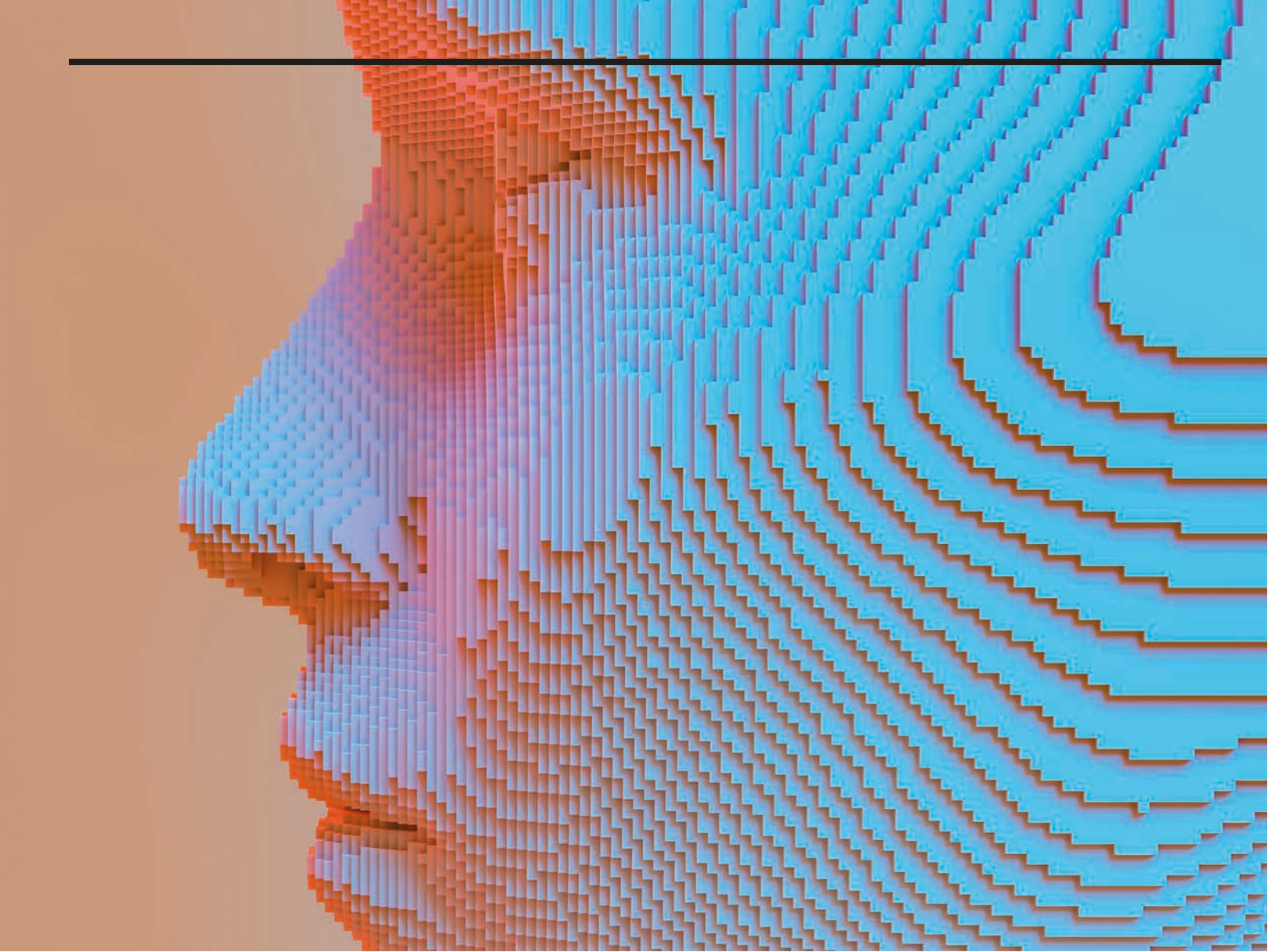


ZERO STARS.

WOULD NOT RECOMMEND.

- Hacker

- ✓ Australian-Made Platform
- ✓ Evidence-Based SecOps
- ✓ Next-Generation SIEM and NDR
- ✓ 24x7 Security Operations Centre
- ✓ Threat Hunting and Incident Response



THE INTERSECTION OF AI AND CYBER SECURITY: IMPLICATIONS FOR CYBER DEFENCE

— BY VANNESSA VAN BEEK, AUSTRALIAN SECURITY LEAD, AVANADE —

The rapid advancement of artificial intelligence has not only revolutionised industries, but it has also provided new tools for threat actors, significantly increasing the scale of cyber attacks.

According to a report by Egress, phishing attacks surged by 40 per cent in 2023, largely due to the use of generative artificial intelligence (AI) to craft more convincing and personalised phishing emails.¹ This increase highlights the growing trend of AI-assisted reconnaissance and hyper-targeted spear-phishing attacks, which are becoming more prevalent and harder to detect.

In addition, Trend Micro's research indicates a rise in AI-driven cybercrime in the first half of 2024: 'Threat actors are leveraging AI to automate and enhance various stages of their attacks, from initial reconnaissance to the execution of complex, multi-stage operations.'²

This includes the use of AI to write malicious code, reverse-engineer existing programs, and inject harmful content into otherwise legitimate models.

A collaborative study by Microsoft and OpenAI also found that state-affiliated threat actors are increasingly using AI for malicious purposes.³ The state-affiliated threat actors tracked by Microsoft using large language models to augment their ongoing cyber attack operations include Forest Blizzard, Emerald Sleet, Crimson Sandstorm, Charcoal Typhoon and Salmon Typhoon. These actors utilise AI to conduct open-source research, translate technical documents, and generate scripts for phishing campaigns. While AI offers significant benefits, its misuse by threat actors poses a substantial risk to cyber security. The sophistication and scale of these attacks underscore the urgent need for cyber security measures to counteract these evolving threats.

In 1950, Alan Turing posed a question that remains relevant today: 'Can machines think?' The 'Turing Test' is designed to evaluate whether a machine could imitate human intelligence convincingly enough to fool a person. The rise in scams and increasingly persuasive phishing emails generated by AI might suggest we are approaching – but not yet at – this point. The question for cyber defence is not just whether machines can think, but whether they can help us think faster and more securely in an increasingly hostile cyber landscape.

While AI has the potential to help both attackers and defenders, in the short term – according to a recent report from Blackberry – 'threat actors may have an advantage, as they can quickly adopt new techniques without worrying about production readiness'.⁵

Attackers, unbound by organisational constraints, have the luxury of time and secrecy. They leverage AI to automate processes and deploy tactics at speed. In contrast, defenders are bound by policies, procedures and budgets. Their focus is to defend the attack surface and respond. The growing gap in AI adoption between attackers and defenders increases the disparity in cyber security, making organisations more susceptible to threats that AI could combat.

THE COST OF LEGACY THINKING AND UNDERINVESTMENT

Legacy thinking is a silent adversary in cyber security; it perpetuates reliance on outdated systems and processes. The result is a reactive approach to security, where defences are bolstered only after breaches occur. This approach is not only inefficient, but is also costly. According to Gartner, the current cyber security environment requires far more investment in preventive measures than most organisations are willing or able to fund. Even if spending on preventive investments were multiplied tenfold, many organisations would still be exposed to significant cyberthreats. This underinvestment in response and recovery capabilities is driving cyber security teams into the ground.

Recent surveys reveal that 62 per cent of cyber security leaders have experienced burnout at least once in the past year, with nearly half experiencing it twice.⁵ The message is clear: adrenaline does not scale in the complex world of cyber security, and relying on it is unsustainable.



Vanessa Van Beek

THE ROLE OF AI IN ADDRESSING SECURITY OPERATIONS CENTRE CHALLENGES

The 2022 Devo SOC Performance Report highlights the significant challenges faced by security operations centres (SOCs), including information overload, excessive workloads, and difficulties in recruiting and retaining skilled professionals. These challenges contribute to alert fatigue and exacerbate inefficiencies, leaving SOC analysts overwhelmed and reactive, rather than proactive. AI-driven tools can significantly enhance incident-response capabilities by automating routine tasks, summarising and reporting incidents quickly, and allowing analysts to focus on high-value activities like threat detection and defence. This not only improves the quality and efficiency of security operations, but also shifts operational costs to more strategic initiatives. The integration of such AI tools is critical in alleviating the burden on SOC teams, and ensuring that security operations remain resilient in the face of increasing threats. AI is being integrated into cyber security solutions to provide real-time threat-detection and response capabilities. Organisations like Microsoft, Splunk, Google, CrowdStrike, Fortinet and Palo Alto Networks are at the forefront of this integration, enabling security teams to swiftly identify and neutralise threats. Despite these advancements, many organisations are slow to adopt AI solutions into their cyber security operations.

INCREMENTAL AI INTEGRATION: A PHASED APPROACH

Adopting AI in security operations does not have to be an all-or-nothing proposition. Instead, consider a phased approach, starting with the integration of AI into less-critical tasks, and gradually moving to more significant functions as confidence and understanding grow. This incremental approach mitigates the risks associated with AI deployment, ensuring that systems are robust and effective before being entrusted with critical security functions. Fostering a culture of continuous learning and adaptation is crucial. Security teams must be encouraged to stay updated on AI developments and continuously refine their skills. This ongoing education

ensures that they can effectively leverage AI tools and respond to evolving threats with agility and precision.

THE HUMAN ELEMENT: WHY AI SHOULD COMPLEMENT, NOT REPLACE

While AI has the potential to transform security operations, the human element remains indispensable. AI systems should be seen as complementary to human expertise, not as replacements. Skilled analysts are essential for interpreting AI outputs, providing context, and making nuanced decisions that AI alone cannot. By working in tandem with AI, human analysts can enhance their capabilities and achieve better outcomes, ensuring that AI is used to its full potential while retaining the critical human judgment necessary for effective cyber security.

NAVIGATING THE RISKS: LESSONS FROM PAUL VIRILIO

Paul Virilio, a renowned philosopher, once remarked: ‘The invention of the ship was also the invention of the shipwreck.’

This observation underscores the inherent risks in any technological advancement; however, just as ships have enabled thriving civilisations, AI has the potential to elevate security operations. The key is not to avoid these risks, but to navigate them wisely. While AI can enhance threat detection, automate routine tasks and provide predictive insights, its deployment requires careful consideration of integration issues, ethical concerns, and access controls to ensure protection from misuse.

The Turing Test, originally designed to determine if machines could convincingly mimic human behaviour, provides a relevant framework for today’s cyber security leaders. The test emphasises the importance of trust – trust that AI can perform tasks requiring human-like intelligence, and trust that it can complement human capabilities without replacing them. The challenge is to ensure that AI tools are rigorously tested, ethically deployed, and used to enhance, rather than replace, human intelligence. AI’s role in security operations should be to handle the data-intensive tasks that would overwhelm human analysts, allowing them to focus on the complex decision-making that requires their expertise. This approach not only builds trust in AI, but also ensures that security operations are both effective and resilient.

It is perhaps time to pause and consider AI as a vital ally in the fight against cyberthreats. By fostering a collaborative environment where AI enhances human expertise, security operations can evolve to meet the challenges of the modern threat landscape.

As Reid Hoffman aptly stated: ‘Artificial intelligence should be limited. Artificial intelligence should be accelerated.’ The future of cyber security lies not in choosing between AI and human expertise, but in synthesising the two. By embracing this

synthesis, taking incremental steps in AI integration, and addressing the critical gaps in response and recovery capabilities, organisations can build a more resilient security posture – one capable of withstanding the relentless and evolving nature of cyberthreats. ●

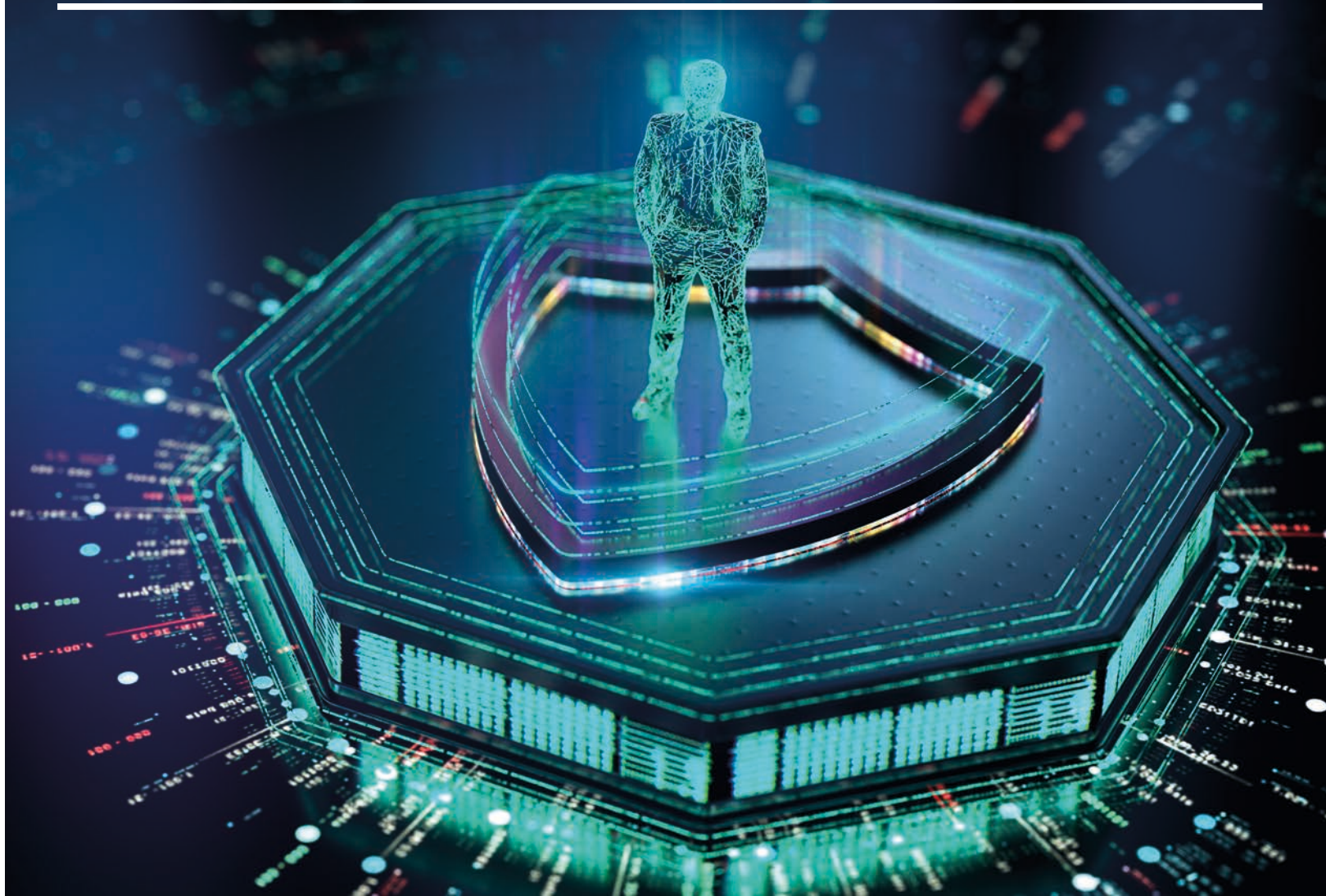
Vannessa Van Beek is the Australian Security Lead at Avanade, a Microsoft and Accenture company. She leads the Australian team providing security services to protect information, critical infrastructure, applications and key business processes from cyberthreats. She has over 30 years’ experience in IT, which includes an early focus on data networking and digital transformation. Most recently, Van Beek led security operations, platform engineering and architecture at Kinetic IT. She is an AISA member and has spoken AISA conferences throughout Australia.

Footnotes

1. KnowBe4’s 2024 Phishing by Industry Benchmarking Report Reveals that 34.3 per cent of Untrained End Users Will Fail a Phishing Test
2. Trend Micro. (2024). Pushing the Outer Limits: Trend Micro 2024 Midyear Cybersecurity Threat Report. Retrieved from <https://www.trendmicro.com/vinfo/hk/security/research-and-analysis/threat-reports/roundup/pushing-the-outer-limits-trend-micro-2024-midyear-cybersecurity-threat-report>
3. Staying ahead of threat actors in the age of AI | Microsoft Security Blog
4. BlackBerry Quarterly Threat Intelligence Report Finds Governments and Public Services Facing 40 per cent More Cyberattacks
5. Cybersecurity Leader Burnout — Causes and Solutions (gartner.com)

References

- Addiscott, R., & Hevesi, P. (2024). ‘Top trends for cybersecurity in 2024’. Gartner Report.
- Egress. (2023). ‘2023 Phishing Threat Trends Report’. Retrieved from https://www.egress.com/media/mq4kwitu/egress_phishing_threat_trends_report.pdf
- Gopal, D. (2023). ‘Essential components of a cyber-risk management program’. Gartner Report.
- Hoffman, R. (2021). ‘Artificial intelligence should be limited. Artificial Intelligence should be accelerated’.
- Mixter, C., & Xu, D. (2024). ‘Addressing the talent shortage in cybersecurity’. Gartner Report.
- Turing, A. M. (1950). ‘Computing Machinery and Intelligence’. MIND, 59(236), 433-460.
- KnowBe4. (2024). ‘2024 Phishing by Industry Benchmarking Report’. Retrieved from https://www.knowbe4.com/hubfs/2024-Phishing-by-Industry-Benchmarking-Report-EN_US.pdf
- Trend Micro. (2024). ‘Pushing the Outer Limits: Trend Micro 2024 Midyear Cybersecurity Threat Report’. Retrieved from <https://www.trendmicro.com/vinfo/hk/security/research-and-analysis/threat-reports/roundup/pushing-the-outer-limits-trend-micro-2024-midyear-cybersecurity-threat-report>
- Devo. (2022). ‘2022 SOC Performance Report’. Retrieved from <https://www.devo.com/wp-content/uploads/2023/06/2022-Devo-SOC-Performance-Report.pdf>



Worlds collide

— BY BENJAMIN RILES —

In 2016, after nine years in fine-dining kitchens, I found myself looking for a sea change on the banks of a South Coast creek line.

Cooking had been my life. But after many nights of adrenaline-fuelled double shifts in the kitchen, I was reaching a boiling point. The constant demands, cuts, scars and burns – both physical and mental – were taking their toll. It was clear I needed a break.

If you've ever seen the inner workings of a high-end kitchen, you know the type of relentless energy I'm talking about. It's an environment that breaks you down, only to build you back up again, moulded into what the kitchen needs you to be. *The Bear* captures that intensity all too well – too well for me to watch, actually.

Welcoming the fresh air, I joined my best friend, who had been immersed in Australian native bush regeneration. We were at Broughton Creek in Foxground, New South Wales – rugged terrain, heavy rainfall, and lush green canopies. It felt far removed from the pressure cooker I had been living in.

The surroundings were just what I needed – or so I thought. It was a strange moment, looking back now, to be so deep in nature while observing what felt like a

new-age digital phenomenon on my phone. I had been closely tracking the crypto market, keeping an eye on the latest news and watching the rise of some big names in the space. And that's when things took a pear-shaped turn.

During a quick five-minute break, I checked my phone. One of the crypto companies I followed posted a deal: buy some coins and get extra in return. It seemed like a great opportunity, and I had 'heard' of this scheme before. I transferred nearly \$1000 worth of Bitcoin and went back to work.

As time passed, I kept checking my phone. There was no sign of the return. I told myself that crypto transactions took time. Who am I to question the technology? I trusted these people. Eventually, I knew something was astray. My heart started to pound. My hands were sweaty, eyes alert. I couldn't let my friend see me like this. I was glad I was alone.



Benjamin Riles

I kept searching for answers, hoping it was standard procedure. With every passing minute, the knots in my stomach tightened.

I sat down, trying to make sense of it, and that's when it hit me – like a blast from a hot, steamy oven to the face. I had been scammed. I was angry, embarrassed and confused all at once. My mind raced with questions. How did they pull this off? How could I have been so foolish? I dug deep – and never spoke of it.

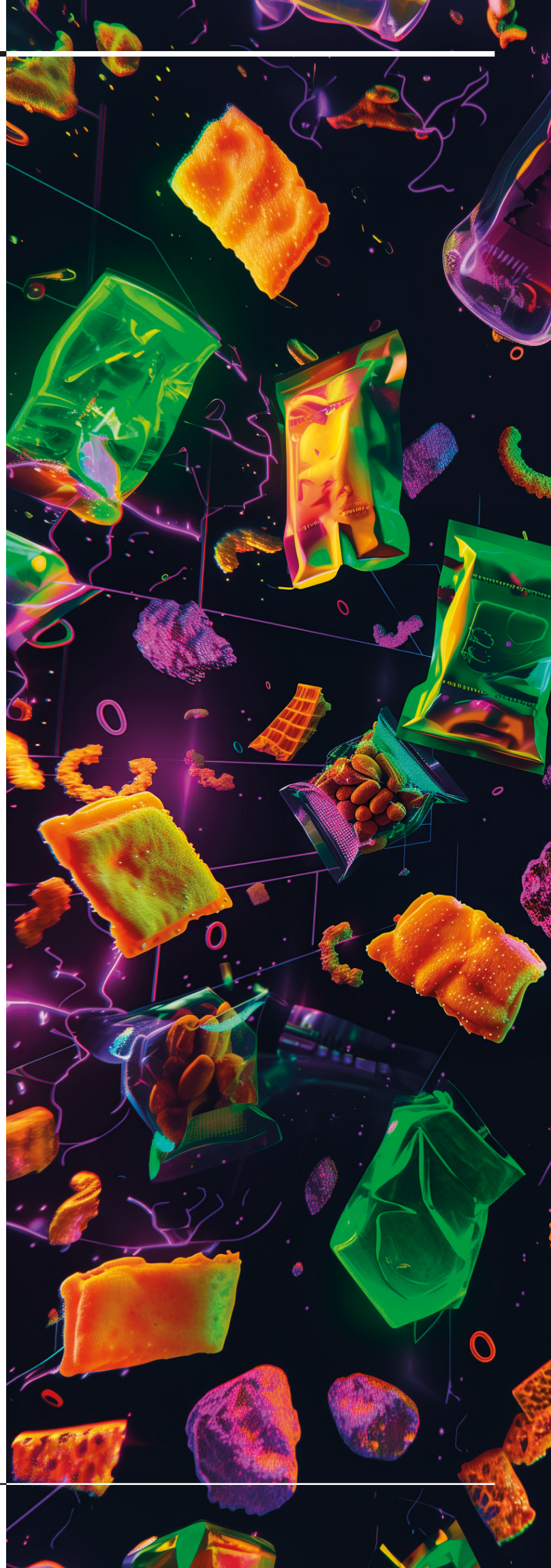
Fast forward to 2022. The lockdowns were ending, and I had spent the past few years consuming everything I could about cyber security and technology. I had been scammed, after all. I needed resolution – I wanted to know how they did it.

