Cyber Today

EDITION 1, 2021

THE ETHICS OF SMART DEVICES

TAKING A SHOT IN THE DARK (WEB)

RANSOMWARE: FROM BAD TO WORSE

AISA

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

- Incident Management
- Phishing Take-Down
- Security Bulletins
- Security Incident Notifications
- Sensitive Information Alert
- Early Warning SMS
- Malicious URL Feed
- Education

MEMBERSHIP ENQUIRIES

+61 (0)7 3365 4417
membership@auscert.org.au
auscert.org.au

AUSCERT

AUSCERT2021
Cyber Security Conference
20 YEARS

20th Annual AusCERT Cyber Security Conference

SOARing with Cyber

11th - 14th May 2021 // The Star Hotel, Gold Coast, Australia

4 DAYS

50+ SPEAKERS

IN PERSON & VIRTUAL

REGISTER NOW » conference.auscert.org.au

PUBLISHED BY :

EXECUTIVE MEDIA
NEW YORK | SYDNEY | MELBOURNE | ADELAIDE
EST 1972

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
Giulia Heppell
giulia.heppell@executivemedia.com.au

EDITORIAL ASSISTANTS
Kate Hutcheson, Simeon Barut

DESIGN
Alex Fleischer

PARTNER ORGANISATIONS
AusCERT, Cybermerc,
Forcepoint SC Pty Ltd,
Progress Software Pty Ltd,
Rapid7 Australia Pty Ltd, SANS,
SecureWorks

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.

All stock images sourced from iStock.com

Vegetable based inks and recyclable materials are used where possible.

Proudly Printed
In Australia

Contents

FOREWORD

UPDATE

INSIGHT

SPOTLIGHT

CYBER ATTACKS

CYBER SAFETY

SECURITY

CRITICAL INFRASTRUCTURE

HR AND RECRUITMENT

EDUCATION AND TRAINING

Foreword

A message from Tony Vizza, AISA Board Director.

Tony Vizza

There has been no shortage of adjectives and superlatives used to describe the year that was. 2020 was a watershed year in disruption – a word that IT and cyber security professionals know intimately well. It's a word that often describes challenging events or, inversely, a word that can also describe positive change.

The disruption caused by COVID-19 affected the IT and cyber security worlds profoundly. This time last year, many of us were involved in desperate bids to help our organisations ensure that an entire workforce was able to work remotely, or, in some cases, provide that functionality for the very first time. Immediately after, we were tasked with the formidable duty of keeping our colleagues cyber-safe while protecting the information assets of the organisation. As the year dragged on, in June we were advised by Prime Minister Scott Morrison of increased sophisticated state-based cyber attacks, while witnessing breach after breach making the headlines. In those precarious weeks and months, compounded by lockdowns and restrictions, it's fair to say that most of us developed, evolved and increased our resilience, not just in terms of cyber security, but also as individuals, families and communities. It's important to recognise, however, that many were unable to cope with the challenges the year brought, stretching mental health services beyond their normal capacity.

As the fog of uncertainty has slowly begun to clear, organisations have discovered that remote work is far more viable than what was initially thought, realising huge cost savings in terms of travel and real estate, with minimal impact on productivity. Many organisations, in fact, are now in the process of adopting remote work on a permanent basis. Since the pandemic emerged, some organisations, particularly in the IT sector, have seen huge increases in revenue and profitability. AISA's State of the Digital Nation: Cyber Security in Australia 2020 survey supports the view that the disruption provided many in the cyber security industry with a silver lining, even though many of us felt some pain early on.