I left behind my aspirations for a successful chef career, started working part-time, and enrolled in a Certificate IV at university. Dark rooms? Black hoodies? Large monitors? Great pay? Catching the bad guys? Sign me up! I stumbled upon a life-changing opportunity. The Deloitte Cyber Academy offered paid work in cyber and a bachelor's degree to complement it. I couldn't say no.

No dark rooms and no hoodies? But at least some big screens! I landed in governance, risk and compliance (GRC). There's a huge assumption that cyber security is all technical – coding, penetration testing, secure configuration, and tracking down threats in real time. The reality? Not all of cyber is technical. I discovered a whole world of cyber that, to my benefit, relied on soft skills while still requiring critical thinking.

After years of honing interpersonal skills and managing high-intensity situations in close quarters (with knives!), I developed the ability to communicate effectively, helping me to hit the ground running in the world of GRC. I still brought my chef skills to the table – just in a different way. The transition wasn't as blunt as I expected. Staying calm under pressure and working as part of a team are vital in both kitchens and cyber. I was quick to realise that cyber is more diverse than most people outside of the industry think, and that's something I want to raise awareness about. Sure, coding is important, but give me a break, I've just spent 15 years chopping vegetables!

In my first two years in cyber security, I've seen shifts in the landscape that even I, as a newcomer, still can't believe. Artificial intelligence (AI) has become embedded in workplaces, transforming industries, and drones are being developed for automated deliveries. With every advancement, I'm left wondering: Who is securing these systems and processes? What policies are being put in place to ensure the safety of these innovations? Technology advances faster than policy, and that's just the nature of it. We're constantly playing catch-up.





One of my favourite things about this field is the community. Cyber thrives on networking, support, conferences and sharing ideas. It's a refreshing change from my experience in hospitality, where labour abuse and secrecy often ruled the day. Fortunately, I have seen that attitude begin to shift in hospitality, with the next generation influencing and bringing more transparency to the industry. This kind of collaboration is something we're seeing shift across many industries. My recent favourite example was that they were looking into the playbooks of the medical industry and what frameworks they have that are time-tested, and using these for incident response.

Engaging is easy in this industry, but keeping pace is another challenge. Drones and cyber security? Just got my Civil Aviation Safety Authority-certified Remote Pilot Licence. AI in the workplace? Responsible use, please. Quantum cryptography? Be quantum agile. The Security of Critical Infrastructure Act? Let's focus on compliance. One of Australia's biggest changes is coming? The Privacy Act reform is right around the corner. DevOps and AppSec? I'm attending the next conference, even if I don't understand everything. My take is that this industry has enabled us with the tools and opportunities to keep learning and asking questions. Don't be shy about it. Speak up, express yourself, and stay fresh.

My challenge is the constant turnover, but it might be the same in all industries. It just seems that in kitchens, skills are passed on quickly from one chef to the next, but in cyber, it can take years to absorb the experience of seasoned professionals. This makes it harder to stay connected to mentors and experts, but it also has its benefits – my network has expanded, and I'm learning from colleagues who have gone on to new roles in different companies.

From coolrooms to cyberspace, crypto scams to AI-driven workplaces, my journey has been one of contrasts. But one thing has remained constant: my desire to learn, adapt and remain positive. My moniker is Cyber Chef (no, not the web Swiss Army knife). I'm taking the skills I learnt in hospitality and using them to push forward and excel in this fast-moving industry. Whether it's a pot luck or a policy, my recipe for success (and one I'm happy to share) remains the same: clear communication, solid confidence, bounds of energy, and a willingness to learn and have fun while doing it.

I hope that wasn't too cheesy and inspires somewhat of a thought. •

Benjamin Riles – aka Cyber Chef – has broken free from the heat of the kitchen, bringing less salt and more sweets to the cyber security industry. Recognised for his strong entry into the field, Riles aims to specialise in security awareness and hopes to one day bolster the security of the gaming industry.

How privilege access management can reinforce your cyber security posture

BY SCOTT HESFORD, SENIOR DIRECTOR OF SOLUTIONS ENGINEERING, ASIA PACIFIC, BEYONDTRUST

AN INCREASING PROPORTION of today's cyber security threats involve the misuse of digital identities.

Indeed, stolen credentials may allow nefarious players to gain access to an enterprise's core systems, where they can cause disruption and damage or steal valuable data. At the same time, misused credentials and digital identities have become a significant problem because of the increase in their use. As a result of the continuing growth in online transactions and cloud-based services, businesses are faced with managing multiple login profiles and IDs.

One of the most effective ways of reducing the threat surface of an organisation is through an identity-centric approach that includes securing privileges and access, while also managing the entire identity attack surface to neutralise identity-specific threats. At the core of this approach is privilege access management (PAM).

PAM focuses on controlling and monitoring access to privileged accounts within an organisation's IT infrastructure. Privileged accounts, often held by administrators, superusers, or other high-level personnel, possess elevated access rights that allow them to make significant changes, install software, and access sensitive data.

PAM seeks to safeguard these powerful accounts by implementing policies, processes, and technologies that mitigate the risk of unauthorised access and potential misuse. One of the primary goals of PAM is the implementation of the principle of least privilege: to limit access to privileged accounts to only those individuals who require it for their specific roles and responsibilities, and time needed.

This is achieved through granular access controls, multi-factor

authentication, session monitoring, and the regular rotation of credentials. By enforcing the principle of least privilege, PAM minimises the attack surface and reduces the likelihood of security breaches resulting from compromised or misused privileged accounts.

One of the key benefits of implementing PAM is its ability to enhance overall digital security. By securing privileged accounts, organisations can prevent unauthorised access, mitigate the risk of insider threats, and safeguard sensitive information. PAM also aids in regulatory compliance, including aspects of the Essential Eight.

PAM solutions also offer visibility into user activities within privileged accounts, allowing organisations to track and audit actions taken by administrators. This not only helps

in identifying potential security incidents, but also facilitates the investigation of any suspicious activities.

PAM tools contribute to an organisation's ability to respond promptly to security incidents, reducing or mitigating the impact of breaches and enhancing overall incident response capabilities.

Implementing a robust PAM strategy to limit digital access to resources across any organisation to the right people – with policies in place to ensure that they are who they say they are, and that they're accessing the right things for the right duration of time – will significantly reduce the spread of entry-level attacks caused by compromised credentials. •



Scott Hesford





PROTECT YOUR **Paths to Privilege™**

➤ **Identity-First Security**

**Let us help you achieve
Essential Eight alignment**

- Application Control
- User Application Hardening
- Restricting Admin Privileges



**Scan here to
learn more**

BeyondTrust is the global cybersecurity leader protecting Paths to Privilege™ with an identity-centric approach. We are leading the charge in transforming identity security and are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at beyondtrust.com



How any organisation can get started with cyberthreat intelligence

— BY CHRIS HORSLEY, CHIEF TECHNICAL OFFICER AND CO-FOUNDER, COSIVE —

It's common for security leaders and analysts to believe that it's impossible to run a cyberthreat intelligence program without a multimillion-dollar budget allocation for tools, feeds and expensive analysts. Meanwhile, many of those same organisations are already doing threat intelligence: they just don't know it yet.



Chris Horsley

GATHERING INTELLIGENCE: BE THE EYES AND THE EARS

Like military intelligence, threat intelligence involves understanding the capabilities and tactics of cyberthreats and adversaries. When doing threat intelligence, we're acting as the eyes and ears of the organisation by providing actionable

intelligence to support decision-making.

Gathering threat intelligence can start with reading industry blogs, participating in cyber security communities, and following what threat actors are doing. Everything we do to gather information on threats, tactics and actors is part of gathering threat intelligence. Security operations teams often have at least one or two operators who are curious, and actively gather and contextualise information about threats.

These operators are already stepping into the role of unofficial threat intelligence analysts.

SHARING INTELLIGENCE: USE WHAT YOU'VE ALREADY GOT TO DISSEMINATE INTEL

Gathering information about the threat landscape can inform our own decision-making and actions; but to benefit others, threat intelligence must be shared. The good news is that many teams are already sharing threat intelligence. Sharing blog posts and reports relevant to your organisation via Slack or a wiki is simple, foundational threat intelligence sharing. Before long, you can move on to machine-to-machine sharing with MISP or STIX.

CONTEXTUALISING INTELLIGENCE: WHAT DOES THIS REPORT MEAN FOR YOUR ORGANISATION?

The difference between raw information sharing and effective threat intelligence involves contextual understanding: analysing and relating threat intelligence to your organisation's own circumstances. This can be as simple as writing three bullet points when sharing a blog post about newly discovered common vulnerabilities and exposures to say that your organisation runs the affected

software, that this is a critical vulnerability, and that you need to take action on this immediately.

By contextualising intelligence, we make it relevant and actionable.

SHARING BEYOND THE SECURITY TEAM: WHO NEEDS TO KNOW THIS?

Threat intelligence shouldn't be kept within security teams; we need to produce threat intelligence products, such as internal reports and feeds. With its capacity to inform better decision-making and courses of action, many people in the organisation stand to benefit from our threat intelligence insights. This stakeholder-centric focus represents a step change in the maturity level of an organisation's cyberthreat intelligence (CTI) practice – from ad hoc, informal threat intel, to the beginnings of a CTI 'program'.

There are two primary stakeholders who are typically most interested in threat intelligence outside the security team: executives and technical teams.

EXECUTIVES AND NON-TECHNICAL TEAMS: SHARE CONCISE REPORTS WITH MUST-KNOW ORGANISATIONAL CONTEXT AND RECOMMENDATIONS

Executives want to understand, at a high level, what sort of threats their organisation is facing to help them make good strategic decisions. A classic example is ransomware. Executives are trying to understand how likely it is that the organisation will be targeted, and what budget and resources they need to allocate to mitigate the risk of ransomware attacks. They may also be thinking about a remediation strategy for a successful attack, including cyber insurance and business continuity planning. Threat intelligence can help them to make more informed decisions in all these areas.

When sharing threat intelligence with executives or other teams like business channel owners, it's best to summarise threats, relevant context and recommended actions in a concise format. Focus on high-level strategic information relevant to executive decision-making (e.g., a concise weekly email briefing or monthly threat report).

TECHNICAL TEAMS: CONTINUAL INTEL FEEDS FOR DEFENDERS AND PLATFORM BUILDERS

Technical teams need to know what systems they run, how exposed they are, and what security controls they have. When we understand the software and systems our organisation uses, we can tell our technical team about highly relevant threats, such as a vulnerability in the VPN concentrator we use that must be patched immediately before it is exploited.

Unlike executives, technical teams often want to be given low-level tactical threat intelligence, like specific indicators of compromise and detection rules (e.g., from

exporting indicators of compromise (IoCs), to tools like Splunk for detection). We must ensure that any automated feeds we provide are not only the right format, but are also actionable, timely, high quality, and minimise false positives.

MEASURING SUCCESS: TRACK PROGRESS WITHOUT JUST COUNTING IOCS

Is the threat intel we're sharing with stakeholders having an impact? To know the answer, we need metrics we can use to measure the success of our threat intelligence program.

It's tempting to choose volume metrics because they're easy to quantify (e.g., the total number of indicators shared or briefings distributed); however, when it comes to threat intelligence, there's often an inverse relationship between volume and quality. It is better to share a low volume of quality threat intelligence than a high volume of noise, which is not relevant, actionable, or useful for stakeholders.

Ultimately, the quality of threat intelligence is determined by how valuable your stakeholders find the intelligence, and if they are able to use it to inform decision-making and operations. Seek their feedback early and often.

START SMALL, SHARE WISELY

Doing CTI well doesn't necessarily require a vast budget allocation or a team of dedicated analysts. Many organisations are already making use of threat intelligence, often without realising it. By leveraging existing resources; focusing on high-quality, actionable intelligence; and sharing it effectively with key stakeholders, organisations can build resilience against threats and make more informed decisions.

Remember that, at its core, the true value of intelligence lies in its relevance and impact to our organisation, not in the volume of data and intel shared. By continuously seeking feedback from stakeholders and adapting your approach to their needs, it's possible to run a successful threat intelligence program even when limited by budget, tools, and people. A full CTI program can be developed over time, but any organisation can get started today if they're willing to start small. •

Chris Horsley is the Chief Technical Officer and Co-founder at Cosive, a consultancy specialising in cyberthreat intelligence and security operations. At Cosive, Horsley leads the company's threat intelligence sharing and MISP initiatives, and is a frequent speaker and trainer at industry conferences and meet-ups on these topics. Prior to co-founding Cosive, Horsley spent many years in the international CSIRT community, including working as an incident responder for both AusCERT and JPCERT/CC, the Japanese national CSIRT.

How ThreatLocker® can help you implement the Essential Eight

THE ESSENTIAL EIGHT are eight mitigation strategies developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) for companies to help secure themselves from cyberthreats. They include:

- patch applications
- patch operating systems
- multi-factor authentication
- restrict administrative privileges
- application control
- restrict Microsoft Office macros
- user application hardening
- regular backups.

THE ESSENTIAL EIGHT MATURITY MODEL

Robust cyber security isn't just an option; it's a necessity. The ASD offers a valuable framework for organisations aiming to enhance their cyber resilience: the Essential Eight Maturity Model (E8MM).

The E8MM is designed to guide you through implementing the Essential Eight cyber security strategies, providing a structured approach to enhance your defences. With each maturity level, except for Maturity Level Zero, you address

increasing degrees of sophisticated threats. This ensures that you're not just keeping pace, but are also staying ahead of the evolving tools, tactics and techniques used by cyber adversaries.

According to the ASD's ACSC, 'Generally, Maturity Level One may be suitable for small to medium-sized enterprises, Maturity Level Two may be suitable for large enterprises, and Maturity Level Three may be suitable for critical infrastructure providers and other organisations that operate in high threat environments'. Organisations should establish a target maturity level and a clear plan, while remaining adaptable to implementing higher maturity levels as their circumstances permit.

HOW THREATLOCKER® CAN HELP

ThreatLocker is a Zero Trust endpoint protection platform that can be utilised as a tool by your organisation in aligning more closely with the higher, more secure maturity levels of the E8MM – enhancing your overall cyber security posture. The following

are just some of the ways that ThreatLocker can help:

- ThreatLocker can help your organisation patch applications by alerting you of discontinued software running in your environment with a free Software Health Report. ThreatLocker Application Control can be used to quickly disable any such software.
- ThreatLocker can help your organisation patch operating systems by alerting you when there is a Windows-related update available on your system.
- ThreatLocker can help your organisation implement multi-factor authentication by having the option to require ThreatLocker administrators to use multi-factor authentication. The ThreatLocker Unified Audit can also not be modified or deleted by anyone, and is held by default for 30 days (but this can be extended).
- ThreatLocker Elevation Control and Ringfencing™ can be used to restrict application administrative privileges.
- ThreatLocker Application Control can help your organisation to implement application control on Windows, macOS and Linux.
- ThreatLocker Configuration Manager can help your organisation restrict Microsoft Office macros.
- ThreatLocker Application Control can help your organisation harden user applications by only allowing what is required and denying everything else, as well as Ringfencing applications to limit what applications can do – whether it's interacting with another application, your files, data, or the internet.
- ThreatLocker Storage Control can help your organisation protect its regular backups by limiting who can access backups. •



To learn more about how ThreatLocker can fortify your defences, book a demo or sign up for a free trial today at threatlocker.com



IMPLEMENT THE ESSENTIAL 8 WITH THREATLOCKER®

Elevate your cybersecurity by leveraging
ThreatLocker® to meet Essential 8 standards.

- ✓ Patch Applications: Use ThreatLocker® Software Health Report and Application Control to remove outdated software.
- ✓ Restrict Admin Privileges: Validate and manage privileged access through ThreatLocker® Elevation Control.
- ✓ Application Control: Ensure workstations are secure with ThreatLocker® Application Control.
- ✓ Block Office Macros: Stop harmful macros in downloaded Microsoft Office files using ThreatLocker® Configuration Manager.
- ✓ Regular Backups: Protect backups from unauthorised changes with ThreatLocker® Storage Control.

And more!

Contact us to
get started!



THREATLOCKER®
ZERO TRUST ENDPOINT PROTECTION PLATFORM

threatlocker.com

BEYOND THE CONTRACT: THE SILENT KILLER OF YOUR BUSINESS

— BY ASRAR ISMAIL, FOUNDER, CYBER DAME —

As technology continues to evolve, we are continuously looking for the next new, shiny thing that we can adopt. Companies are increasingly relying on third-party vendors, suppliers and partners to streamline operations, reduce costs, and boost efficiency. While these relationships can drive growth and innovation, they also expose organisations to myriad risks.



From data breaches to regulatory noncompliance, third-party risks can severely impact a company's reputation, financial stability and operations. This article explores the nature of third-party risks and offers practical strategies for mitigation, complete with a real-world example and an actionable checklist.

UNDERSTANDING VENDORS

The term 'vendor' encompasses a broad spectrum of entities that provide goods, services or resources to an organisation. This expansive definition includes:

- › **Suppliers:** Entities that provide raw materials, components, computer parts or finished products.
- › **Contractors:** Individuals or companies hired to perform specific tasks or projects.
- › **Service providers:** Organisations offering specialised services (e.g., IT support and marketing agencies).
- › **Product providers:** Companies that supply finished goods for resale or use.
- › **Consultants:** Experts providing professional advice and guidance.
- › **Technology partners:** Firms supplying software, hardware, or tech infrastructure.
- › **Outsourcing partners:** Companies to which certain business functions are delegated.
- › **Distributors:** Entities that help in the distribution of products to end users.

WHY HAVE VENDORS BECOME INDISPENSABLE TO ORGANISATIONS?

In an era of rapid technological advancement, global competition and increasing specialisation, vendors play a pivotal role in an organisation's success. Reasons vendors become indispensable include:

- › **Enabling core competency focus:** By outsourcing non-core functions to specialised vendors, companies can concentrate on their primary strengths. For instance, a tech startup might focus on product development while outsourcing HR and accounting functions.
- › **Access to specialised expertise:** Vendors often possess deep expertise in their specific domains. This allows businesses to tap into knowledge and skills that would be costly or time-consuming to develop in-house.
- › **Cost efficiency:** Leveraging vendors can lead to significant cost savings. Bulk purchasing power, economies of scale, and reduced need for in-house infrastructure all contribute to lower operational costs.
- › **Scalability and flexibility:** Vendors provide the flexibility to quickly scale operations up or down in response to market demands. This agility is crucial in today's fast-paced business environment.

- › **Innovation catalyst:** Interaction with a range of diverse vendors exposes companies to new ideas, technologies and processes. This cross-pollination of knowledge can spark innovation and drive competitive advantage.



Asrar Ismail

- › **Global reach:** International vendors help businesses expand their global footprint, providing local market insights and overcoming logistical challenges in new territories.
- › **Risk mitigation:** By diversifying the supplier base, companies can reduce the risk of disruptions. If one vendor faces issues, others can step in to ensure business continuity.
- › **Competitive edge:** Access to top-tier vendors can give companies a significant edge. For example, exclusive arrangements with premium suppliers can differentiate a brand in the market.
- › **Operational efficiency:** Specialised vendors often bring streamlined processes and best practices, enhancing overall operational efficiency.
- › **Capital efficiency:** Utilising vendors for certain functions can reduce the need for large capital investments in equipment, technology or facilities.

While vendors have become indispensable, there are also risks that they bring.

POTENTIAL THIRD-PARTY RISKS

Third-party risks encompass any potential threats arising from an organisation's reliance on external entities to perform services or provide goods. These risks can manifest in various forms, including:

- › **Cyber security vulnerabilities:** Vulnerabilities stemming from third-party relationships pose a significant and evolving threat to organisations. These risks encompass a range of potential exposures, including data breaches facilitated by vendors with access to sensitive systems, insecure application programming interfaces that create backdoors for attackers, shadow IT introduced by employees using unauthorised third-party services, and outdated systems maintained by vendors that are susceptible to known exploits. The interconnected nature of modern business ecosystems means that a single weak link in the chain of third-party relationships can potentially compromise an entire organisation's security posture, leading to data theft, malware infections and other cyberthreats. As such, robust vendor risk management and continuous security assessments are crucial for maintaining a strong



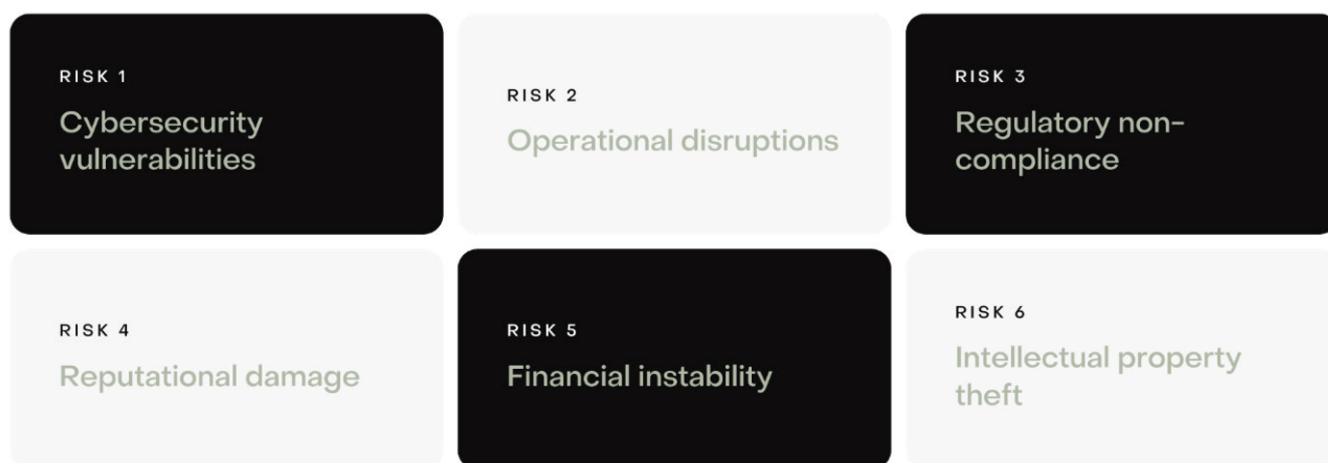
A checklist to manage third-party risk

cyber security defence in today's interconnected digital landscape.

- › **Operational disruptions:** Disruptions arising from third-party dependencies represent a critical vulnerability for modern businesses. These risks manifest in various forms, each capable of severely impacting an organisation's ability to function effectively. Supply chain interruptions can bring production to a standstill, while service outages from key providers like cloud services can paralyse entire operations. Quality issues with vendor-supplied components or services may necessitate costly recalls or lead to service failures, damaging customer trust. Additionally, capacity limitations of vendors unable to scale alongside a growing business can create significant bottlenecks, hindering expansion and efficiency. Collectively, these operational risks underscore the importance of robust vendor management strategies, diversification of critical suppliers, and contingency planning to maintain business continuity in the face of third-party failures or shortcomings.
- › **Regulatory noncompliance:** Organisations face potential liability for regulatory infractions committed by their third parties, particularly in domains such as data protection and financial services. This risk encompasses several key aspects: vendors' mishandling of personal data can result in breaches of regulations like the General Data Protection Regulation, while industry-specific rules in sectors like health care and finance demand stringent vendor compliance. The engagement of international vendors introduces further complexities, as differing regulatory landscapes across borders must be navigated. Moreover, insufficient visibility into vendor processes can hinder an organisation's ability to demonstrate compliance, potentially leading to audit trail issues. Consequently, robust vendor oversight and compliance management are crucial to mitigate the risk of regulatory

penalties and maintain organisational integrity in an increasingly complex regulatory environment.

- › **Reputational damage:** Third-party actions can substantially affect an organisation's reputation, as the public often fails to differentiate between a company and its vendors. This reputational risk encompasses several crucial aspects: a vendor's unethical practices, such as labour violations or environmental damage, can tarnish one's brand by association. Mishandling of customer data by vendors can erode trust in the organisation, while high-profile mistakes or controversies involving third parties can lead to negative publicity. In the age of social media, vendor-related issues can swiftly escalate into a public relations crisis, with the potential for rapid and widespread amplification. Consequently, vigilant management of vendor relationships and proactive reputation monitoring is essential to safeguard an organisation's public image and maintain stakeholder trust in an increasingly interconnected business landscape.
- › **Financial instability:** The fiscal wellbeing of third parties can directly impact an organisation's own financial stability and operational continuity. This risk manifests in several key ways: the bankruptcy of a critical vendor can disrupt operations and incur unforeseen costs, while poorly structured contracts may lead to unexpected fees or price hikes. There's also the risk of financial fraud by vendors, potentially resulting in substantial losses. Moreover, engaging international vendors can introduce currency exchange rate risks. Consequently, thorough financial due diligence, robust contract management and diversification of critical vendor relationships are crucial strategies for mitigating these financial risks. Organisations must remain vigilant in monitoring the financial health of their third parties to ensure their own fiscal stability and uninterrupted operations in an increasingly interconnected business environment.
- › **Intellectual property theft:** Sharing confidential information with external parties can expose your intellectual property to theft or misuse. Vendors who have access to trade secrets may inadvertently or maliciously divulge this information. Additionally, unauthorised use of patented technologies by third parties can lead to patent infringement claims. Counterfeiting is another concern, as manufacturers or distributors may produce counterfeit versions of your products. Finally, unclear agreements regarding data ownership can result in disputes over intellectual property rights.



Some of the critical third-party risks

THE TARGET DATA BREACH

To illustrate the potential impact of third-party risks, let's examine the infamous 2013 Target data breach. In this incident, cybercriminals gained access to Target's network through credentials stolen from a third-party vendor providing heating, ventilation, and air conditioning services to Target stores. The breach resulted in the theft of 40 million credit and debit card numbers, and 70 million customer records.

CHALLENGES AND CONSIDERATIONS

While vendors are crucial for success, their integration comes with challenges. Ensuring consistent quality across multiple vendors can be complex, as different suppliers may have varying standards and capabilities. Managing a diverse vendor ecosystem requires robust communication and coordination to ensure smooth operations, and to avoid conflicts. Over-reliance on key vendors can create vulnerabilities, as disruptions to their services can have a cascading effect on the business. Sharing sensitive information with vendors increases cyber security risks, necessitating careful data management and protection measures. Finally, ensuring that vendors align with the company's values and culture is essential but challenging, as differing perspectives and approaches can hinder effective collaboration.

A COMPREHENSIVE APPROACH

To effectively manage third-party risks, organisations must adopt a proactive and systematic approach. Below is the highlighted strategy on how to minimise the risk associated with cyberthreats:

- 1. Risk assessment:** Conduct thorough due diligence on potential third parties before engagement. Evaluate their financial stability, security practices, regulatory compliance and reputation.
- 2. Contractual safeguards:** Implement robust contracts that clearly define expectations, responsibilities and liabilities. Include clauses for data protection, confidentiality, and the right to audit.
- 3. Ongoing monitoring:** Regularly assess and monitor third-party performance and compliance.

Implement continuous monitoring tools and processes to detect potential issues early.

- 4. Access management:** Limit third-party access to only essential systems and data. Implement strong authentication measures and regularly review access privileges.
- 5. Incident response planning:** Develop and test incident response plans that include scenarios involving third-party breaches or failures.
- 6. Training and awareness:** Educate employees about third-party risks and their role in managing them. Foster a culture of risk awareness throughout the organisation.
- 7. Diversification:** Avoid over-reliance on a single third party. Where possible, maintain relationships with multiple vendors to reduce concentration risk.

CONCLUSION

In today's interconnected business world, vendors are not just external entities, but are also integral partners in an organisation's success. The vendors are an easier target to the intended victim, primarily because they provide the agility, expertise and resources necessary to thrive in a competitive landscape; however, realising these benefits requires a strategic approach to vendor selection, management, and integration.

As businesses continue to evolve, those that master the art of vendor relationships will be best positioned to innovate, grow and succeed in an increasingly complex global marketplace. ●

Asrar Ismail is an accomplished information security professional and a founder of Cyber Dame, specialising in helping businesses implement and audit ISO 27001 and Australian Cyber Security Centre frameworks using Microsoft 365 tools. As both an auditor and implementor, Ismail leverages her expertise to ensure organisations achieve robust security compliance and governance. In addition to her professional practice, Ismail is a passionate educator, having taught at the University of the Sunshine Coast, and has facilitated courses on cyber security governance, policy, ethics, and law at The University of Queensland.

Ready for anything.

Resilience & security in the AI era.



BY PETER SOULDBY, HEAD OF SECURITY, BRENNAN

The AI wave is cresting. Use cases are swelling. Uptake is surging. As AI becomes embedded in business operations, it's easy to get swept up in the excitement of what it can do. But there's a flip side: AI brings with it a new set of challenges, making resilience and security more important than ever. If your systems aren't prepared to handle disruptions, or your security isn't airtight, AI won't be your ally—it could be a vulnerability.

Be it a cyber breach, IT failure, human error, or natural disaster, system outages hurt and are powerful reminders of how interconnected our systems are. Now, imagine the same scenario, but with AI playing a central role in critical decisions or automated processes. The stakes get higher. So does the need for mature, trusted technology partners who can bake resilience

into your IT infrastructure, ensuring AI works for, not against you.

Resilience is about more than just bouncing back. It's about being prepared so you don't have to. Yes, MSPs are well-versed in disaster response and proactive planning, two essentials as AI tools become increasingly integrated into business systems. More importantly, the right MSP also ensures systems are robust enough to withstand interruptions before they occur.

In an AI-driven world, security risks multiply. AI tools can process vast amounts of data, but they're also attractive targets. If hackers compromise an AI system, they could disrupt plenty, from customer service bots to predictive analytics that inform major business decisions.



“We live in a world where risk is on the rise; not just from criminal activity, but from increased complexity, AI’s paradigm shift, stricter compliance and governance requirements, as well as the realities of human error. That’s why we believe true security is always proactive, always testing, always probing, and never takes a break.”

PETER SOULSBY, HEAD OF SECURITY

The role of the MSP in this landscape is crucial—not only to guard against breaches but to protect the integrity of AI-driven systems. They can monitor for threats in real time, ensure data is secured, and provide human, hands-on incident response expertise.

AI may also blur the lines between IT and security even further. As organisations adopt sophisticated AI tools, having one integrated provider who can manage both sides of the equation becomes even more critical. MSPs are uniquely positioned to handle this convergence, offering comprehensive solutions that ensure your IT infrastructure and AI systems are both resilient and secure.

In this new AI era, businesses must be ready for anything. By partnering with a tried-and-true Systems Integrator that can anticipate problems, react quickly, and secure systems proactively, organisations can ride the AI wave without the fear of disruption. Because when technology is moving this fast, resilience and security aren’t merely nice-to-haves. They’re non-negotiables.

brennanit.com.au

1300 500 000

sayhello@brennanit.com.au





Is your organisation ready to adopt a unified approach to identity management?

The Value of a Unified Identity Platform

In today's digital world, with more devices connected and a growing number of users, organisations face increased challenges in managing identities and access rights. As a result, a unified identity approach is on the rise. But what exactly is unified identity and why is it becoming an imperative for businesses?

The Rising Threat of Identity Breaches

Cybercriminals are constantly evolving their tactics and identity is a prime target. A 2024 report by the Identity Defined Security Alliance revealed that 90% of organisations experienced identity-related security incidents in the past year. The financial impact of these breaches is substantial; the Ponemon Institute found that breaches involving stolen or compromised credentials cost businesses an average of \$4.88million USD. The stakes are high and organisations must adopt a revised strategy to protect their digital identities.

The Pitfalls of a Fragmented Identity Strategy

Despite identity's critical role in cybersecurity many organisations still use fragmented identity solutions across their ecosystem for user authentication, access management, threat intelligence and governance. This leads to increased costs, inefficiencies and security challenges:

- **Integration Issues:** Various identity tools may not work seamlessly together undermining rapid response and detection to identity threats both during and after authentication.
- **Operational Inefficiencies:** Multiple identity solutions increase costs, add operational friction and divert time and focus from IT and security teams.
- **Increased Phishing Risks:** Users often require different login credentials for each vendor, heightening the risk of phishing attacks which account for 16% of data breaches (according to IBM).

Looking Beyond Authentication

Focusing only on authentication can create security gaps. Security and IT leaders should consider the entire identity lifecycle – from onboarding to access management. A wholistic approach helps organisations strengthen defences by identifying and addressing vulnerabilities at every stage of identity management ensuring a more comprehensive security posture.

The Case of a Unified Identity Platform

Instead of managing multiple tools, organisations are moving towards a more unified approach to Identity. According to Gartner, by next year 70% of new deployments in access management, governance, administration and privileged access will be unified identity and access management platforms. This shift reflects the benefits a unified approach offers:

- **Wholistic view of Identity:** A unified platform provides a comprehensive view of all identity data helping organisations identify vulnerabilities and manage access more effectively.
- **Consistent Security Policies:** Organisations can enforce secure-by-design access policies consistently across all users, resources and devices.
- **Faster Threat Detection and Response:** With a unified identity platform, organisations can detect and respond to threats more quickly mitigating risks before they escalate into authentication-based attacks.

A unified identity platform provides a comprehensive solution that addresses the evolving identity needs of organisations, enhancing security, reducing costs and complexity, and improving user experience—all within a single, unified system.

Is your organisation ready to adopt a unified approach to identity management?

okta.com/au



Identity is mission-critical
security infrastructure.

okta

The World's Identity Company

Learn more at okta.com/au

THE THREE 'R'S YOU NEED ON YOUR CYBER SALES RADAR

— BY PAUL MALEY AND MEG TAPIA —

Three statistics every cyber professional needs to know.

Statistic number one: by the end of 2024, the global cyber security industry will be worth around US\$194 billion.

If you think that figure is large, you'd be right. It's more than twice the size of the United Kingdom's defence budget, and is larger than the gross domestic product of more than half of the world's countries, including countries like Kuwait, Hungary and Slovakia.

But as eye-watering as that number may be, it pales in comparison to the projected size of the industry, which, by some estimates, is set to grow to US\$563 billion by 2032.

What's driving that astonishing growth? Cybercrime? The post-COVID digital uplift? A proliferation of cyber compliance regimes and privacy legislation? Yes, and no.

The single biggest force driving new cyber security spending is the rapid adoption of new technologies.

Don't assume that includes artificial intelligence (AI), by the way. AI, machine learning and things like post-quantum encryption might be dominating the headlines, but their impact on the cyber security industry is, at this stage, modest – at least when set against more conventional challenges.

According to Statistica, the big growth areas involve securing the rapid adoption of new technologies, like cloud-based applications and Internet of Things security. These are large-scale transformations valued in the tens of millions of dollars, and which take years to implement.

One day, AI might up-end the cyber industry, but, right now, what most customers want is reliable detection and response products that effectively integrate the spectrum of threat vectors across a customer's estate – from legacy gateways and cloud applications, to endpoint security.

Statistic number two: while the private sector might be the single-biggest customer for cyber security products and services, the second-largest is government.

According to Statistica, the banking, financial services and insurance sector accounts for 32.61 per cent of the industry, but government is not far behind, accounting for 24.1 per cent.

This should surprise no-one. Government is the single-largest actor in most economies, and as the size of government grows, so too do its cyber needs. The proliferation of cyber compliance regimes, particularly around critical infrastructure, is another key driver.

Statistic number three: only one company – Microsoft – has more than 15 per cent of market share. IBM has 11 per cent, Accenture and Broadcom Inc. have five per cent, and Palo Alto Networks has four per cent.

A whopping 46 per cent of the market is serviced by companies in the 'other' category and, if you're reading this, chances are you're with one of them.

Taken together, what do these statistics tell us?

They tell us that the cyber market is massive and growing, that customers still want traditional cyber fixes, and that the vendor market is fragmented, with an untold number of small and medium-sized enterprises (SMEs) vying for business that is definitely up for grabs.

With so many companies selling cyber products, the challenge for most vendors, therefore, is how to be heard above the noise.

So what's the answer there? Again, it comes in threes.

The first is relevance. Too often, cyber vendors approach government with product-led sales strategies. This might work at a retail level, but enterprise-level challenges need a different approach. Pitching government customers with a new product is like trying to sell blue-coloured widgets to a client that has white. Your customer might prefer blue, blue might even be cheaper, but the aggravation associated with changing from white widgets to blue is usually not worth it. Government contacts tell us that the differentiation is often too insignificant to be worth the inconvenience of change.



The other problem with this approach is that it virtually guarantees your sales force will be relegated to the lower echelons of the public service. Responsibility for widget colour policy is a mid-level management problem. The strategic direction of a 6000-person strong government department and the technologies leveraged to enable that direction is a CISO or Deputy Secretary problem.

Engaging with procurement officials is important, but if you want to sell at the enterprise-wide level, you need to get higher up the food chain. The vendors that have the most success with government are those that successfully position their products as strategic capabilities, rather than discrete software offerings that might be considered optional extras. This increases the opportunities for enterprise-wide purchase orders, while at the same time repositioning their brands within the government marketplace.

How do the most successful companies do this?

This brings us to the second concept: relationships. Every sales executive knows the value of trusted relationships. In government, they're crucial. Governments are rigidly hierarchical, much more so than the private sector. It's true that the larger a corporation becomes, the more bureaucratic it gets – a fact that often complicates engagement. But compared to governments, SMEs are flat structures, meaning the point of initial contact matters less.

In every kind of business, relationships are the beating heart of success. Focusing on balance sheets and innovative products matters, but not as much as cultivating strong relationships with customers. By forging trust and loyalty, a good vendor–client relationship will give you insights into client challenges that no request for tender will articulate.

Companies like Microsoft, IBM and Accenture don't think about sales transactions, they think about transformative change. They focus on turning

contacts into allies and contracts into partnerships. They offer collaboration and problem-solving, not just blue-coloured widgets, opening doors to opportunities before they hit the market.

The third concept is risk. Governments are risk-averse. The old joke about never getting fired for buying IBM is funny (sort of) because it's true, figuratively speaking. Persuading any ICT decision-maker to reconfigure their estate is a big ask, usually because it involves asking them to take a risk on the unknown. The safe course is usually to do nothing, or, when forced to make change, to build incrementally on known capabilities whose efficacy has been tested.

New vendors building relationships inside government often forget what a big ask they make of government clients. This will get harder if the legal landscape for cyber professionals changes, as seems likely. Civil, and even criminal liability, for data breaches is moving from the board and C-suite to the CISO level. In the long run, this will be good for cyber security, but it won't make decision-making any easier.

An engagement strategy focused on risk mitigation reassures government clients that you have the capacity and strategic foresight to proactively address potential challenges. This builds confidence, which, in turn, builds trust in your cyber products and commitment to their success.

The next time you're thinking about how to position your company in a crowded cyber market, look at your approach to relevance, relationships and risk. Are you selling blue-coloured widgets, or are you positioning as a partner for long-term stability and growth? ●

Paul Maley is a journalist, policy adviser and Director of Hemisphere East, a consultancy firm that advises cyber clients.

Meg Tapia is Managing Director of Novexus and Special Adviser to Hemisphere East.

Cyber security for the cloud era

AS BUSINESSES USE artificial intelligence and the cloud to sharpen their competitive edge and push the boundaries of innovation, the technology world is entering into a groundbreaking period of change. It is both uncharted and exciting.

In the face of this new frontier, thought-leading organisations have shifted their approach to security, and have evolved the way they approach risk in the cloud. This new approach maximises the impact of security team resources, and drives down the number of critical issues in their environment until they reach zero. This is so security is never a barrier to change; but, rather, is an enabler.

Today's reality requires security teams to navigate an ever-growing array of services and technologies. The attack surface is expanding, so how do you avoid blind spots? The solution isn't just about adopting tools; it's about embracing a new cloud operating model where security is a shared responsibility.

In this model, security isn't just the job of one team; it's woven into the fabric of development, operations and every cloud initiative. Developers ship updates daily or even hourly, and to support this pace, security must be agile and integrated. With better visibility and real-time insights, both security and development teams work together seamlessly, addressing risks before they become threats.

Instead of security being a bottleneck, it becomes an enabler of innovation. When teams work together, security efforts scale as the cloud infrastructure grows. This model empowers everyone – from developers to security experts – to stay aligned and manage risk without impeding progress.

The results of this approach speak for themselves.

'[We get] all the context and information we need to identify what we need to do, how we should act, and which vulnerabilities are the highest priority ones to

remediate,' says Agoda's Chief Information Security Officer. 'For our on-premises environment ... queries give us information and guidance on remediation, which is very helpful for DevOps.'

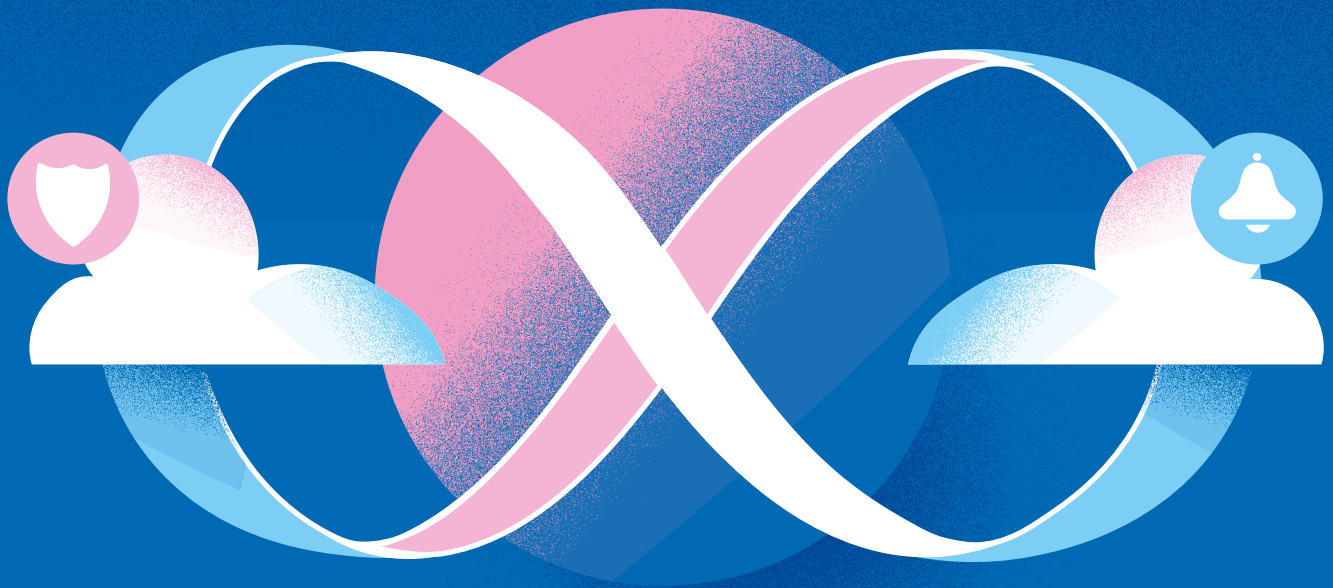
'Maintaining our security posture is invaluable work, but if our engineers have to search for information for each incoming security alert, they're not able to work on other projects,' says Ansarada's Chief Operating Officer. '[Now], they have access to detailed information at their fingertips to fix an issue and get back to writing code for new products that we're excited about.'

It's not just about minimising risk; it's about fostering a culture of shared accountability for maximum business impact. As cloud adoption grows, so does the need for a unified approach. By embracing this collaborative mindset, businesses can unlock the full potential of the cloud, driving growth while staying secure in a rapidly evolving digital landscape. •





Unified Cloud Security from Prevention to Detection



Understand how **WIZ** cloud security provides
full-stack visibility and pinpoint accuracy
to help you prioritize critical risks.

See Wiz in action at wiz.io



Age restrictions on social media

— BY KYLE WATERS —

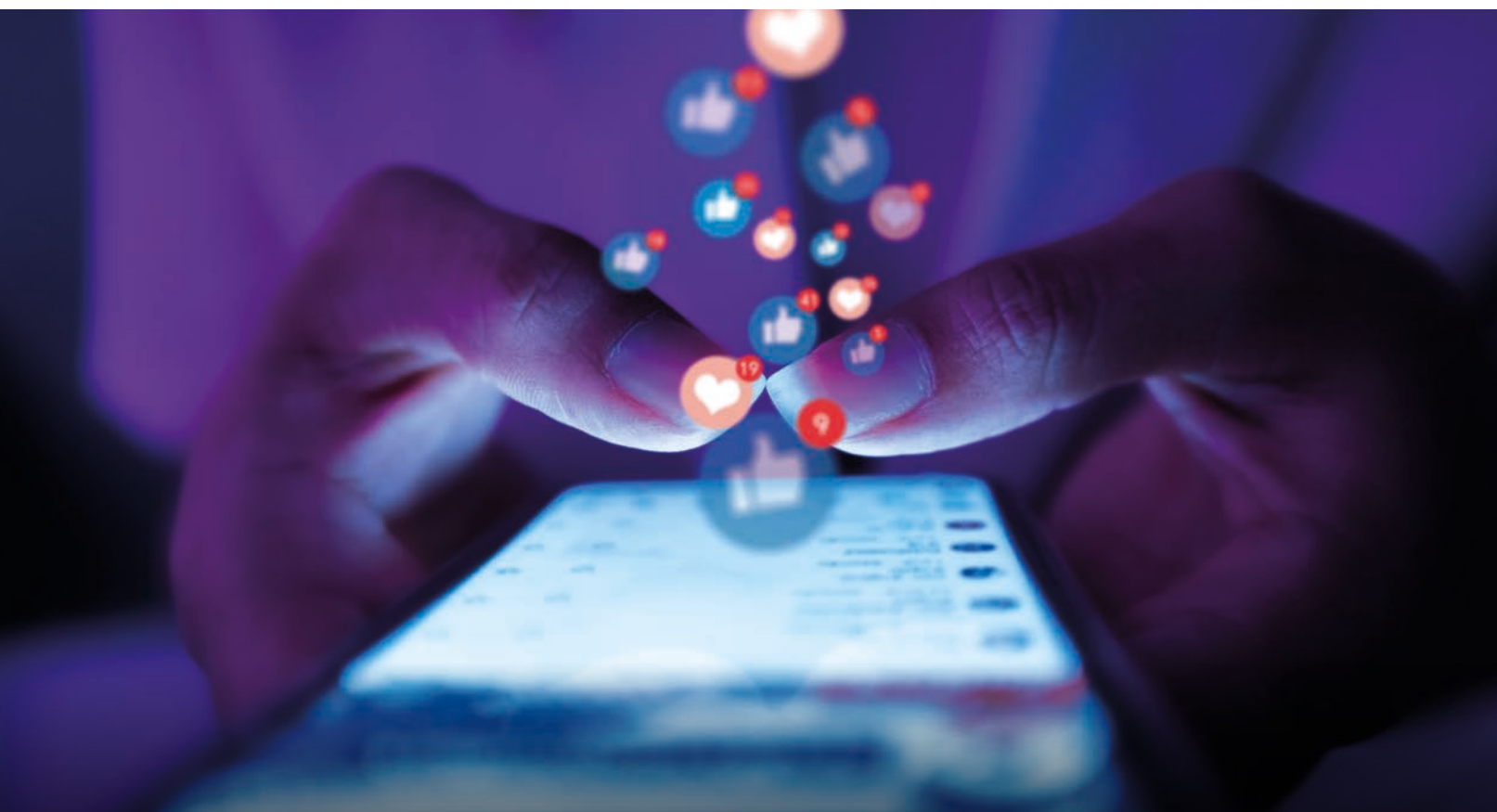
Think back to when you were a teenager – specifically when you were at school and all those students you knew (or maybe you were one) were smoking or drinking underage. A lot of people would think of it as a normal part of growing up, because while all the different laws and legislations were in place to stop anyone under the age of 18 from doing that, everyone knew or were aware of someone that still did it.

The new legislation about age restrictions on social media that the government and opposition are looking to pass is no different to the laws passed to prevent kids from smoking and drinking underage. While it is a very well-intentioned piece of legislation, it is also rushed and poorly considered, because, in a perfect world, what the legislation would do is (at best) force kids to learn about the dangers within social media – like extortion and sextortion, harassment, bullying, data and privacy breaches, catfishing, misinformation,

phishing, and so on – after they reach a certain age, and still by themselves.

In most cases, current age restrictions on most websites usually consist of either a question box asking if the user is the correct age (such as ‘Are you over 18?’), or asking the user for their date of birth and, in a very few cases, possibly asking for a verified profile to be created before allowing access. All of these methods release the owners of the website from the responsibility of anyone underage from accessing the website, putting the onus on the user being 100 per cent truthful about the details they’re providing, as well as making them liable for any wrongdoing caused to or by them.

It is true that this method of age restriction can be used as a temporary stopgap until a better and more permanent solution can be put in place; however, this is not what has been proposed by the legislation because the Australian Government has taken the shortest route to a solution that it doesn’t fully understand, for



a problem that it also doesn't fully understand, and it's basing this on the information being provided by other people that also do not fully understand the situation.

As an analyst, I enjoy data; so, after looking over the information provided to the public by the government, the media coverage, speaking to students and teachers, and discussions with other cyber professionals (both for and against the age restrictions), I have concluded that the legislation at its most optimistic would only be about 25 per cent effective. The rest would be like age restrictions on smoking and drinking, in that if you don't want to be restricted and have the right false ID, or know someone old enough, then you can bypass the laws and gain access, which most (including those already using social media) will undoubtedly do. The reason for this is that by the time most children are 12 years old, they will already have two to three social media profiles (including gaming profiles), not to mention the fact that, on average, at least 42 per cent of kids have a smartphone/device by age 10, 72 per cent by age 12, and 91 per cent by age 14.

So, if age restrictions on social media isn't the way forward to protect our kids, then what is?

Well, the answer to that, dear reader, is cyber awareness and education in schools, specifically within the later stages of primary school (grades 5 and 6, possibly even grade 4), all through high school, and even beyond into tertiary education.

The reason for education over legislation is simple: if you teach kids how to be safe and what the repercussions of not being safe are, then you are not only preparing them for the dangers that are present, but you're also preventing them from having to discover the dangers themselves the hard way – much like the way kids are currently taught about sexual health and STDs in schools. The fact that there are no current federal requirements for schools to include cyber awareness in education and, at the state level, that there is no real consistency between what is required and what isn't, means that kids are stepping out into the digital world blindfolded.

If the Australian Government and the opposition want to truly make an effective and long-lasting change that will protect kids from harm, then other solutions should be considered – such as incorporating cyber awareness into the current IT curriculum as a module, regular in-school programs performed by schools, or by getting industry professionals in to do talks and

presentations – providing schools with resources and volunteers to help them provide any education around cyber until a proper solution can be implemented.

But one of the most important things that was ignored before the legislation was put forward was actually talking to the students who are affected by these issues, and finding out what they are dealing with, what they believe the solution to be, and not just assuming we already know.



Kyle Waters

...by the time most children are 12 years old, they will already have two to three social media profiles (including gaming profiles), not to mention the fact that, on average, at least 42 per cent of kids have a smartphone/device by age 10, 72 per cent by age 12, and 91 per cent by age 14

Social media is so ingrained in our day-to-day culture as adults, but it is also ingrained in theirs; they use it more often to communicate and socialise with family and friends, learn through research and publications, create their own small businesses, develop basic and complex social skills, and create and distribute content. To sum it up: it is how they have learnt to connect with the larger world.

In an article recently published by another masthead, students in New South Wales basically said the same thing I am saying – they even implored the government to not put through a legislation that will impose age restrictions because they're adamant it will not work. More significantly, they even asked for digital and social media literacy

to be taught in schools instead of restricting their access, because they knew that in order for true protection and safety to be achieved, knowledge must be gained.

The digital world is indeed a dangerous place, but so is the non-digital world. If we made the same effort to teach kids how to navigate one as much as we try to do with the other, then not only will they be able to walk a bit safer in both, but they will be able to build off our knowledge, add their own, and pass the whole lot onto the next generation who will do the same, all because, as a society, we made the decision to educate and not legislate. •

Kyle Waters is a self-described 'polymath' who, in addition to various retail, hospitality and volunteer roles, has worked in numerous technical and support roles over the last 20 years. Waters has developed an extensive range of knowledge and training across multiple disciplines and qualifications – such as a Certificate IV in Cybersecurity, ITIL V3 and V4, CCNE L1 and 2, Certificate III Training and Mentoring, and Certificate IV Sound and Lighting, to name a few – most of which he undertook while working full-time in unrelated fields.

Secure an income while you secure your future in cyber security

EDITH COWAN UNIVERSITY (ECU) is creating opportunities for students to earn while they learn, by providing a paid internship program with global technology giant IBM and its clients right across Western Australia.

The successful program focuses on high-demand skill areas key to Western Australia's digital economy, with ECU graduates working in the industry as software engineers, data scientists, mobile application developers and project managers – many of them straight out of university.

Jakub Antoniewicz is one of them, securing a full-time job as an applications engineer with IBM during his internship, while completing his final year of a computer science degree, majoring in software engineering.

'That was a great way for me to prepare for the workforce,' says Antoniewicz. 'During my internship with IBM, I got to develop an internal application for a client that

I continued to work on during my graduate position, [which] is now used by over 300 unique users every week.

'It's extremely rewarding to be able to get an opportunity that allowed me to help people so quickly in my career.'

WORK-INTEGRATED LEARNING WORKS

According to ECU alumnus Dr Christopher Bolan, work-integrated learning (WIL) is a 'significant opportunity for all involved'.

The Co-founder of successful cyber company Seamless Intelligence, Dr Bolan says his team fosters students' potential each year through the program.

'The ECU WIL program is fantastic for both students and the industry. It gives the students real-world experience within well-known companies in their chosen sector, and therefore increases their employability post graduation,' says Dr Bolan.

'Our approach has been to create projects that explore new ideas. This gives the students a chance to extend their skills without some of the pressure/demands of customer-facing work.'

AUSTRALIA'S BIGGEST CYBER SECURITY CENTRE AT YOUR FINGERTIPS

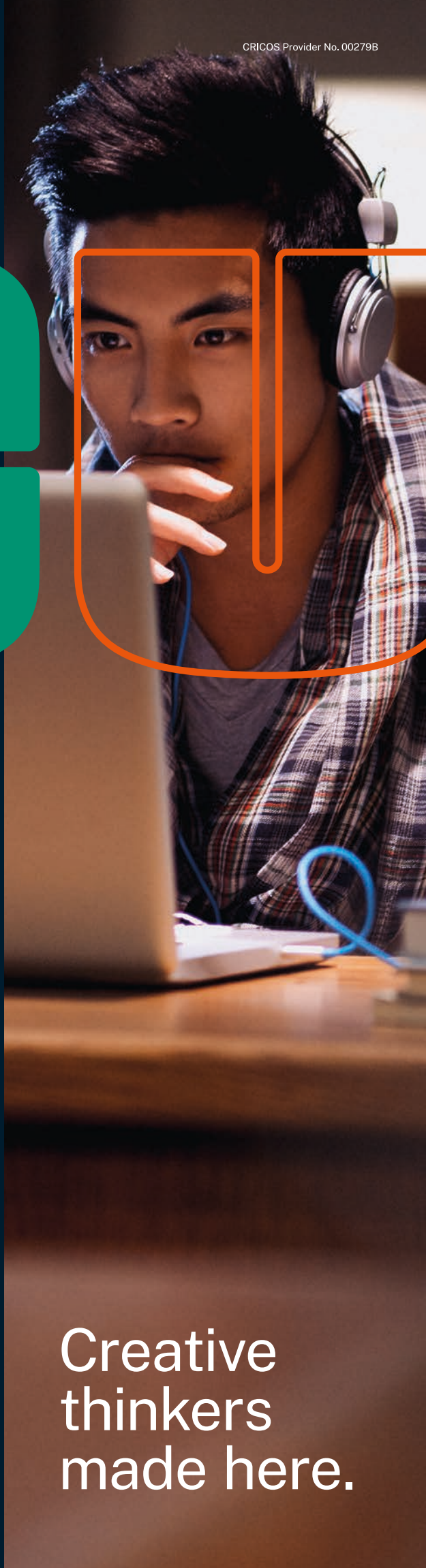
ECU is home to one of Australia's largest security operations centres – the first of its kind in an Australian university, and one of only a handful worldwide.

It's in this world-class facility that cyber security experts investigate the nature of ransomware attacks and develop countermeasures.

The facility gives students the opportunity to gain the real-world skills needed to thrive in any cyber career. ●

To learn more about how to secure your cyber security future, visit ecu.edu.au/research/sri





Stay one step ahead with Australia's only International Cyber Security Centre of Excellence.

With our reliance on internet-based technology, there's never been a greater need to protect Australian businesses, government and the community.

ECU offers the largest academic cyber security and research program in Australia. We are the first and only university from Australia to join the International Cyber Security Centre of Excellence as an Affiliate Member. This organisation was initiated in 2019 by universities across UK, Europe, the US and Japan and acts as a hub for cyber security research, education and advocacy.

ECU's School of Science offers world-class research in Critical Infrastructure Security, Emerging Technologies, and Secure Systems, and has a history of delivering successful research projects for State, Federal and Defence agencies. Our cyber team includes a member from the Interpol Global Cybercrime Expert Group.

We welcome the opportunity to discuss research collaborations with public and private businesses and individuals who have a shared interest in the security industry.

For more information
[ECU.EDU.AU/RESEARCH/SRI](https://ecu.edu.au/research/sri)

**Creative
thinkers
made here.**



TRAINING
A  tesseract Company



LEADING IT FOR

30
YEARS

TAKE YOUR CAREER TO THE NEXT LEVEL

**CISSP®, CISM®, CRISC®, SABSA®,
CISA®, CCSP®, CIPP/E, CIPM, CIPT,
ISO 27001, CSF+P + MORE...**

World-class instructor led training
keeping you at the forefront of
Cyber Security

alctraining.com.my

HRDF FUNDING AVAILABLE

Please speak with us
on how we can help
you apply



Scan here for our
full upcoming schedule

PROFESSIONAL CYBER SECURITY CERTIFICATIONS

FOUNDATION TO ADVANCED LEVELS – OFFERED VIA FACE TO FACE, VIRTUAL OR SELF-PACED.

Cyber Security Foundation+Practitioner™

5 Days

This flagship course is the standout training program for anyone who needs a sound understanding of Cyber Security. The ideal base on which to build your career or upskill your team. Proven over many presentations, the course features a robust syllabus with a strong emphasis on practical exercises and local content to reinforce understanding.

CISSP® Certified Information Systems Security Professional

5 Days

CISSP® is long regarded as the gold standard of security qualifications. This intensive 5-day course provides information security professionals with a fully-immersed, minimum-distraction training experience that will broaden and deepen understanding of all CBK domains.

CISM® Certified Information Security Manager

4 Days

CISM® defines the core competencies and standards of performance expected of a world-class information security manager. It provides executive management with the assurance that those who have earned their CISM have the experience and knowledge to offer effective security management and advice.

CRISC® Certified in Risk & Info. Systems Control

4 Days

CRISC® prepares IT professionals for the unique challenges of IT and enterprise risk management and positions them to become strategic partners to the enterprise. This course comprehensively covers the full CRISC syllabus and prepares for the CRISC exam.

CISA® Certified Information System Auditor

4 Days

CISA® is the global standard among information systems (IS) audit and control professionals. Possessing the CISA designation demonstrates proficiency and is the basis for measurement in the profession. The course comprehensively covers the full CISA syllabus and prepares for the CISA exam.

CCSP® Certified Cloud Security Professional

5 Days

Attackers never rest, and along with all the traditional threats targeting internal networks and systems, an entirely new variety specifically targeting the cloud has emerged. The six domains of CCSP provide a thorough coverage of the security risks and mitigation strategies critical to data security in the cloud.

SABSA® Foundation

5 Days

Getting your architecture right is key to effective security. SABSA® is the world standard for security architecture and ensures that the security needs of your organisation are completely met as an integral part of your IT management infrastructure.

NIST Cybersecurity Framework Practitioner®

5 Days

ALC's NIST Cybersecurity Framework Practitioner (CFP) course immerses participants in all aspects of the theory behind the framework but applies a regional flavour on how the framework can be applied to an Australia or New Zealand context through extensive use of local case studies.

ISO/IEC 27001 Lead Implementer

5 Days

ISO 27001 is the international standard for effective Information Security Management Systems. This course provides comprehensive coverage of all aspects of an ISO 27001 project for implementing and maintaining a successful Information Security Management System.

ISO/IEC 27001 Lead Auditor

5 Days

ISO 27001 is the recognised international standard for best practice in information security management systems (ISMS) within any organisation. This course will prepare you to plan and execute audits of information security management systems in line with the international standard ISO/IEC 27001.

OWASP Top 10 Practitioner Course

2 Days

The OWASP Top 10 Training Course is designed to arm developers and IT professionals within your organisation with the most current knowledge and skills in web application security. The primary objective is to enhance their understanding and ability to combat the most significant security threats prevalent today, as identified by the Open Web Application Security Project (OWASP) in their widely recognised Top 10 list.

OffSec OSCP Bootcamps and Subscriptions

We have partnered with OffSec as their only Learning Partner in Australia and New Zealand delivering OSCP Bootcamps for penetration testers looking to advance their career. Along with OSCP, we are also the one stop shop for all their online self-paced certification including, but not limited to:

SEC-100: CyberCore – Security Essential

PEN-103: Kali Linux Revealed

SOC-200: Foundational Security Operations and Defensive Analysis

TH-200: Foundational Threat Hunting

WEB-200: Foundational Web Application Assessments with Kali Linux

Self-paced and Exam Only offering:

If you have been self-studying, need to take the exam again or want to update your certificate to the latest version, we can help with self-paced bundles and exam only purchases at the best possible price.





RMIT University Leading the Way in Cyber Security

RMIT University is a global university of Technology, Design and Enterprise. We have a rich cyber security eco-system, having been the first institution in Australia to offer a Master of Information Cyber Security degree in 2000, to today where we have a full circle teaching suite and world leading cyber security researchers.

Our cyber program offerings span from vocational education certificates, through to undergraduate and post graduate teaching programs and training offerings, all of which are deeply connected with industry partnerships. We apply a multi-faceted approach to all our activities in the cyber security field at RMIT, looking beyond the technical aspects to include organisational and human aspects.

#1 in Australia

in 2022, RMIT won the Award for Most Popular Career Services in Australia*

12,456 industry placements

for students in 2022

#1 globally

for our efforts to reduce inequality**

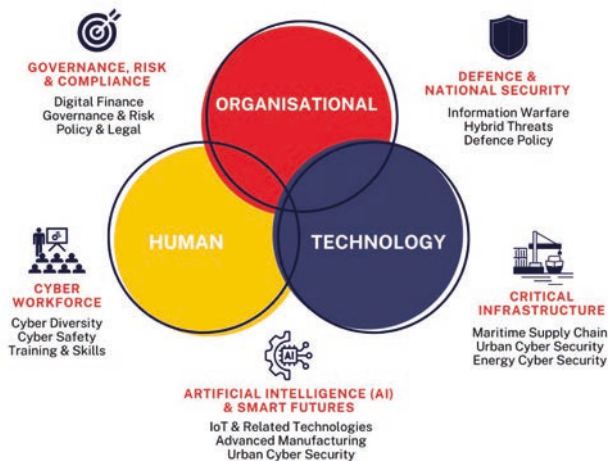
*Australian Association of Graduate Employers (AAGE), Graduate Recruitment Industry Awards 2022,

**Times Higher Education (THE) University Impact Rankings 2023

RMIT's Industry Focused Cyber Research and Teaching



RESEARCH DOMAINS & THEMES



Cyber Research at RMIT

Established in 2020, The RMIT Centre for Cyber Security Research and Innovation (CCSRI) is an award-winning global centre with a multi-disciplinary and applied approach to research, education and innovation within cyber security, considering the human, organisational and technological aspects of the field.

The Centre brings together more than 50 researchers from across RMIT University's STEM, Business and Law, Design and Social Context Colleges in both Australia and Vietnam.

The Centre for Cyber Security Research and Innovation works with industry, government and academia in Australia and internationally to focus on many different areas of cyber security, including governance, risk and compliance, cyber workforce, defence and national security, as well as artificial intelligence and smart futures.

RMIT Industry Focused Teaching

The School of Computing Technologies provides world class computing research and innovative information technology education. The School offers Cyber security programs at undergraduate and post graduate levels in collaboration with industry partners. Students learn technology fundamentals in the RMIT signature Bootcamp2Studio model, and then master the concepts of cyber security in advanced courses. RMIT's industry partnerships provide internship and work-integrated learning opportunities in cyber industries to work on realistic projects, learn teamwork and develop cyber solutions for the end users. The School's offerings in AI, Data Science and Software Engineering augment in developing cyber security dynamic capabilities. A strong nexus between research and teaching in the cyber security area ensures that our students learn the latest techniques in solving industry problems.

Connect with us today

RMIT Centre for Cyber Security Research and Innovation



RMIT School of Computing Technologies



Money see, money do: why ransomware isn't going anywhere

*For all the grandstanding, most Australian companies are just paying up, according to **David Braue**.*



For a company that exists to strengthen the security of its customers' IT environments, the recent news that security giant Fortinet had itself been breached was bad enough. But when negotiations went south because the company wouldn't pay the ransom, it began living many companies' worst nightmare, as 440 gigabytes of confidential data was reportedly published in an Amazon S3 bucket that was made available to anybody who wanted it.

While acknowledging the breach – which Fortinet said occurred when an individual gained access to a limited number of files stored in a third-party, cloud-based file storage system – the company had minimised its likely scope by arguing that the compromised data 'included limited data related to a small number (less than 0.3 per cent) of Fortinet customers'.

With a global customer base of more than 775,000, this breach would have compromised around 2265 customers – or around 194 mebibytes of data, on average, per customer. And while this particular incident may not have involved a conventional ransomware infection, its compromise of so much data reflects a new normal of ransomware, in which many cybercriminal gangs are focused more on exfiltrating data and simply releasing it if a ransom is not paid.

For many years, Australian government bodies have proclaimed loudly that companies should not give in to ransomware demands, relying instead on protective infrastructure, such as file surveillance tools and air-gapped backups, to ensure that they can recover data if ransomware strikes.

A recent Censuswide-Cohesity survey of 300 Australian IT and security executives, however, suggested that the reality is quite different: 81 per cent of respondents admitted paying a ransom during the previous two years, even though 73 per cent said the official policy of their company was to never do so.

Defiance quickly wilts when the reality of ransomware hits. With just four per cent of respondents saying they were able to recover data and restore their business processes within three days, 92 per cent were willing to pay a ransom if necessary to get back up and running.

With 72 per cent of respondents confirming that they had been hit by ransomware during the second half of 2023 alone, the survey confirmed

that ransomware remains incredibly profitable for cybercriminals – with 64 per cent of respondents saying that their companies would be willing to pay over \$4.5 million (US\$3 million) to recover their data and business processes.

Ransomware, in other words, has evolved from being an occasional accident into a significant, persisting risk that, like many other types of risk, has been grudgingly accepted as just another cost of doing business in 2024.

AN EQUAL OPPORTUNITY IMPLODER

Despite governments' increasing efforts to curtail their activities, ransomware gangs have refined and intensified their attacks with remarkable success.

Fifty nine per cent of organisations globally were hit by ransomware last year, as security firm Sophos noted in its State of Ransomware 2024 report, which found that percentage slightly lower in Australia at 54 per cent.

That means that on any given day, a large number of Australian CIOs and CISOs at ransomware-affected organisations are working to evaluate, contain, counter and potentially negotiate a settlement with cybercriminals.

In August alone, ransomware gangs – such as RansomHub, Lynx and Rhysida – compromised targets including engineering firms Hudson Civil Engineering, Kempe Engineering and McDowall Affleck;

mining interest Evolution Mining; disability support organisation Engedi; insurance underwriter All Parks Insurance; hearing services provider Bloom Hearing; furniture retailer Early Settler; and more.

Government bodies are also being routinely hit by ransomware, according to newly released data that, iTnews reported, revealed federal government departments and agencies had suffered 257 data breaches between 2020 and 2024 – 70 of which were due to malicious or criminal attacks – and dealt with 14 ransomware infections last year alone.

Sophos found contemporary ransomware to be highly effective at spreading across a victim company's environment, with just over a third of respondents saying the malware impacted between 51 per cent and 80 per cent of their devices – confirming that ransomware remains tricky to unpick once it has established a foothold in a victim environment.

This is particularly problematic for environments such as health care, where – as Australian organisations

**Fifty nine per cent
of organisations
globally were hit
by ransomware last
year, as security firm
Sophos noted in its
State of Ransomware
2024 report,
which found that
percentage slightly
lower in Australia at
54 per cent**

such as MediSecure, St Vincent's Health and Western Australia's Harry Perkins Institute of Medical Research have recently learnt all too well – ransomware attacks on mission-critical systems can leave healthcare facilities unable to perform surgeries and other basic functions.

Some ransomware infections are a by-product of well-intentioned configuration changes, such as at one Australian healthcare organisation that was recently hit by the BlackCat ransomware gang after it set up a firewall rule exposing Windows Remote Desktop Protocol (RDP) access to the internet at large.

That left it vulnerable after the ransomware gang accessed data from a credential stuffing attack – which, as Cythera Senior Cybersecurity Consultant Alistair Longley told this year's AusCERT Conference, 'got a hit on our client [after] a known username and password was sprayed against the internet indiscriminately'.

'That client ended up in a Pastebin list,' Longley explained, referring to a public forum where credentials are openly shared between cybercriminals, who index and access them in what he called 'about as open source intelligence as it gets ... You can literally just google an IP address and get the username and password'.

Once BlackCat acquired the credentials, it logged into the healthcare provider's network. Within 12 hours, Longley – who was part of a Cythera team called to investigate the breach by the company's insurer – said the gang had secured administrator privileges and had 'complete control over everything'.

Within 16 hours, he said, all of the medical provider's data had been exfiltrated as every single server and workstation was progressively 'completely encrypted with ransomware'.

The compromise of healthcare organisations is particularly problematic because they secure 22 per cent more data, on average, than companies in other industries, according to a recent Rubrik analysis, The State of Data Security, which also found that the average healthcare organisation loses 20 per cent of its total sensitive data holdings whenever there is a successful ransomware encryption event. This is far higher than the six per cent, on average, across other industries, suggesting that the wide diversity of healthcare organisations' often-outdated systems continues to plague efforts to protect life-critical systems and sensitive data holdings, growing over five times faster than the global average.

SQUARING OFF AGAINST MORE ATTACKERS THAN EVER

Despite law enforcement organisations' recent take-downs of ransomware groups like LockBit, Conti, Trigona and Dispossessor, the financial success of ransomware continues to attract a steady stream of new entrants.

During the first half of 2024, security firm Rapid7 observed 21 new ransomware groups – with its Ransomware Radar Report finding that the number of 'leak sites' increased 23 per cent to 2611 for the half year, with one new entrant, RansomHub, posting details of 181 ransomware victims between February and June alone.

Despite law enforcement organisations' recent take-downs of ransomware groups like LockBit, Conti, Trigona and Dispossessor, the financial success of ransomware continues to attract a steady stream of new entrants

Rapid7 also observed a decline in the number of active ransomware families, suggesting that groups are refining their attacks and focusing on high-value targets in industries like health care, which accounts for 21 per cent of all ransomware incidents, as found by a recent Barracuda Networks analysis.

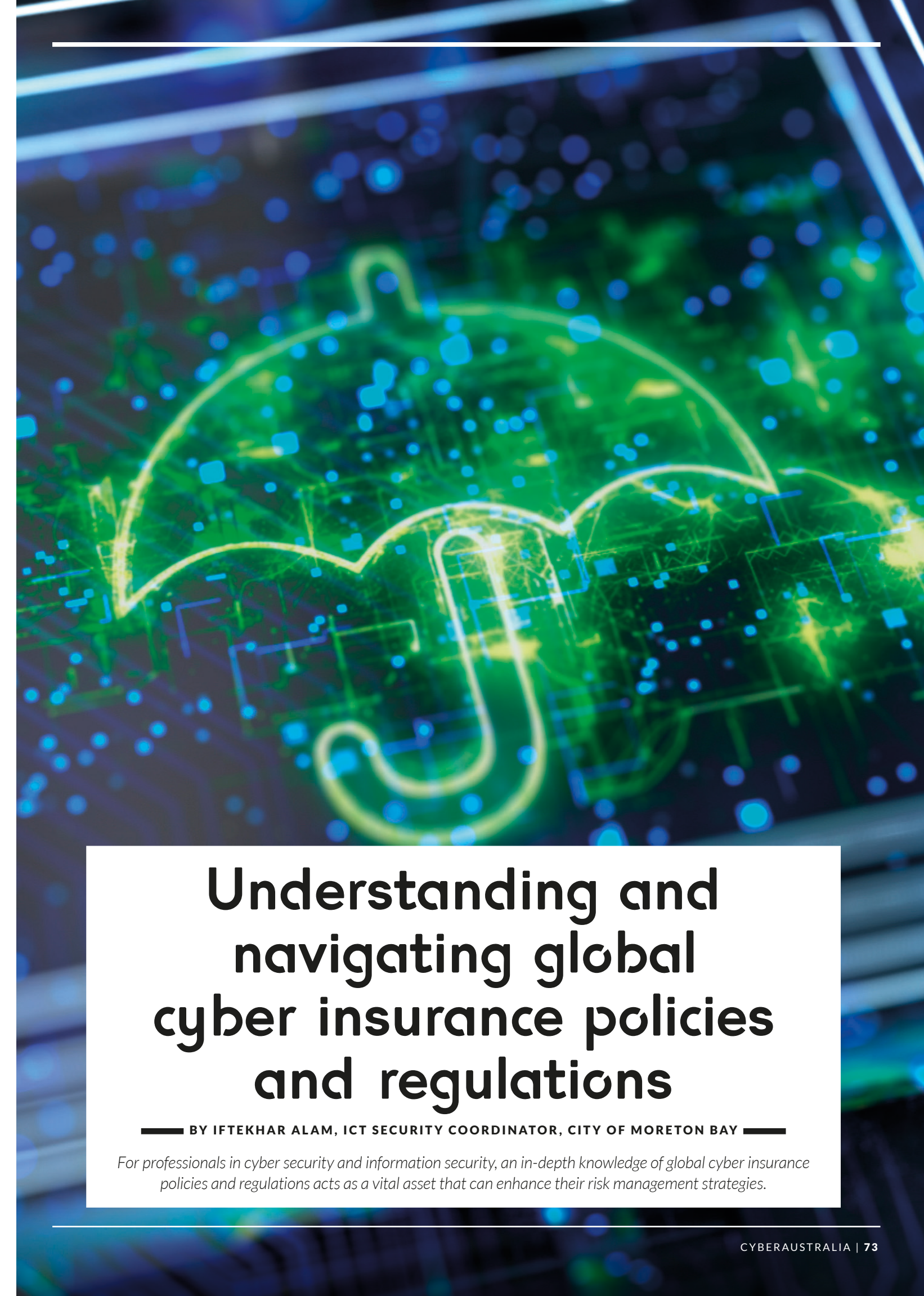
As well as the usual reminders about security best practice, experts advise protecting data using defensive mechanisms like keeping at least 13 months' worth of data backups in static cloud storage that provides auditable access control and cannot be compromised from the network; and keeping at least 12 months of detailed activity logs, also in uncompromisable storage, to assist with forensic analysis should anything happen.

Such protections could be the difference between recovering your operational environment, and paying cybercriminals untold ransoms to get your company back online because you couldn't do so yourself.

The surge of ransomware-as-a-service tools account for one in six ransomware attacks, with Barracuda Vice President of Global Security Operations Adam Khan noting that attackers often use 'tried and tested approaches', such as scanning, lateral movement, and malware download that 'can trigger security alerts that provide security teams with several opportunities to detect, contain, and mitigate ransomware incidents'.

Even then, many CISOs may end up watching in disbelief as ransomware gangs savage their networks – as at the company Cythera assisted where, Longley said, 'someone explicitly went out of their way as an IT admin to allow the connection to RDP'.

He added, 'For a malicious actor or penetration tester, this is the equivalent of rolling out a welcome mat and putting it in front of your network, and then getting confused why people keep rocking up.' •



Understanding and navigating global cyber insurance policies and regulations

— BY IFTEKHAR ALAM, ICT SECURITY COORDINATOR, CITY OF MORETON BAY —

For professionals in cyber security and information security, an in-depth knowledge of global cyber insurance policies and regulations acts as a vital asset that can enhance their risk management strategies.



Iftekhar Alam

As cyberthreats grow more complex, integrating cyber insurance into an enterprise's risk management plan is crucial. It not only ensures comprehensive preparation, but it also offers cyber security experts peace of mind in the event of security incidents with financial, reputational or legal consequences.

Recognising that cyber risk poses an enterprise-wide threat, affecting every business unit within an organisation, is critical. Transferring this risk to a third party, such as a cyber insurance provider, is a common strategy for organisations attempting to mitigate some of the burdens associated with enterprise risk. The New York State Department of Finance recommends several steps for integrating cyber insurance into the enterprise risk-management framework:

- › develop a formal cyber insurance risk strategy
- › address silent cyber insurance risk
- › evaluate systemic risk
- › accurately measure insured risk
- › educate insureds and insurance producers
- › obtain expertise in cyber security
- › require notification to law enforcement.

Cyber security and information security professionals should follow four steps when navigating

cyber insurance for an organisation: assess, evaluate, manage and measure. When assessing a cyber insurance plan, gathering information on the data and personally identifiable information held by the organisation, and any data collected and retained from customers for business purposes, is crucial. Moreover, consideration must be given to local and international regulations on data privacy, such as the General Data Protection Regulation, Health Insurance Portability and Accountability Act, Payment Card Industry Data Security Standard, the Australian Privacy Act, etc. Evaluating the consequences of a cyber attack is essential when determining the scope of cyber insurance coverage; for instance, ensuring that any third party or vendor accessing the company's data has sufficient or adequate cyber liability insurance.

After deciding to purchase cyber insurance, the organisation should consider the aspects to be covered by the insurance, which may include:

- › recovery costs after an incident
- › legal advice expenses
- › forensic investigation costs
- › costs stemming from legal advice due to a cyber incident or data breach
- › penalties imposed by regulators.

Managing cyber risk navigation requires understanding the five key sections of an insurance policy, followed by every cyber insurer – declaration



clauses, the insurance agreement between the company and the insurer, conditions of the contractual obligation, exclusion clauses, and varied declarations and provisions. One should not become complacent with their current cyber insurance contract, as cyber attacks are dynamic and relevant risks constantly evolve. Thus, reviewing the existing cyber insurance policy, agreement and offerings annually, and seeking the best deal and coverage, is essential to stay ahead and avoid unnecessary costs and consequences.

According to Dimitra Markopoulou, the definition of cyber insurance varies across the industry, with no universally accepted standard. Generally, cyber insurance refers to policies that cover first-party and third-party losses stemming from computer-based attacks or failures in a company's information technology systems. The European Insurance and Occupational Pensions Authority defines cyber insurance as coverage for losses arising from malicious and non-malicious incidents related to handling, storing and transmitting electronic data, including through the internet and computer networks. Similarly, the European Union Agency for Cybersecurity views cyber insurance as a product designed to protect businesses and individuals from internet-based risks and broader risks associated with information technology infrastructure and

activities. In the United States, the Department of Homeland Security describes cyber insurance as a tool to mitigate losses from various cyber incidents, including data breaches, business interruptions, and network damage. Given these differences in policy and requirements, professionals should obtain a proper understanding and interpretation of the policy based on the region and country they serve.

In conclusion, a sophisticated understanding of global cyber insurance policies and regulations is indispensable for any information security professionals aiming to strengthen their risk management strategies. As cyberthreats become increasingly complex, incorporating cyber insurance into an organisation's enterprise risk-management framework is essential. It facilitates the transfer of risk and ensures compliance with evolving regulatory landscapes. By proactively developing a comprehensive cyber insurance strategy, regularly reviewing policies, and addressing potential coverage gaps, professionals can significantly enhance their organisation's resilience against cyber incidents, safeguarding critical assets and ensuring operational continuity. •

Iftexhar Alam, a distinguished expert in information security and cyber security, has dedicated more than 15 years to continuous professional development, learning, mentoring, and advancement. His vast experience spans across sectors such as finance, insurance, banking, health care, government and telecommunications. As the ICT Security Coordinator for the City of Moreton Bay, he oversees the information security program and leads the cyber security team. He holds a Bachelor of Information Technology from the University of Southern Queensland, and a Graduate Certificate in Business Administration from Charles Sturt University (CSU). Moreover, he holds prestigious certifications: Certified Information Systems Security Professional and Certified Cloud Security Professional. He is also currently pursuing the Master of Business Administration at CSU to further enhance his managerial and leadership capabilities.

References

- CHUBB. (n.d.). Cyber insurance. <https://www.chubb.com>
- Lanois, P. (n.d.). Navigating Cyber Insurance. <https://www.isc2.org/Professional-Development/Skill-Builders/Cybersecurity-Leadership>; ISC2
- The Department of Financial Services. (4 February 2021). Insurance circular letter no. 2 (2021). <https://www.dfs.ny.gov/>. https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02
- Markopoulou, D. (2021). 'Cyber-insurance in EU policy-making: Regulatory options, the market's challenges and the US example'. Computer Law & Security Review, 43, p.105627. doi: <https://doi.org/10.1016/j.clsr.2021.105627>

The *Digital ID Act 2024* is good news for Australians!

THE DIGITAL ID Act 2024, coupled with the government initiatives to create a digital ID ecosystem, is a historic step for organisations and consumers.

The Act introduces safeguards for digital identity and verification (ID&V), building upon the Trusted Digital Identity Framework (TDIF). For consumers, this strengthens privacy protections. The TDIF makes the system more trustworthy and interoperable through the compliance and assurances it obtains from participating parties, and the promises the intermediary makes that it will do the right thing in security and privacy.

The digital ID ecosystem is a collaboration between government and commercial ID&V providers to enhance the customer experience across systems, and make it more attractive to use services that can deliver significant benefits.

THE BALANCING ACT: IDENTITY VERIFICATION

ID&V is required in many interactions between organisations and their customers; however, it

often creates privacy risks when organisations require customers to share and retain documents. Balancing regulatory requirements – like ‘Know Your Customer’ (KYC) for financial services – with privacy is a challenge.

ID&V: SECURE AND PRIVACY FOCUSED

Using secure ID&V solutions can provide significant benefits, such as:

- **Reduced risk:** eliminating the need to collect, transmit and store sensitive personal information, plus providers that are TDIF accredited are held to an high standard.
- **Improved performance:** ID&V solutions typically outperform manual processes – reducing errors, improving service and reducing fraud.
- **Enhanced privacy:** customers retain control over their sensitive personal information and choose what attributes to share for the specific purpose. For example, a licensee only needs to know the patron is over 18 to purchase

alcohol, not their date of birth or their identity.

- **Improved experience:** ID&V can streamline the process, leading to faster onboarding and better customer experiences.

HOW ID&V WORKS

Accredited ID&V providers use machine learning and artificial intelligence to:

- **Authenticate documents:** verify government-issued IDs (passports or driver’s licences).
- **Verify identity:** confirm the person presenting the ID is a live person and the owner.
- **Provide assurance:** organisations receive a code that confirms that the ID&V has been completed, eliminating the need to store IDs.
- **Customer experience:** ID&V involves incorporating these tools into the customer experience.

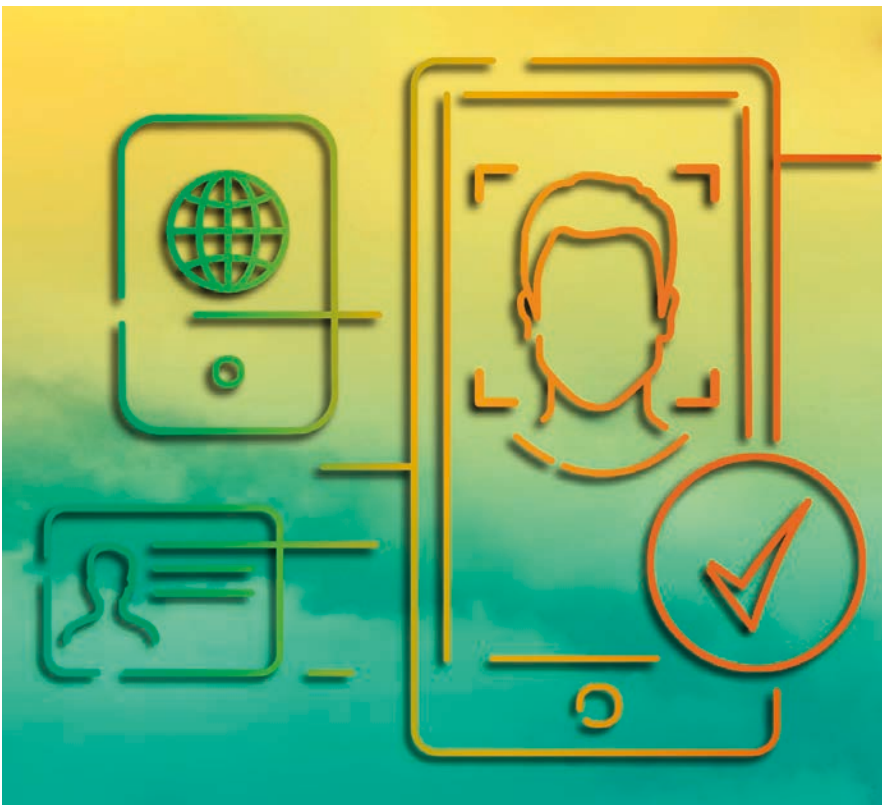
LEVERAGE THE BENEFITS

- **Understand regulations:** Clearly understand your specific regulatory requirements for your organisation. While KYC requires verification, regulation may not mandate retention.
- **Review processes:** Evaluate your current ID&V to reduce reliance on physical documents.
- **Explore ID&V solutions:** This includes research-accredited ID&V providers approved under the TDIF. Make sure you choose a solution to enhance privacy and a better customer experience.
- **Implement:** Implement an ID&V into a customer process and integrate re-verification throughout the customer journey.

DON'T WAIT, EMBRACE IT TODAY!

ID&V offers a privacy-enhancing approach to ID, enhancing security, customer experience and trust. •

Contact IIS Partners to explore and implement digital ID&V solutions tailored to your needs.





In order to comply and make use of the new **Digital ID Act** and regulations,

Choose the firm that has **Contributed** to them for **20 years.**

IIS Partners

We can help you implement Digital ID and navigate the intersection of the Privacy Act, AI, SOCI, APRA and ASIC regulations to build customer trust.

contact@iispartners.com, +61 2 8303 2438

For decades we have said,
It's just good business.
iispartners.com

SECURITY
& PRIVACY

SHORT-TERM MAIL, LONG-TERM RISK

— BY JAMIESON O'REILLY, FOUNDER, DVULN —

The use of temporary mailbox services during software development may seem harmless, but it can lead to severe security breaches.



A recent case involving a global cloud security vendor demonstrates how the use of a public throwaway mailbox exposed thousands of customer secrets, cloud snapshots and other sensitive resources, putting their customers at significant risk.

WHAT ARE TEMPORARY MAILBOXES, AND WHY ARE THEY USED?

Temporary or 'throwaway' email services are commonly used by developers during the testing phase of an application to validate functionalities linked to email addresses, such as user registrations or password resets. Setting up multiple email addresses for testing purposes can be time-consuming and costly, particularly when using paid services like Microsoft or Google. To streamline this process, many developers turn to free, temporary email services like Mailinator, YOPmail or Maildrop to receive and verify test emails quickly.

These services are actively marketed towards quality assurance (QA) testers. For instance, Mailinator is widely promoted as a key resource for QA teams automating their email and SMS workflow testing, with thousands of testers relying on it daily; however, despite some legitimate use cases, improper use of these services can lead to catastrophic security breaches.

THE DANGERS OF PUBLIC INBOXES

An example of risky behaviour occurred when a QA tester was observed using a YOPmail account for a management-type user of an application under development. Many testers may not realise the potential danger of using a publicly accessible inbox for test users, whether in staging or production environments. This lack of awareness creates significant security vulnerabilities.

Developers, QA teams and even penetration testing firms have been observed using YOPmail accounts to authenticate their testing procedures. These accounts frequently remain in application databases as apps move from staging to pre-production, and eventually into production – where they are often forgotten, yet still remain active.

HOW TEMPORARY MAILBOXES LED TO A MAJOR SECURITY BREACH

A particularly concerning incident involved a global cloud security vendor that inadvertently exposed sensitive customer data due to the careless use of temporary email services. This vendor, a trusted platform for many organisations worldwide to secure their cloud environments, had been using temporary mailboxes

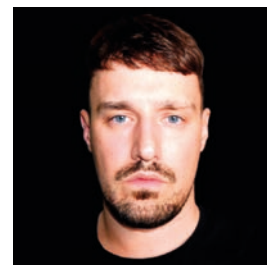
like Mailinator and YOPmail within their development team to test administrative account functionality. These mailboxes were meant to receive test emails for administration account activities during development, but were left active in the system after testing was completed.

This oversight resulted in the exposure of thousands of secrets, snapshots and other cloud resources, ironically, from customers who were using this platform to secure their data. By accessing temporary mailboxes such as `admintest@mailinator.com` and `qa_user_test@yopmail.com`, it was possible to identify a substantial amount of sensitive information, including credentials and critical assets.

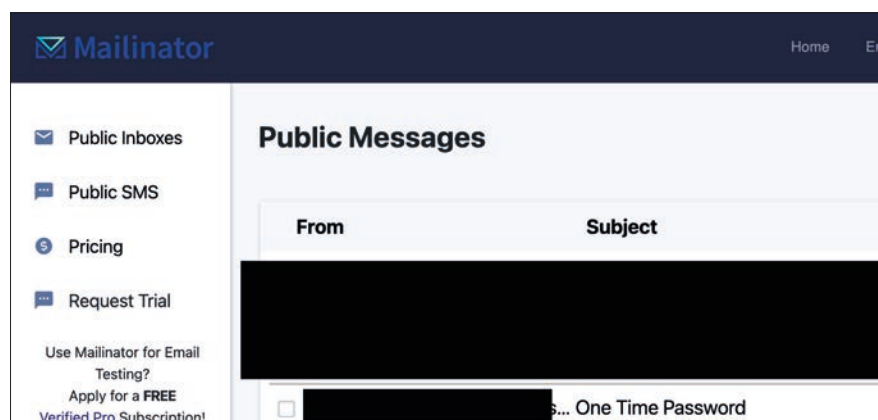
DEMONSTRATING 'WHAT IF?'

The results of this exposure were alarming. Here are some examples of public, temporary mailboxes discovered with sensitive user accounts tied to them:

- › **Law enforcement field arrest app:** This public inbox was set up by a third-party development agency for an American company specialising in law enforcement applications, such as arrest tracking and evidence examination. The exposure of this information represented a serious breach of privacy and security.
- › **Mobile device management access:** An IT staff member at a medium-sized business used this public inbox to configure company devices with IBM's MaaS360. By doing so, they inadvertently granted public access to the system, compromising all connected devices – all because someone failed to consider 'what if?'
- › **Global cloud security vendor:** In another instance, a temporary mailbox was used during development to test administrative account functionalities. By accessing this public mailbox, an attacker could find emails containing one-time



Jamieson O'Reilly



passcodes (OTPs) and administrative login credentials. With these details, they could easily gain administrator-level access to a security tool used by high-profile companies to protect their data.

This tool was used by numerous enterprises worldwide to safeguard their data, yet an unauthenticated user gained entry due to a forgotten temporary email account. Upon examining the existing users in the admin panel, multiple administrator accounts were found linked

to YOPmail and Mailinator addresses, suggesting that this risky practice was not isolated.

THE REAL-WORLD CONSEQUENCES

These examples highlight a frightening reality: how the improper use of temporary mailboxes in software development can lead to severe security breaches. Publicly accessible mailboxes are available to anyone who knows or guesses the address, meaning that sensitive information – like OTPs, password reset

Asset Management

ALL ASSETS GRAPH

1

AWS Config Delivery ...

1

AWS Configuration Re...

332

SSM Instance Patches

9

SSM Instance Informa...

95

SQS Queues

1778

Secrets Manager Secr...

12

APIGateway RestAPIs

12

AWS DNS Zones

8

RDS Snapshots

1

RDS Instance

49

KMS Keys

296

AWS Lambdas

9

Elastic IP Address

20

ElastiCache Clusters

5

EKS Clusters

116

ECS Task Definitions

8

ECS Clusters

173

ECR Repositories

30

EC2 Key Pairs

20

EBS Volumes

201

Network Interfaces

321

EBS Snapshots

27

AWS Internet Gateway...

28

AWS Vpcs

84

EC2 Subnets

72

EC2 Security Groups

20

Load Balancer V2s

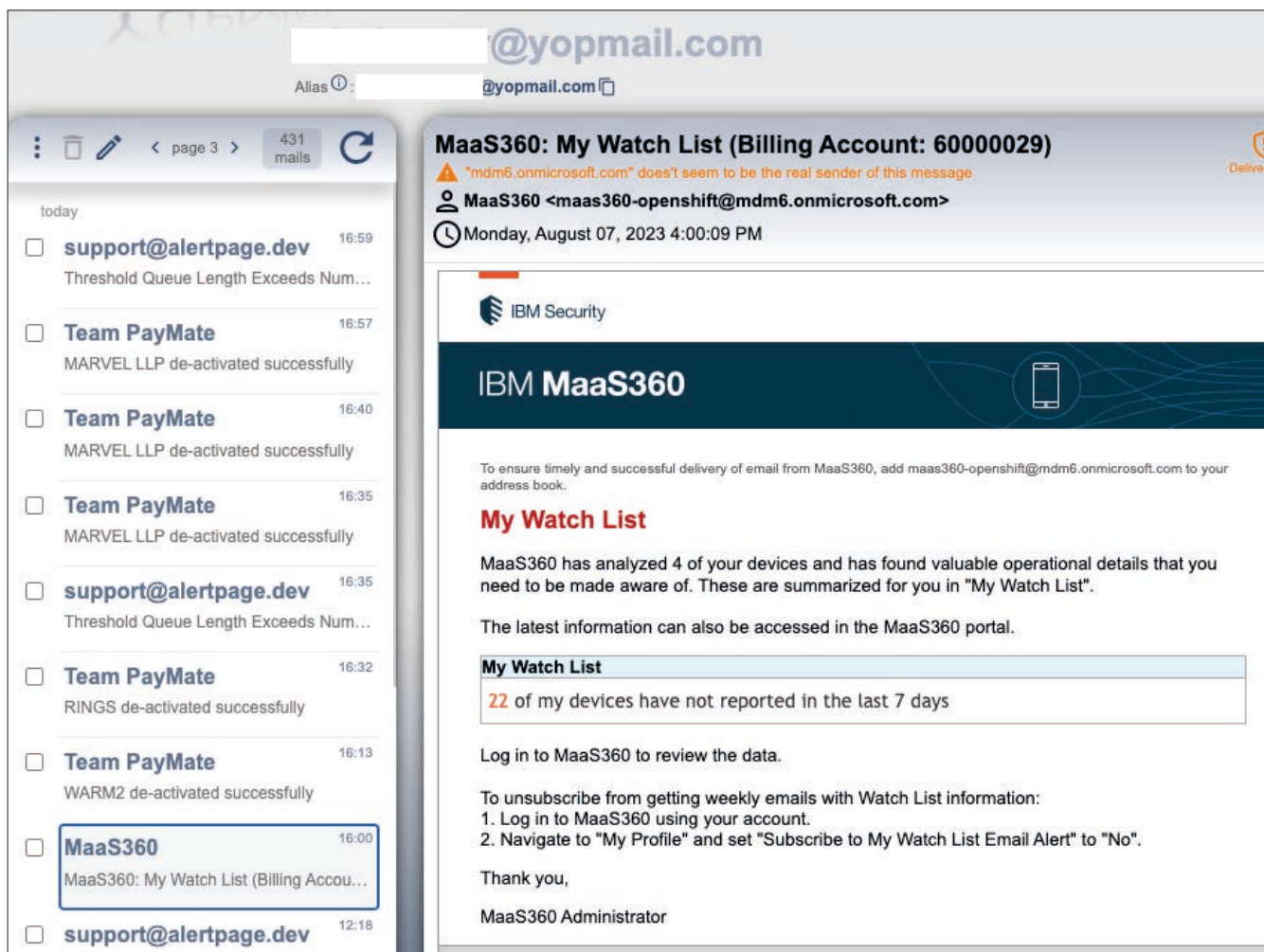
87

EC2 Images

test user

Help

test new user	Not applicable	r007@mailinator.com	Auditor	Edit	Delete
	Test	r@mailinator.com	Admin	Edit	Delete
Test Invite		267@mailinator.com	Admin	Edit	Delete
testemployeeadmin123	--	aeadmin123@mailinator.com	Admin	Edit	Delete
test		ae3000@mailinator.com	Contributor	Edit	Delete
Test	Cont	?8@mailinator.com	Admin	Edit	Delete
Test tenant Id		?727272@mailinator.com	Admin	Edit	Delete



links or confidential data – can easily fall into the wrong hands.

The most troubling part is how widespread this practice is. Developers often use these services for administration accounts, significantly increasing the security risk.

WHAT CAN BE DONE?

To mitigate these risks, all parties involved in software development and security need to take proactive steps:

For developers:

- › Use dedicated testing environments with controlled email services.
- › Avoid using public temporary email services, especially in staging or production environments. Implement filters to block emails from these services in applications.

For organisations:

- › Conduct regular security audits and educate teams about best practices. Make security a priority at every stage of development.
- › Monitor for the presence of temporary email accounts in systems and databases.

For everyone:

- › Stay informed about security trends and risks. Understanding potential vulnerabilities is the first step in protecting both individuals and organisations.

CONCLUSION

Temporary email services may offer convenience, but they pose significant risks. As demonstrated by the example of the global cloud security vendor, a minor oversight can lead to major security breaches. By asking ‘what if?’ and considering the potential consequences, costly mistakes can be prevented, and systems can remain secure. ●

With more than 12 years of experience in information security, Jamieson O'Reilly specialises in application security, cryptography, secure design and secure application development. As a leader in offensive security, he has conducted countless red team exercises and adversary simulations against some of the hardest targets in the world – from banks and casinos, to government agencies – to test their resilience against advanced persistent threats. His expertise helps organisations uncover critical vulnerabilities and build robust defences against highly skilled attackers.

Cutting through complexity: elevating security and simplifying compliance

As Australian organisations evolve their digital capabilities, they face an increasingly complex cyber security landscape. High-profile breaches and cyber attacks highlight escalating risks, while regulatory bodies continue to impose stricter standards. Whether complying with frameworks like ISO 27001, the United States National Institute of Standards and Technology, or Australia's Essential Eight, the challenge for organisations is twofold: achieving compliance while strengthening cyber security defences.

FOR ORGANISATIONS, THE cost of failure is high – ranging from reputational damage and operational disruptions, to regulatory fines. Yet, many Australian organisations lack a defined cyber security road map to continually improve their posture and stay ahead of evolving threats. While global and local cyber security frameworks offer a structured path, resource constraints and competing priorities often prevent organisations from realising their full potential. In industries where compliance is mandated, the process often becomes a checklist, leaving organisations vulnerable to threats.

COMPLIANCE ALONE DOES NOT GUARANTEE SECURITY

While meeting regulatory requirements is crucial, compliance alone does not ensure a strong security posture. Organisations should see their compliance journey as a stepping stone toward robust cyber security. By integrating security best practices, businesses can protect against threats while meeting regulatory obligations. This transforms compliance from a box-ticking exercise into a comprehensive strategy for building resilience.

BALANCING COMPLIANCE AND SECURITY

To achieve ongoing compliance and improve cyber security maturity, organisations need tools that go beyond manual methods. Simplifying compliance management must go hand in hand with security practices. Automated solutions are key to balancing these priorities, as ensuring compliance efforts are occurring also boosts security.

HOW CYBERHEED CAN HELP

Every business, regardless of its size, needs access to affordable tools to

measure and enhance its security posture. CyberHeed provides a comprehensive, automated solution to simplify and enhance security for organisations of all sizes. It eliminates manual complexities, enabling businesses to manage compliance across frameworks such as ISO 27001, the United States National Institute of Standards and Technology, and the Essential Eight. Its tailored features empower organisations to proactively identify gaps, track real-time progress, and ensure continuous improvement in their security posture, meeting regulatory requirements while building long-term resilience. At its core, CyberHeed simplifies and automates compliance, helping organisations boost their security and defend against evolving cyberthreats.

AUTOMATED COMPLIANCE TRACKING

Organisations often struggle to track compliance with multiple frameworks. Manual processes are time-consuming and error-prone, leading to lapses. CyberHeed automates compliance tracking across frameworks, continuously monitoring compliance and reducing the burden on IT teams.

TAILORED RISK ASSESSMENTS

CyberHeed provides tailored assessments to identify cyber security

gaps and generate action plans for improvement. Designed to benefit both small businesses and larger enterprises, CyberHeed's platform adjusts to your organisation's target maturity level, offering a path to improved security.

BY 2025, 60 PER CENT OF ORGANISATIONS WILL USE CYBER SECURITY RISK AS A PRIMARY DETERMINANT IN THIRD-PARTY TRANSACTIONS, YET, ONLY 23 PER CENT ARE FULLY PREPARED¹

SCALABLE SOLUTIONS FOR ENTERPRISES OF ALL SIZES

Australian organisations range from small and medium-sized enterprises (SMEs), to large enterprises, each with unique challenges. CyberHeed is built to scale, offering SMEs affordable, enterprise-grade cyber security, and helping larger enterprises manage complex, multi-framework compliance requirements, streamlining operations across different teams and regions. •

¹ According to Gartner





Unlocking **Smarter** Compliance, Risk Management



Save time and resources with CyberHeed's automated platform, designed to simplify compliance and elevate security. Reduce manual effort, stay compliant, and enhance your risk management with ease.

Try CyberHeed today and experience smart, seamless compliance

www.cyberheed.com/signup

From hoodies to nation-states: rethinking the cybercrime paradigm

— BY SABEEN MALIK, VICE PRESIDENT OF GLOBAL GOVERNMENT AFFAIRS AND PUBLIC POLICY, RAPID7 —

When discussing ransomware, many still envision a lone hacker in a dimly lit basement or garage, exploiting outdated security gaps through simplistic methods like phishing emails or leaked credentials. This myopic view overlooks a far more sophisticated and insidious reality: the rise of 'cybercrime as a service'.



Much like software as a service, cybercrime has evolved into a complex, lucrative ecosystem, complete with big players, intermediaries, and a well-defined supply chain. A deeper understanding of this paradigm shift is crucial if we are to develop effective strategies to combat what continues to be a growing threat.

At the heart of this ecosystem, and a linchpin for cybercriminal operations, are initial access brokers – entities that play a pivotal role in facilitating cybercrime. These brokers operate as intermediaries, sourcing vulnerabilities and packaging elements for sale to the highest bidder. This middle layer significantly lowers the barrier to entry for bad actors, making it much easier and cheaper for malicious actors to launch sophisticated ransomware attacks. The actual perpetrators of these attacks often leverage the resources and expertise provided by these brokers, highlighting a disturbing trend: the commodification of cybercrime.

This commodification mirrors the structure of a legitimate business, with cybercrime syndicates functioning as international enterprises. Yet, unlike other transnational criminal organisations, our approach to combating these groups remains fragmented and outdated. Governments often treat ransomware groups as isolated entities, rather than necessarily recognising them as components of a larger, well-coordinated criminal network, which can hinder our ability to develop comprehensive and effective countermeasures.

Initial access brokers, in particular, exemplify the sophistication and specialisation within the cybercrime ecosystem. They do not merely identify vulnerable targets; they provide detailed intelligence on the best times to strike and the most effective methods of entry. This vital information is then sold to the bad actor who uses it to carry out the actual attack. The brokers profit regardless of the attack's success, underscoring their role as facilitators rather than direct participants in the criminal activity.

The sectors most often targeted by these groups are those often ill-equipped to defend against such sophisticated threats, which can include health care, financial services, and critical infrastructure. These high-value targets are attractive not only for their potential payouts, but also because their disruption can cause significant societal harm, amplifying the impact of the attacks.

To address this threat, we must shift our mindset and strategies. Viewing cybercrime as a service industry reveals the importance of targeting not just the perpetrators, but also the infrastructure and intermediaries that enable these attacks. This requires international cooperation and the

development of new legal frameworks to tackle the unique challenges posed by digital services. For instance, mutual legal assistance treaties (MLATs) are great for cooperation among those countries that want to use this process effectively. A potential issue, however, is that many of these criminal networks exist in countries where MLAT requests experience long delays in responding to data requests. Alongside this, the process can also stall at many steps, in part because it was designed before the cloud became the primary storage platform for many decentralised internet services.



Sabeen Malik

Viewing cybercrime as a service industry reveals the importance of targeting not just the perpetrators, but also the infrastructure and intermediaries that enable these attacks

Australia's recent legislative reforms on ransomware reporting are a step in the right direction, but they remain limited in scope. A more holistic approach is needed – one that includes robust privacy laws and greater collaboration between the public and private sectors. By understanding the broader ecosystem of cybercrime, we can develop more effective strategies to disrupt these activities at multiple levels.

For example, one practical step is to conduct a national audit of data and digital services to identify those that are of high value and particularly vulnerable to exploitation. This exercise would help prioritise resources and develop targeted protections for the most critical assets. Additionally, investing in digital identity programs and other cyber security initiatives can provide an extra layer of defence against these sophisticated threats.

A RANSOMWARE FRAMEWORK: THE THREE CS

A collaborative relationship between the private and public sectors is crucial in fortifying our defences against critical threats like ransomware attacks. To combat these sophisticated threats, a nuanced approach that leverages the strengths of these private and public sectors is required through, what I term, the 'Three Cs' framework: context, capabilities and collective action.

Context

Context means understanding not just the data, but also the narrative it tells us about attacker motivations, methods and targets. It involves distinguishing what pieces of information are relevant to crafting a strategic response, and what ones may serve as mere distractions. Full transparency without context is like providing a map without landmarks – it offers data, but little guidance on navigating threats.

For instance, while the private sector can supply a wealth of real-time data, government entities can often interpret these datasets within the broader geopolitical context. This interpretation transforms raw data into prioritised, actionable intelligence, allowing for targeted responses rather than generic, one-size-fits-all solutions.

Capabilities

Understanding the capabilities of an organisation, whether in the private or public sector, is fundamental to effective cyber security. It's not just about having tools; it's about applying them wisely. For example, while the private sector may excel in rapidly aggregating data, government agencies often possess a deeper understanding of the geopolitical landscape that can influence cyberthreat origins and motivations. By assessing capabilities, we ensure that all players are utilising their strengths and using them in the most impactful way.

Collective action

Once the right context has been established and the capabilities have been assessed, organisations need to collectively synchronise efforts between various stakeholders to share insights, strategies, and data points that enrich the overall understanding of the cyber landscape. Here, the need for a symbiotic relationship between the private and public sectors becomes evident.

Private sector entities often possess advanced technological capabilities, such as sophisticated intrusion-detection systems, comprehensive threat-intelligence platforms and powerful data analytics tools. They gather vast amounts of data through their daily operations, which, when shared appropriately, can provide invaluable insights into emerging cyberthreats; however, this data might not be fully utilised without the broader context provided by public sector intelligence. Public agencies bring a wider geopolitical and strategic understanding that can interpret private sector data within the context of national and international security threats.

This symbiosis is exemplified by collaborative initiatives where government bodies contextualise the data provided by private companies, enabling a targeted and strategic response. For example, when a private sector firm identifies a new form of malware, government agencies can quickly communicate this information, advising other entities within the network on how to bolster their defences, thus preventing a broader security breach.

The public sector can also enable a unified response to cyberthreats by setting standards and regulations that guide the collective actions of diverse organisations. This regulatory framework ensures that all parties adhere to best practices and share critical information responsibly, which is especially important in sectors that are essential to national infrastructure.

The relationship between these sectors isn't just beneficial, but is also essential against more aggressive and organised threat actors. It enables a dynamic flow of information and resources that enhances the overall security posture of both private companies and public institutions.

By fostering an environment where information-sharing is guided by context and strategic insights, we ensure that our responses to cyberthreats are both rapid and effective. Underscoring the urgency of this approach is feedback from academics and other experts, who recognise that the traditional methods of combating cybercrime are insufficient in the face of its rapid evolution.

Rethinking our approach to cybercrime requires a fundamental shift in perspective. We must move beyond the outdated notion of lone hackers and instead recognise the organised, business-like nature of modern cybercriminal enterprises. By targeting the infrastructure and intermediaries that support these activities, and leveraging the 'Three Cs' framework, we can develop more effective and comprehensive strategies to protect our digital assets and ensure a safer cyber environment for all. •

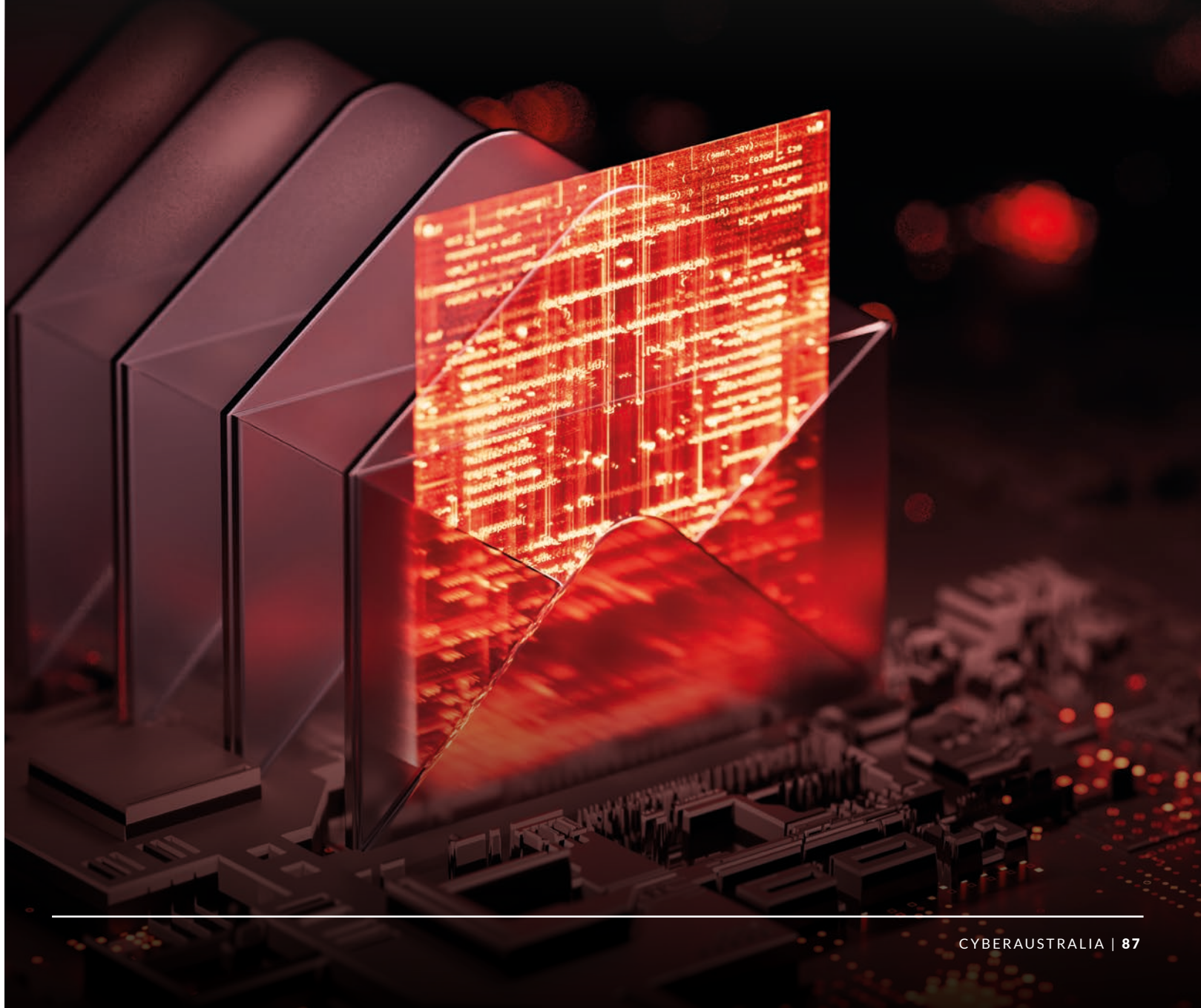
~~~~~  
Sabeen Malik is a global thought leader on digital economy and tech policy issues, law and economic development, innovation economies, and next-generation emerging technology and economic trends. As the Vice President of Global Government Affairs and Public Policy at Rapid7, Malik is responsible for leading all global, federal and state government relations activities, and developing and executing Rapid7's strategic global corporate, regulatory, and government relations strategies. She is also responsible for ensuring strong relationships with regulators and government leaders.

---

# Silver-tongued swindlers usher in a new epoch of cybercrime

— BY DARREN PAULI, CYBER SECURITY EXPERT, TELSTRA —

*Imagine you need to hack into an organisation. You could try to break through its security systems and hope you don't set off any alarms, or you could convince an employee to let you in. Which sounds easier?*







Darren Pauli

**P**hishing, a form of social engineering, is a tried-and-tested method for convincing people to conduct some action like running malicious files or offering up sensitive information like logins, personal information, and corporate data. It often goes hand in hand with technical hacking, and can give a leg up to cybercriminals

looking to bypass cyber security defences.

Phishing often looks familiar: scams about missing deliveries, overdue bills, and security notifications are endlessly sent to our phones, email addresses, and social media accounts. But a new breed of criminal is taking advantage of what we think scams look like, and is enjoying success.

Scattered Spider is a group of young hackers scattered across Western countries, possibly including Australia. They are brash, bold and technically competent, showcasing the kind of social engineering mastery usually reserved for offensive security professionals and state intelligence agencies. They are silver-tongued swindlers who are as convivial and convincing as they are dangerous and destructive.

They have targeted large organisations across the West in coordinated, multi-stage and persistent campaigns that include reconnaissance, information-gathering, and technical hacking. They target leaders. They target staff. And they have the most seasoned security professionals on edge.

There is little to determine these criminals from legitimate callers. Scattered Spider has posed as technical auditors in a series of calls to support staff in a bid to glean internal information to shore up their perceived legitimacy in subsequent attacks. It uses members across the world to attack local companies using local accents. If granted access, the group could gain a foothold in corporate networks from where further attacks can be launched.

Organisations across Australia must take notice. Many place a heavy emphasis on customer service,

offering alternative methods of authentication for people who cannot remember standard information like account numbers and passwords. In essence, these staff are 'here to help'.

It is this service that Scattered Spider and groups like it exploit to devastating effect.

We have entered a new era of cybercrime. This epoch is characterised by easy access to vast pools of personal information on Australians sold on cybercrime forums, along with groups that bring a new creativity and daring to their attacks that blow out of the water the old notions of what scams look like.

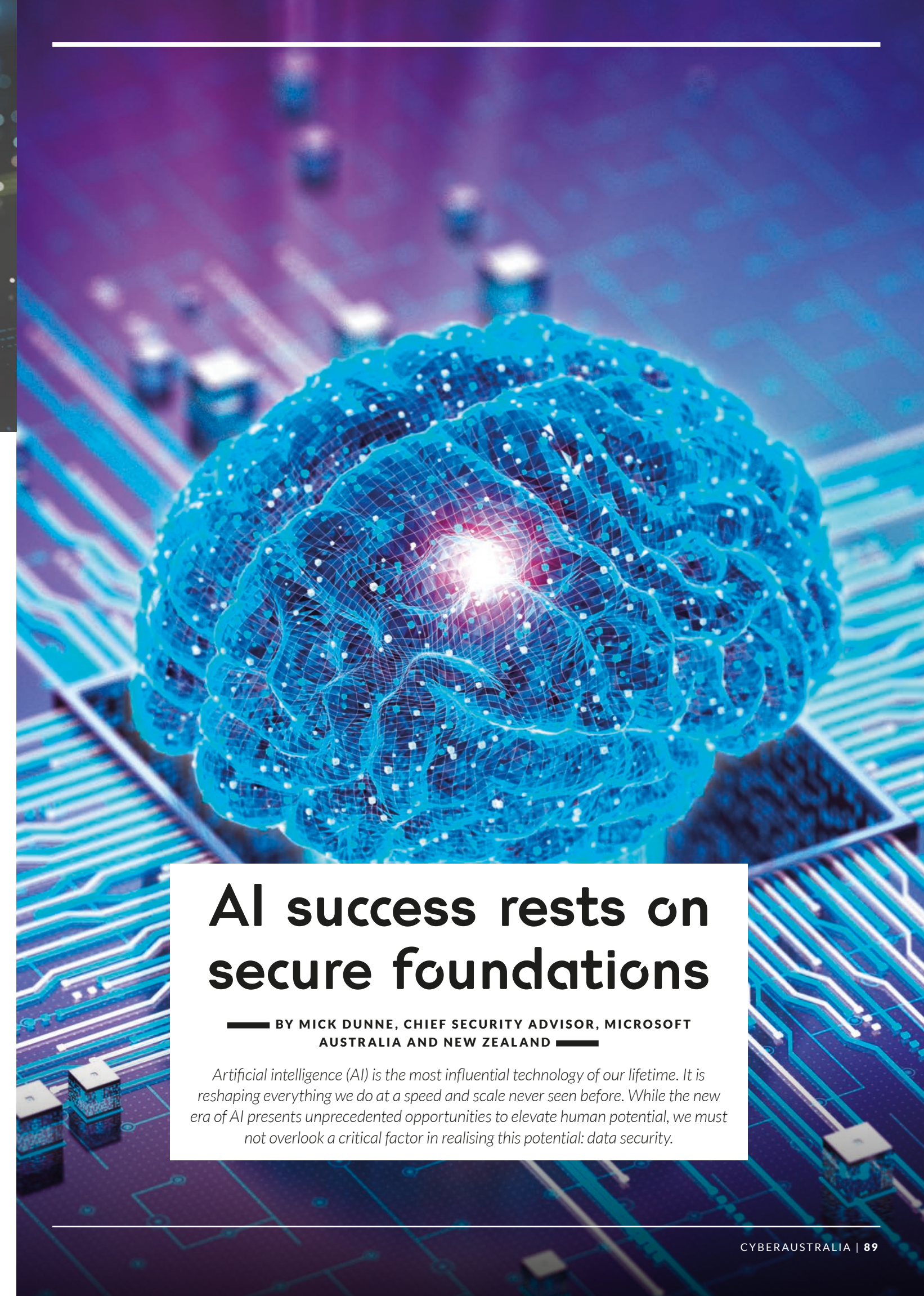
Organisations must review how they identify legitimate customers or suppliers. Could a convincing, friendly voice convince staff to bypass standard processes in order to help? What access can staff grant to such a person? What sensitive information can such staff access?

Scam awareness is not enough, because Scattered Spider agents are often indistinguishable from legitimate callers. Rather, organisations should consider more secure forms of authentication like hardware second-factor authentication keys or through an enrolled device. They should limit the ability for front-of-house staff to change passwords for critical accounts. They should ensure that formal authentication methods are cyber secure, and that staff have no technical ability to make exceptions to them, even if they wanted to. Even if the CEO calls.

For now, most scammers are indeed using the types of ruses many of us have come to expect. But a digital Rubicon has been passed. Artificial intelligence only promises to help make scams even more convincing for those without the skills of Scattered Spider. It is therefore absolutely imperative that organisations take note and take action today. ●

Darren Pauli is a cyber security expert with more than a decade's experience writing on security. He came to Telstra's cyber security unit after serving as an InfoSec correspondent for various tech-focused publications.



A glowing blue digital brain, composed of a mesh of points and lines, is centered on a background of a circuit board. The brain has a bright white light source in its center, creating a lens flare effect. The circuit board features various components like capacitors and resistors, with glowing blue lines representing electrical traces.

# AI success rests on secure foundations

— BY MICK DUNNE, CHIEF SECURITY ADVISOR, MICROSOFT AUSTRALIA AND NEW ZEALAND —

*Artificial intelligence (AI) is the most influential technology of our lifetime. It is reshaping everything we do at a speed and scale never seen before. While the new era of AI presents unprecedented opportunities to elevate human potential, we must not overlook a critical factor in realising this potential: data security.*





Mick Dunne

**T**he foundations of data security might seem mundane or even outdated in the face of advanced artificial intelligence (AI) capabilities; however, having confidence and trust in your data and systems is critical to be able to embrace AI securely and safely. Protecting data (which is critical to building a powerful AI capability) starts with the basics.

### THE IMPORTANCE OF THE BASICS

Every organisation, regardless of size or sector, needs to master the fundamentals of security. This means being disciplined about asset inventory, patch management and access control – they may not grab headlines,

but they are indispensable to preventing many common cyberthreats.

According to Microsoft's latest Digital Defense Report, basic security hygiene practices – such as enabling multi-factor authentication, applying zero trust principles, using extended detection and response software, keeping systems up to date, and protecting data – still protect against 99 per cent of attacks.

It boils down to the common saying: 'Hackers don't break in, they are let in.' These basics aren't just a check box exercise; they are the bedrock upon which all advanced security measures – and, by extension, AI initiatives – are built.

### PROTECTING THE FUEL FOR AI

Data is the fuel that powers AI, and its security and integrity are paramount.



AI systems depend on accurate, complete and relevant data to function correctly. If the data is tampered with (intentionally or not), AI's outputs may become unreliable, leading to potentially suboptimal decisions.

Data classification also plays a crucial role here; however, it's often done poorly or not at all. Properly classifying data ensures that sensitive information is appropriately protected, and that AI systems don't inadvertently expose or misuse it. This is particularly important given the increasing regulatory scrutiny around data privacy and protection.

Likewise, many customers we work with have shared that bringing AI productivity tools into the business has actually helped accelerate data privacy and access efforts. Because an AI tool references the sources, it can very quickly surface where access gaps

are. For example, a confidential business document might be accessible to external users that shouldn't be. So many customers are seeing the benefits of using AI to accelerate their efforts in hardening their data access guardrails.

**AI systems depend on accurate, complete and relevant data to function correctly. If the data is tampered with (intentionally or not), AI's outputs may become unreliable, leading to potentially suboptimal decisions**

**REALIGNING AROUND OUR SECURITY PRIORITY**

At Microsoft, we're deeply focused on security because the stakes have never been higher.

We launched our Secure Future Initiative (SFI) in November 2023 to ensure security is the top priority in everything we do. With the increasing scale and sophistication of cyber attacks, SFI is about embedding security into every aspect of our operations and products to protect both Microsoft and our customers.

In May 2024, we evolved SFI around three core principles: secure by design, secure by default and secure operations. These principles shape our efforts across six key areas – from protecting identities and securing networks, to detecting and responding to threats. By focusing on these areas, we're helping our customers reduce vulnerabilities and build resilient systems that can stand up to today's cyberthreats.

SFI is also about creating a security-first culture at Microsoft. We're committed to continuous improvement and making sure that security is at the heart of every decision. By aligning with industry standards, SFI helps our customers confidently embrace AI and other technologies, knowing they're built on a secure foundation.

**SECURITY AND AI: A SYMBIOTIC RELATIONSHIP**

AI has the potential to transform organisations, but only if it is built on a secure foundation. The above security basics are crucial to unlocking AI's potential because they ensure that the data that AI relies on is secure and trustworthy, and that the systems that AI operates within are resilient.

Neglecting these basics puts your AI initiatives and organisation at risk. In a world where cyberthreats are constantly evolving, doing the basics well is not just advisable – it's essential. ●





# Australia's digital battleground: facing the shadows of cyber warfare

**AUSTRALIA, OFTEN CELEBRATED** for its vibrant economy and unique way of life, is also home to a rapidly evolving digital ecosystem. As the nation embraces technological innovation, it grapples with a significant downside: an alarming rise in cyber security threats. Being one of the wealthiest and most digitally connected countries in the world, Australia is a prime target for a global cybercrime industry worth over \$15 trillion. The country is experiencing a year-on-year increase in cyber attacks, with threats becoming increasingly sophisticated and automated.

Compounding these challenges is a significant labour shortage in various sectors, particularly cyber security and IT. This shortage has left Australian organisations struggling to find the skilled professionals necessary to defend against these evolving threats. To combat this multifaceted issue, businesses must not only address resourcing and skills shortages, but also cultivate a strong culture of cyber security awareness across all levels of their organisations.

**THE RISING VOLUME OF CYBER ATTACKS**

In recent years, Australia has faced a staggering increase in

cybercrime incidents. According to the Australian Signals Directorate's Australian Cyber Security Centre, more than 94,000 reported cybercrime incidents occurred in financial year 2022 alone – a remarkable rise from previous years. These incidents reflect an escalating threat to businesses, government agencies and individuals alike.

Cybercriminals are now targeting a wide range of sectors – from health care to finance – and are seeking to exploit vulnerabilities in various systems. Several factors contribute to this surge, including the widespread adoption of digital platforms and the increased reliance on remote work. As organisations accelerate their digital transformations, the attack surface expands, providing more opportunities for malicious actors.

**GROWING SOPHISTICATION OF CYBERTHREATS**

The sophistication of cyberthreats has also escalated dramatically. Cybercriminals are utilising advanced tactics, including ransomware, phishing and supply chain attacks – making them increasingly difficult to detect and mitigate. Ransomware, in particular, has become a preferred method of cyber

extortion, with attackers encrypting sensitive data and demanding substantial payments for its restoration.

Furthermore, the use of artificial intelligence and machine learning by cyber adversaries complicates the landscape even further. These technologies enable attackers to develop more sophisticated methods for infiltration and evasion, rendering traditional security measures less effective. As threats grow increasingly complex, organisations must evolve their cyber security strategies to stay ahead of the curve.

**THE LABOUR SHORTAGE DILEMMA**

Compounding the challenges of rising attacks and growing sophistication is a significant labour shortage in the cyber security sector. With demand for skilled professionals far outstripping supply, organisations find it increasingly difficult to recruit the talent necessary to defend against evolving threats. Recent reports indicate that Australia faces a shortfall of tens of thousands of cyber security workers, which significantly hinders both businesses and government entities in implementing robust security measures.



This talent shortage is particularly burdensome for small and medium-sized enterprises, which often lack the resources to attract and retain qualified personnel. As a result, many organisations find themselves vulnerable to cyberthreats, and unable to keep pace with the evolving digital landscape.

## RECOMMENDATIONS FOR ADDRESSING CYBER SECURITY CHALLENGES

To navigate these challenges effectively, Australia must adopt a multifaceted approach that encompasses outsourcing cyber security functions, aligning with best practices, and fostering a culture of cyber security awareness. Recommendations include:

### 1. Outsourcing cyber security functions

One viable solution to address both the labour shortage and the increasing volume of attacks is to outsource cyber security functions to specialised firms. Managed security service providers, offer a range of services, including threat detection, incident response and vulnerability assessments. By leveraging the expertise of these providers, organisations can significantly enhance their security posture without the need for extensive in-house teams.

Outsourcing allows businesses to access a broader talent pool and stay abreast of the latest security technologies and trends. Moreover, it enables organisations to focus on their core operations while entrusting cyber security responsibilities to professionals dedicated to the field.

### 2. Aligning with best practices: Essential Eight and NIST Framework

Organisations should also adopt the Essential Eight framework, which outlines practical steps for strengthening defences, significantly reducing the risk of cyber attacks. Complementing the Essential Eight is the NIST Cybersecurity Framework, which offers a structured methodology for identifying and mitigating risks. Together, these frameworks can enhance an organisation's cyber security posture.

Regular security assessments and penetration testing are vital for identifying vulnerabilities before they can be exploited. Additionally, cyber security governance, risk and compliance companies can assist organisations in implementing these best practices, ensuring a focused approach to safeguarding critical assets and sensitive data.

### 3. Fostering a culture of cyber security awareness

Human error continues to be one of the leading causes of cyber incidents. Therefore, organisations must cultivate a culture of cyber security awareness among employees. Training programs that educate staff about phishing, social engineering and safe online practices are essential in mitigating the risk of successful attacks.

Encouraging a proactive approach to reporting suspicious activities and potential threats is equally important. Empowering employees to take ownership of cyber security can significantly enhance an organisation's overall security posture.

### 4. Investing in talent development

To tackle the labour shortage, Australia must invest in education and training programs that nurture a new generation of cyber security professionals. Collaborations between educational institutions, government, and industry can

create pathways for students and professionals to gain the necessary skills and certifications.

Promoting cyber security as a viable career path through internships and apprenticeships can also help attract talent to the field. Furthermore, upskilling existing employees through continuous education can bridge the skills gap, ensuring that organisations possess the expertise required to combat cyberthreats.

## CONCLUSION

As Australia navigates the complexities of its digital landscape, it faces considerable challenges in cyber security due to the increasing volume and sophistication of attacks, coupled with a significant labour shortage in the field.

By adopting a proactive strategy that includes outsourcing cyber security functions, aligning with best practices, fostering a culture of awareness and investing in talent development, Australia can strengthen its defences against cyberthreats. In doing so, the nation can continue to thrive as a land of promise, unburdened by the shadows of cybercrime.

The path forward lies in collaboration, innovation and a steadfast commitment to safeguarding Australia's digital future. •

*Discover more about AUCyber, including its award-winning cyber security solutions and managed services, at [www.aucyber.com.au](http://www.aucyber.com.au)*





# AUSCERT now offers tabletop exercises as part of its governance, risk and compliance services!



**IN TODAY'S DIGITAL** age, the ability to swiftly and effectively respond to security incidents is important for any organisation. AUSCERT is proud to offer tabletop exercises (TTXs) as a component of its governance, risk and compliance services. These simulations are designed to test your organisation's preparedness in managing and responding to a variety of incidents. Through these exercises, you can identify critical gaps in your incident response plans, ensuring that your team is fully prepared to handle real-world crises.

Every organisation has its own unique challenges and goals when it comes to cyber security and incident response. Recognising this, AUSCERT provides a custom-designed TTXs tailored specifically to meet the objectives and requirements

of your organisation. Whether you need to focus on cyber incident response, business continuity, crisis management, or a combination of these areas, AUSCERT's TTXs can be adapted to align perfectly with your needs.

Additionally, AUSCERT offers comprehensive support throughout the entire process. From the initial planning stages, to execution and evaluation, AUSCERT can assist your organisation in delivering effective TTXs. Its goal is to ensure that the scenarios it creates are realistic and relevant, providing a meaningful test of your response capabilities.

## **INCLUSIVE PARTICIPATION ACROSS ROLES**

One of the key benefits of AUSCERT's TTXs is their inclusivity.

Participants from all roles within an organisation – whether operational staff, cyber security professionals, communication teams, executives, or a mix of these – can benefit from these exercises. This diversity in participation ensures a comprehensive understanding of how different roles interact and coordinate during an incident.

AUSCERT's skilled facilitators guide participants through realistic scenarios, prompting them to consider various aspects such as roles, responsibilities, coordination, and decision-making. These exercises are entirely discussion-based, meaning they do not require the deployment of equipment or other resources. Instead, the focus is on fostering a collaborative environment where participants can openly

discuss and refine their strategies for incident response.

### WHY CONDUCT TTXS?

Conducting TTXs offers a multitude of benefits for organisations looking to enhance their incident response capabilities. These include:

- **Testing and validation:** While having clear incident response plans and playbooks is crucial, their effectiveness isn't truly known until they are tested in a controlled environment. TTXs provide a safe, controlled way to evaluate these plans without the risks and consequences of a real incident. This allows you to see how well your strategies hold up under pressure and make necessary adjustments before a real crisis occurs.
- **Improved coordination:** TTXs simulate the pressures of a real incident, allowing participants to experience decision-making and coordination in a lower-stress environment. By practicing these skills in a simulation, participants can better understand their own responses and improve their performance in actual incidents. This experience can lead to more effective communication, quicker decision-making, and more efficient coordination among team members when a real crisis arises.
- **Stakeholder engagement:** TTXs can emotionally engage stakeholders, especially executives, in ways that traditional risk assessments and discussions cannot. By actively involving them in the simulation, TTXs help stakeholders to understand the tangible impacts of potential incidents and the importance of a robust response plan. This engagement can drive meaningful change within your organisation, leading to stronger support for cyber security initiatives and a greater emphasis on proactive risk management.
- **Continuous learning and development:** By conducting TTXs in a progressive, supportive manner that focuses on continuous improvement, organisations can create a culture that views mistakes as

opportunities for learning rather than reasons for penalty. This approach encourages a mindset of growth and resilience, where team members are motivated to enhance their skills and knowledge continuously. Over time, this can lead to a more agile and responsive organisation, better equipped to handle any challenges that may arise.

- **Meet contractual and regulatory requirements:** Many organisations have contractual obligations or insurance policy requirements to regularly conduct TTXs. These exercises can help to ensure compliance with these obligations, potentially lowering insurance premiums, and enhancing your organisation's reputation as a reliable and prepared partner. Furthermore, regulatory bodies like the Australian Prudential Regulation Authority under CPS234 recommend regular testing of incident response plans. TTXs provide a structured, effective way to meet these regulatory requirements, and demonstrate your commitment to cyber security best practices.
- **Better decision-making:** TTXs enhance or validate incident response strategies, ensuring that your organisation can be better prepared for making decisions effectively, efficiently

showcasing a proactive approach to incident management and demonstrating a commitment to continuous improvement.

- **Bridge the gap for non-technical stakeholders:** TTXs help non-technical stakeholders, such as managers and executives, to gain a better understanding of the complexities involved in incident response. Through participation in these exercises, they can appreciate the time and effort required for resolution and recovery, fostering greater empathy and support for cyber security teams. This understanding can lead to more informed decision-making and stronger alignment between technical and non-technical teams.

### READY TO ENHANCE YOUR ORGANISATION'S POSTURE?

AUSCERT believes that preparedness is key to effective incident response. Its TTXs provide a valuable opportunity for organisations to test their plans, engage their teams and build a culture of continuous improvement. Whether you are looking to develop new strategies or refine existing ones, AUSCERT's TTXs offer a practical, effective way to enhance your organisation's readiness for any crisis. •

Contact AUSCERT for more information today!





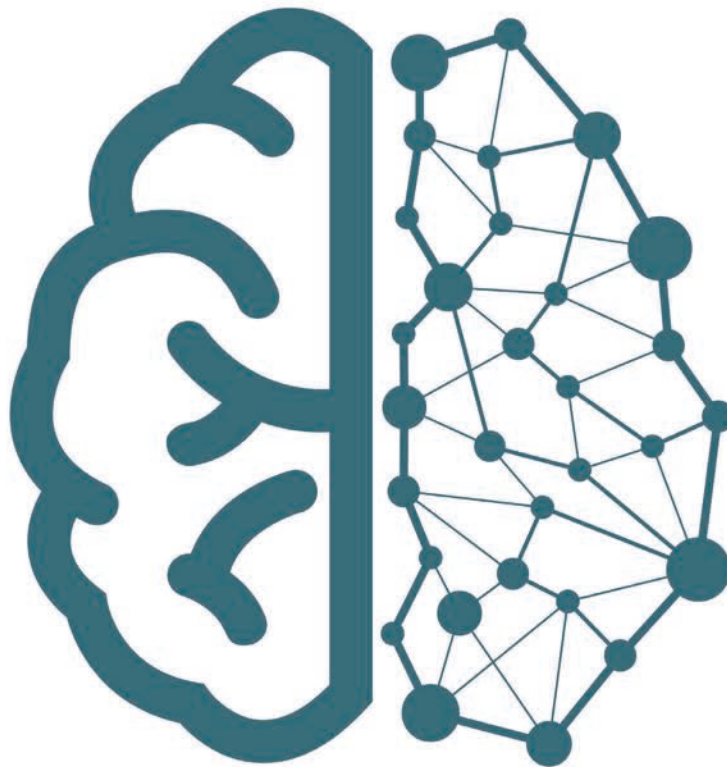
---

# TWO YEARS AFTER CHATGPT, THE GENAI CYBER WARS ARE JUST GETTING STARTED

*Artificial intelligence-equipped attackers are at the gates – so act tactically, and act now, reports **David Braue**.*

**I**t has been hailed as a game changer for personal productivity and business efficiency, but even as companies develop generative artificial intelligence (genAI) strategies and rollout pilot programs, cybercriminals are reaping dividends from embracing a technology that has been equally game changing for the process of targeting and exploiting online victims.

Little wonder: the preternatural skill of genAI large language models (LLMs) in interpreting and producing human-sounding text – backed by increasingly sophisticated analytics engines that allow them to meaningfully evaluate datasets, as well as visual, auditory and externally sourced web pages and other information – has given them the remarkable ability



to pass themselves off as human, crossing the so-called ‘uncanny valley’ at which machines are perceived as being indiscernible from humans.

It’s a threat that was widely predicted as soon as ChatGPT brought genAI into the mainstream – and its impact is already being felt in terms of the effectiveness of email-borne phishing attacks that have, thanks to cybercriminals’ use of genAI, become better written, grammatically correct, and generally better constructed than they ever were in the past.

AI-enhanced phishing attacks affected 91.1 per cent of organisations during 2023, security firm Acronis reported in its Cyberthreats Report earlier this year. The report blamed the November 2022 release of ChatGPT for a 222 per cent surge in email attacks during 2023, and warned that cybercriminals are extensively leveraging malicious derivative genAI LLMs such as WormGPT, FraudGPT, DarkBERT, DarkBART and ChaosGPT.

More than one in 10 social engineering attacks were business email compromise (BEC) attacks during 2023, Barracuda Networks noted in its recent Email Threats and Trends Report Vol. 1, which analysed 69 million email attacks across 4.5 million mailboxes, and, amid a ‘worryingly successful’ flood of phishing emails, found cybercriminals ‘leveraging the capability of genAI to scale and tailor their attacks’.

This was, the report found, driving a ‘steady rise’ in more targeted threats like BEC and conversation hijacking, which ‘require a lot of effort to execute’ but surged by nearly 70 per cent in the year after ChatGPT was introduced.

Such threats ‘need to be taken seriously and either blocked at the gate or quickly contained, neutralised, and eliminated if they make it through’, International Communications Director Tilly Travers noted, advising IT and security professionals to ‘understand how the email threat ecosystem is evolving and what this means for the organisation and its employees in terms of risk, resilience, and incident response’.

### **STILL BEING CAUGHT FLAT-FOOTED**

For all the awareness of genAI-powered phishing attacks, companies are still being caught out by them, as the carefully crafted and personalised attacks expose lingering shortcomings in technological defences and the persisting habits of employees to follow emailed instructions that exude an air of legitimacy.

With a recent Darktrace survey of security stakeholders finding that 84 per cent report being ‘significantly impacted’ by artificial intelligence (AI)-powered cyber attacks – compared to 74 per cent globally – it’s clear that Australian companies are either more susceptible to genAI-powered attacks

than those in other countries, or that the country’s relative wealth and high degree of connectivity makes us particularly attractive to cybercriminals.

With 79 per cent of companies admitting that they are not adequately prepared to handle AI-powered cyberthreats, Darktrace Asia-Pacific and Japan Vice President of Enterprise Security Tony Jarvis noted the ‘industry-changing advantages’ of genAI and, given the strong growth in AI-powered attacks, called it ‘worrying [that] our cyber professionals don’t feel they have the tools to meet this challenge’.

**More than one in 10 social engineering attacks were business email compromise attacks during 2023, Barracuda Networks noted in its recent Email Threats and Trends Report Vol. 1, which analysed 69 million email attacks across 4.5 million mailboxes...**

‘AI is the best defence against AI,’ he said, hinting at the now-ubiquitous use of defensive AI tools – which not only ‘recognise how your network behaves [and] spots unusual behaviour’, but are also now being increasingly paired with genAI LLMs to help analyse and present their meaningful analysis to companies that, Darktrace has also found, are struggling to find enough skilled personnel to manage the everyday flood of security alerts and tools.

While much of the recent conversation around AI has related to its ability to enhance phishing attacks, experts warn that AI is actually being used in a broad range of other ways that security executives must be aware of.

AI has five main characteristics – attack automation, efficient data gathering, customisation, reinforcement learning and employee targeting – that make it flexible enough to support a broad range of attack types, CrowdStrike Senior Product Marketing Manager Lucia Sanham noted in a recent rundown of the types of AI-powered cyber attacks that companies are likely to see.

That includes not only AI-driven phishing attacks, but also ransomware campaigns and AI-driven social engineering attacks, which are more sustained campaigns that utilise malicious GPTs to identify suitable targets, develop an online persona and corresponding online presence to communicate with the target, develop a ‘realistic and plausible scenario’ to generate attention, and write personalised messages or create audio recordings or video footage to keep their attention.



This last aspect has become particularly problematic given genAI LLMs' evermore powerful capabilities around photo, video and audio generation – which can not only produce deceptive 'deepfake' content with a worryingly high degree of verisimilitude, but can also even mimic a person's voice after being trained on just a few seconds of audio captured from a victim's voicemail message or a short, anonymous phone call.

Bring these elements together, and it's not hard to imagine a scenario where a malicious AI not only identifies a finance officer who is likely to have the ability to wire them money, but also researches their interests on social media to gather enough intelligence to confidently approach them with a voice simulating that of a key supplier – purportedly, for example, to inform the victim of a change of bank account details for an upcoming payment.

AI LLMs are also being directly targeted with 'AI poisoning attacks', in which cybercriminals manipulate the inputs to a model to train it to deliver inaccurate information to applications that normally rely on its accuracy.

## WHAT YOU SHOULD BE DOING ABOUT IT

For companies that just want to get on with their business, the escalating threats posed by genAI-equipped cybercriminals are yet another headache – but they can be managed if you take the initiative to invest the time, manpower, and funding into both evaluating your exposure and investing in the right technologies to reduce it.

Security vendors have been proactive about advertising the new AI capabilities they offer, but it's important to learn enough about the technology to be able to evaluate their claims objectively and effectively – and to do so for any genAI tools you may be considering as part of your operational business systems or security response.

Resources such as the Department of Industry Science and Resources' newly released Voluntary AI Safety Standard have laid out meaningful guidelines to help companies work through this process, while the Enkrypt AI Safety Leaderboard uses a number of metrics to compare LLMs' relative risk in terms of their susceptibility to being jailbroken – manipulated into functioning in ways they're not supposed to – as well as their potential for bias, likelihood of seeding malware, and an assessment of its 'toxicity' in terms of being manipulated into producing threatening, insulting, profane, or other outputs.

An important point to keep in mind is the importance of retrieval-augmented generation (RAG), a capability that allows LLMs to access current and regularly updated information – in a security context, for example, this might include details of new threats

and compromises sourced from the MITRE ATT&CK Framework – without having to spend many days, and millions of dollars, retraining the model with that new information.

'It is important to use RAG,' SentinelOne Chief Technology Officer Wayne Phillips told this year's AusCERT Conference, pointing out that the technique is essential for keeping up with the ever-changing cyber security attack climate.

'If you ask the system to bring back a list of indicators of compromise by Wizard Spider that relate to logins,' he explained. 'It won't know what [Russian cybercrime group] Wizard Spider is – so it needs to go to a knowledge base and pull that back.'

Companies should also be careful about putting too much into a single LLM.

'It needs to have not just a ChatGPT-style model that does everything, because they "hallucinate" all the time,' he explained. 'You need to have very discrete models that do very specific things so they don't hallucinate, and then you can swap them out if they stop working.'

Getting strategic about genAI also requires considerable upskilling – think about training your security staff in prompt engineering so they can become adept at extracting the information they need from the system – and a clear plan for testing your own system for vulnerabilities so that you can fix them before AI-equipped adversaries do.

This capability can be delivered automatically by firms such as SecurityScorecard, or through more deliberate and complex engagements with a security consultancy offering strategic penetration testing services – but a key consideration is to test often, test effectively, and to ensure that any identified weaknesses are actioned for remediation as soon as possible.

Just how genAI will change your security strategies and practices will evolve over time, but in an era of heightened cyber attack, it is unacceptable to ignore a technology that has rapidly become core to the arsenal of both cyber attackers and defenders.

'We are entering an era of a cyber arms race where AI will amplify the impact for both the security professional and the adversary,' CrowdStrike CEO and Co-founder George Kurtz – who, ironically, would be thrust onto the world stage in July after a catastrophic systems failure, and not a cyber attack, caused global systems outages – wrote earlier this year when introducing the company's 2024 Global Threat Report.

'The rise of genAI has the potential to lower the barrier of entry for low-skilled adversaries, making it easier to launch attacks that are more sophisticated and state of the art,' he said. 'The "good enough" approach to cyber security is simply no longer good enough for modern threats.' ●

---

# Cyber security trends across Australia

— BY RIKI BLOK, TALENZA —



**T**alenza Cyber completes industry insights at the end of each financial year. We call this the 'Cyber Wrap'. Within this report, we look at trends related to tenure, role-specific insights, salary, education background, and add our own insights from directly recruiting in cyber.

This article has been written to highlight some of the key changes and interesting data points we have witnessed over the last financial year. A full version of our insights deck is available on request.

### THE POST-COVID BOOM IS WELL AND TRULY OVER

Following the first COVID lockdown, there was a feeding frenzy. This last year has seen a far higher percentage of role shifters going sideways or backwards on salary – our latest survey suggests this is 35 per cent, which is incredibly high. We put this down to a few key things:

- › title creep/position creep
- › salary inflation due to post-COVID boom
- › redundancies in larger businesses
- › slowing economy (this has meant less investment in large programs).

There is a fair bit to unpack in those bullets above; however, we see this year as somewhat of a natural correction. Some businesses overspent on talent and projects coming out of COVID – as a result, most cyber budgets have had a moderate increase. This moderate increase has not kept up with the increases from vendors on their core offerings. Effectively, this means that a lot of budgets are actually going backwards this financial year.

### LEADERSHIP ROLE TRENDS

Our specific research and insights go against what the data would suggest.

In the early part of the last financial year, there was a large amount of movement for CISO and team heads/level managers. This seems to have calmed in the latter part of the financial year; overall, 15 per cent of people shifted roles, which is not abnormally high.

We noticed a large number of newly created 'Head of' or CISO-style roles within Tier 2 and Tier 3 financial service businesses, in particular. We expect this trend to continue over the coming years, along with additional growth in the critical infrastructure sector.

In a nutshell, our view is that this is a role family that has an oversupply of candidates against the available roles. It is not uncommon for there to be more than 300 applications for roles in this space.

This means that hiring managers and potential employers have significant choice of profiles. Generally speaking, if you are looking for a role in this space, you need to be very closely aligned to what the company sees as its ideal candidate.

Companies are perhaps less inclined to 'take a chance' on someone from outside the target sector or with slightly different experience.

### GENDER DIVERSITY IS TRENDING IN THE RIGHT DIRECTION

Great initiatives are in place to drive more women into cyber, including well-known groups like the Australian Women in Security Network; however, there is a significant effort with high school and university students to drive higher uptake of STEM programs.

More can be done to retain female talent; however, it is positive to see the percentage of less-experienced women in cyber roles growing year on year. For 0–5 years of experience, the gender split is 25 per cent; however, this drops to 16 per cent for 15–30 years of experience.

Gender split by role families holds some interesting numbers for those with 0–5 years of experience:

- › Governance, risk management and compliance: 34 per cent
- › Cyber defence: 27 per cent
- › Offensive security: 10 per cent.

### JUNIOR ROLES ARE TRENDING UP

This statement might go against what people discuss on LinkedIn – the statistics we have suggest significant growth in particular role families, with little or no growth in others.

Something that isn't spoken about much in this space is the sheer volume of people trying to break into the industry. We now have fully fledged university degrees focused on cyber security, combined with the endless amount of certifications and courses to address the skills gap.

In my opinion, there is a talent mismatch more than there is a talent shortage. By this, I mean that there is an oversupply of junior talent and executive level talent; however, in the 5–10 years of experience level, where most businesses hire, there is a significant shortage of skilled talent.

Cyber defence roles for those with 0–5 years of experience experienced a 20 per cent growth in the last financial year, and it also grew by 30 per cent the year prior. That means that there are around double the amount of junior security analyst, engineer and cyberthreat intelligence roles than two years prior.

Other role families have had stagnant or no growth – offensive security, application security and identity are the three families with almost no growth, which suggests that shortages will continue in these role families.

### WANT TO SEE MORE?

This article just scratches the surface of the insights and research we've gathered. If you're looking for more detailed or specific information, don't hesitate to reach out. I'd be happy to provide tailored insights that align with your needs in the ever-evolving cyber market. ●



---

# RESILIENT LEADERSHIP IN CYBER SECURITY

— BY ROXANNE PASHAEI —

*Maintaining focus and unity in challenging environments.*



---

**S**tepping into the role of cyber security leadership in a change-resistant environment can feel like stepping into uncharted territory, or entering a battlefield where the real challenges extend far beyond managing cyberthreats. While the expectation may be to focus on building defences, managing risks and staying ahead of emerging threats, the true test often lies elsewhere. The greatest challenge isn't always technical; it's about navigating an organisational culture that may not be fully ready for change, or that may not be fully prepared to embrace a fresh approach to security leadership.

In environments like this, resilience becomes essential. It's about adapting, standing firm and pushing forward in a space that may not yet be ready for change – or entirely ready for new leadership approaches.

Even with years of experience, technical expertise alone won't suffice. Growing into the role requires recognising that the real obstacles aren't just technological. The culture encountered can be deeply rooted in tradition, resistant to innovation and comfortable with the status quo. As responsibilities grow, so do the pressures of balancing expectations and resistance. The challenge is no longer just about securing systems – it becomes about ensuring that your voice is heard, and your perspective is valued in a space not yet accustomed to hearing it.

---

**The greatest challenge isn't always technical; it's about navigating an organisational culture that may not be fully ready for change, or that may not be fully prepared to embrace a fresh approach to security leadership**

---

#### **NAVIGATING RESISTANCE IN CYBER SECURITY LEADERSHIP**

In many organisations, particularly those with deeply ingrained practices, new cyber security leadership often encounters subtle resistance. Proposals for security initiatives may be met with hesitation, or even quietly dismissed, while similar suggestions from established voices gain more traction. This reveals a more complex challenge. It speaks to an underlying resistance to change, to fresh perspectives and, at times, to new leadership approaches.

This resistance often arises from a misunderstanding of cyber security's role. Instead of being seen as a strategic asset, security can be perceived as an impediment to operational efficiency.

The real task, therefore, is not just in implementing security measures, but also in reshaping the organisational mindset to understand their necessity and value.

In such environments, resilience is not merely about enduring challenges. It requires adaptability, a willingness to learn and an innovative approach to influence change within the organisation.

#### **BUILDING RESILIENCE: STRATEGIC WINS AND LONG-TERM IMPACT**

Change is never easy. Hence, driving meaningful change in cyber security should often begin with shifting focus away from obstacles and toward what can be influenced. Identifying key stakeholders who share a vision for a more secure and resilient organisation is critical. Aligning security initiatives with the broader strategic goals of the business can be an effective way to win over sceptics.

In many cases, success is built incrementally. Demonstrating the tangible benefits of security through small, measurable wins builds trust and sets the stage for broader initiatives. When security is reframed – not just as a protective measure, but as a driver of operational efficiency and business continuity – it becomes integral to the organisation's success, gradually transforming resistance into acceptance, with the power to shift the narrative.

#### **SHIFTING THE NARRATIVE: TURNING CHALLENGES INTO OPPORTUNITIES**

Driving meaningful change in cyber security often requires a shift in perspective – both for the leaders guiding the effort, and for the organisation itself. Security can no longer be treated as a standalone technical function – it must be woven into the very fabric of the business.

Imagine security not as a barrier to progress, but as a strategic partner that ensures that the business runs smoothly, protects its core operations and safeguards its future. Start small if needed. Focus on achieving small wins that demonstrate the tangible benefits of security. These small successes will begin to add up, and as the value becomes evident, it will be easier to implement larger initiatives.

But make no mistake: this journey is not without its challenges. Resilience is key to navigating the setbacks and difficulties that inevitably arise along the way.

#### **NAVIGATING UNCONSCIOUS BIAS: A HIDDEN CHALLENGE**

One of the less-visible challenges that leaders – especially women – often face is unconscious bias. This bias can be subtle and difficult to identify, but its effects are very real. It can show up in meetings where ideas may be dismissed,

only to be reconsidered when someone else presents them later. While this isn't always malicious, it can still be disheartening and frustrating for those trying to make a positive impact.

Dealing with unconscious bias requires a balanced approach. It's essential to maintain professionalism while ensuring your contributions are acknowledged. A respectful, but firm, reminder can often change the dynamics of a conversation: 'I'd like to revisit my earlier point, as I believe it's critical to our discussion.' Over time, this assertiveness can help reshape how your ideas are received and respected.

## THE ADVANTAGES OF RESILIENCE: STRENGTH AND INFLUENCE

Despite these challenges, resilience offers significant rewards. In an industry where the landscape is ever-changing, the ability to adapt, recover and push forward is critical. Here's what resilience can bring:

- › **Stronger relationships:** Resilience builds trust and respect over time. By demonstrating the ability to handle setbacks with grace and persistence, leaders earn the confidence of colleagues and stakeholders, making it easier to advance security initiatives.
- › **Increased influence:** When security is positioned as a business enabler – aligned with the organisation's broader goals – leaders gain more influence over decision-making. As the value of security becomes clearer, it becomes easier to advocate for necessary changes.
- › **Long-term success:** Resilience ensures that setbacks don't derail progress. It allows leaders to continue moving forward, even in challenging environments, ultimately leading to long-term improvements in the organisation's security posture.
- › **Shaping leadership:** Resilience helps in building stronger alliances within the organisation. Setbacks provide valuable lessons – not only about cyber security, but also about the human and organisational dynamics that underpin it.
- › **Building a culture of change:** Over time, resilience helps create a lasting cultural shift. While change may be slow and incremental, each step contributes to a more security-aware culture, preparing the organisation for future challenges.

## THE DISADVANTAGES OF RESILIENCE: KNOWING THE LIMITS

Resilience also has its downsides, and it's important to be aware of them. These include:

- › **Emotional fatigue:** Constantly pushing through challenges, particularly in an environment

where you're not fully supported, can be exhausting. There are days when you may feel drained and frustrated. Maintaining resilience requires emotional energy, making it crucial to prioritise self-care.

- › **Isolation:** In leadership roles, especially in male-dominated environments with unconscious bias, it can sometimes feel lonely. Even with allies, there may be moments of isolation, where the challenges faced are uniquely yours. Resilience, while powerful, often means standing alone.
- › **Slow progress:** Resilience doesn't always result in immediate success. In deeply traditional environments, progress can be slow. This can lead to moments of frustration, where it feels like you're taking one step forward and two steps back. Learning to be patient is essential.

---

**What I've come to understand through my own journey is that resilience is the true key to success. It's not about being unbreakable – it's about learning to bend without snapping, to keep moving forward even when the road is rough**

---

## CONCLUSION: RESILIENCE AS A KEY TO LEADERSHIP

Navigating the complexities of cyber security leadership, particularly as a woman, presents unique challenges. There are visible hurdles that often exist beneath the surface, making the path forward difficult.

What I've come to understand through my own journey is that resilience is the true key to success. It's not about being unbreakable – it's about learning to bend without snapping, to keep moving forward even when the road is rough.

Resilience has helped me lead my team and my organisation through change, even when that change was resisted. It's allowed me to build stronger relationships, influence culture and show the true value of cyber security. And while it hasn't always been easy, it's a journey I'm proud to have taken.

For anyone stepping into cyber security leadership – especially women – my advice is simple: be resilient, be patient, and view every challenge as an opportunity for growth. Resistance will undoubtedly come, but resilience will help you transform that resistance into your strength and pave the way for lasting impact. ●



# SANS Institute Australia: 25 years of strengthening the nation's cyber security capabilities

**FOR 25 YEARS**, SANS Institute Australia has been at the forefront of building resilience and sovereign capabilities within the nation's cyber security community. With more than 2600 Australian organisations empowered through its cutting-edge training, certification and workforce development, SANS Institute has proven that strong cyber security defences begin with skilled professionals.

**WHY IS THIS IMPORTANT, AND WHY SANS?**

In today's increasingly complex digital landscape, partnering with SANS Institute means more than just gaining access to 85-plus world-class cyber security training courses; it means investing in a strategy that delivers a measurable, positive return on investment through an elevated security posture and reduced operational risks. Trusted

by over 18,000 Australian cyber security practitioners, SANS is dedicated to delivering and validating hands-on cyber security skills needed to defend against new and emerging threats.

**REAL IMPACT, REAL RESULTS, FAST**

What makes SANS different is its commitment to building cyber security capabilities at every level of an organisation. SANS's globally recognised training and Global Information Assurance Certifications across artificial intelligence, cloud security, cyber defence, digital forensics, industrial control systems, offensive operations, leadership and more are designed to provide organisations with the tools and knowledge to improve their security from the ground up. Whether your organisation's focus is reducing risk, protecting sensitive data, or

ensuring compliance with regulatory requirements, SANS training ensures that your cyber security strategy aligns with and enhances your overall business objectives. This alignment allows your organisation to be proactive rather than reactive, helping to prevent security incidents before they occur, while also reducing operational downtime.

**SANS WORKFORCE DEVELOPMENT PROGRAM: THE SOLUTION TO AUSTRALIA'S CYBER SECURITY SKILLS SHORTAGE**

The SANS Workforce Development program plays a vital role in addressing Australia's cyber security skills shortage. From talent assessment and recruitment, to career planning and team building, SANS helps organisations cultivate in-house cyber security expertise by developing the potential within their existing workforce.

**IT'S TIME TO ACT**

For 25 years, SANS Institute has been a constant, trusted partner in Australia's cyber security community. SANS's ongoing partnerships with Australian organisations helps build a stronger, more resilient cyber security ecosystem – one that's prepared for the challenges of today, and the evolving threats of tomorrow. SANS is here to stay, and it will continue to support Australia's cyber security landscape with the same dedication and expertise that has set it apart for decades. ●

*If your organisation is looking to strengthen its cyber security capabilities and support long-term business goals, email [anz@sans.org](mailto:anz@sans.org) or call +61 2 6174 4581 to learn more about how SANS Institute Australia can help elevate your cyber security strategy. Together, we can build a safer, more secure future for your organisation and the broader Australian community.*



The SANS logo is displayed in a large, white, serif font.The GIAC CERTIFICATIONS logo is displayed in a white, sans-serif font, with "GIAC" on the top line and "CERTIFICATIONS" on the bottom line.The 25 years IN AUSTRALIA EST. 1999 logo is displayed in a white, sans-serif font, with "25 years" in a large, stylized font, "IN AUSTRALIA" in a smaller font, and "EST. 1999" in a small font.

# SANS Workforce Development

SANS Australia is dedicated to strengthening the nation's cybersecurity workforce to ensure a more secure future for Australia. From talent assessment to career planning and team building, SANS is your ideal partner for developing a high-performing cybersecurity team.

Accelerate the growth of your cybersecurity team with these offerings from SANS:



**Strategic talent  
development**



**Hands-on  
skills exercise**



**Leadership  
development**



**Skills-based  
placement**



**Role-based  
job paths**



**Team building**



**Career  
progression  
plans**



**Trained and  
certified  
workforce**



**Aptitude tools**

To find out how SANS can help with developing your team's cybersecurity skills,  
**Contact [anz@sans.org](mailto:anz@sans.org) for more information | +61 2 6174 4581**



# AUCYBER

## SECURING AUSTRALIA'S DIGITAL FUTURE

- ⦿ Governance, Risk & Compliance
- ⦿ Cyber Training & Consulting
- ⦿ Managed Security Operations Centre (SOC)
- ⦿ Managed Detection & Response
- ⦿ Cloud Services
- ⦿ Managed IT Services
- ⦿ Backup & Disaster Recovery

1800 282 568



[aucyber.com.au](https://aucyber.com.au)