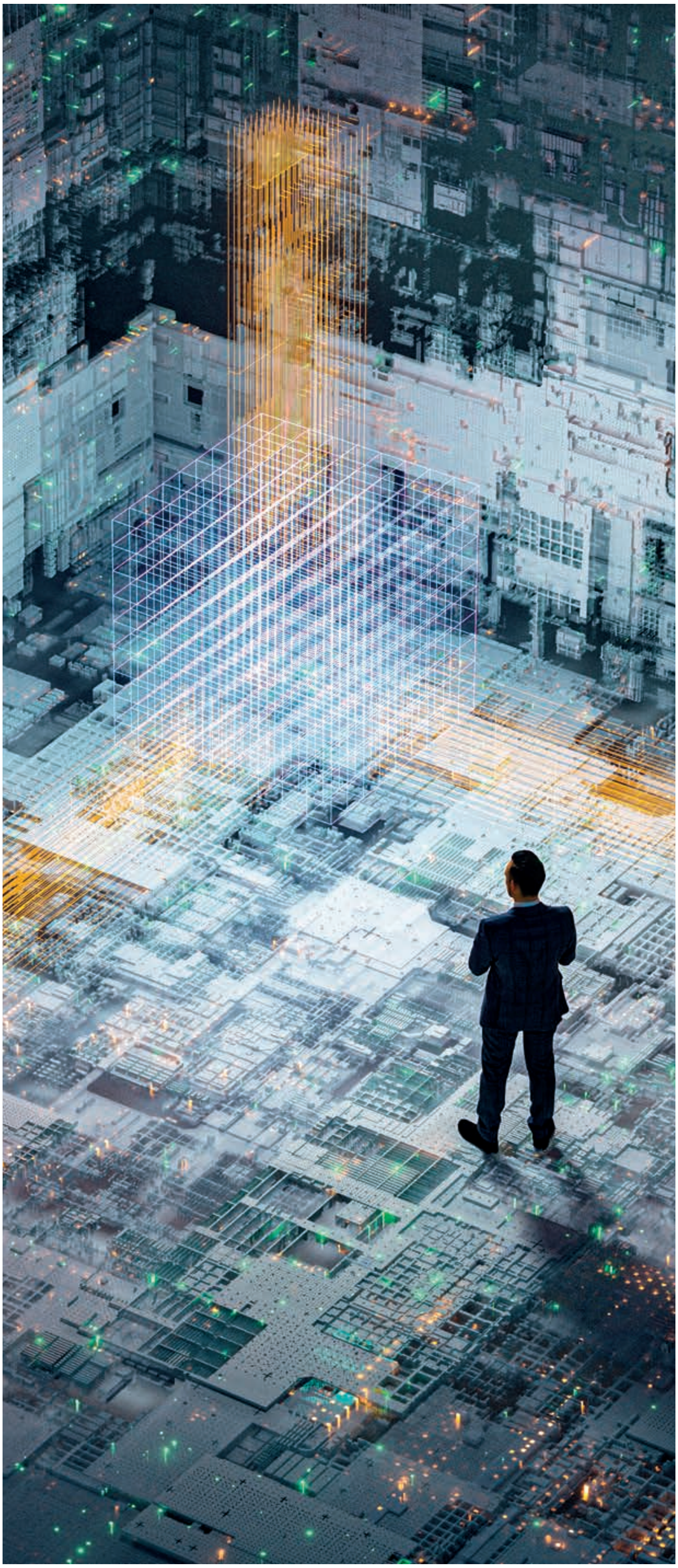
Of course, this disruption has not spared AISA. It feels like a lifetime ago, but at the start of 2020, our members and partners were excited about what was meant to be a successful year ahead. Literally overnight, our branch events schedule was disrupted, and our in-person conferences were either postponed or had to go virtual. We grappled with the question of how to provide the best possible value to members and help to digitally safeguard the community in a pandemic, when face-to-face events simply weren't possible.

It is important to consider that not all disruption is adverse. Proof of this is AISA's membership, which has grown to more than 7500 cyber security professionals – a 42 per cent growth since 2019. AISA continues to provide thought leadership, support and insight to government, industry, academia and the cyber security community, as well as to the broader community across Australia. AISA continues to monitor developments not just in relation to cyber attacks, but also privacy concerns and fake news narratives that represent a growing threat to our way of life, while increasing our resolve towards achieving our mission.

In late 2020, AISA also submitted detailed responses into the review of the Privacy Act and multiple requests for information related to the security of Critical Infrastructure under the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill. AISA board members represented the industry at the NSW Government Parliamentary Inquiry into Cyber Security, and at numerous state and federal government committees related to cyber security.

Perhaps the most promising development at the end of last year was that the AISA Perth Branch managed to deliver an in-person half-day event. Seeing the event take place felt like seeing a light at the end of a very long tunnel. And with low COVID-19 case numbers continuing nationally, the pending release of vaccines and a rebounding economy, better days are certainly ahead.

This year will continue to present challenges for the industry, our members and the community. The pandemic isn't over; the severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2), which causes the COVID-19 disease, continues to evolve and adapt, and governments continue to grapple with containment and management measures; however, businesses, communities and federal, state, territory and local governments across Australia are also adapting as we learn to live in a world with the virus. As vaccination programs roll out across the globe, 2021 will hopefully be a better year than 2020. Confident in this belief, now more than ever, the community and industry will need to continue to work together towards achieving a cyber-safe and secure Australia. ●



Effective security incident handling

BY NEIL CAMPBELL, VICE PRESIDENT APJ, RAPID7

Being organisationally and technically informed.

Neil Campbell

When a security team detects a threat, it's essential that you're ready for what comes next. This requires not only having a tightly coordinated incident response plan, but also a sequence of actions and events assigned to specific stakeholders on a dedicated incident response team. Because while being technically ready to deal with any threat is a major part of dealing with an incident, you also need to be organisationally informed.

Like thousands of other Australian organisations, you likely deal with a multitude of security incidents each day. And, as we all know, fixing a breach is far more costly than prevention. But if you find yourself in the midst of dealing with an incident, here's how to be both technically and organisationally informed.

Beyond the technical

Any incident response needs to include people in positions beyond just technical – whether that's communicating with clients or customers, or managing regulatory and media requirements. You need the appropriate experts in your organisation involved in, and agreed on, strategy from the beginning.

Stakeholders from legal, corporate communications, human resources and other departments should also be involved in the preparation and execution of any incident response activity. Minutes count when a network has been infiltrated or data has been breached. Waiting to figure out processes in the heat of the moment will likely result in confusion and, worse still, slower overall response times to the incident itself. When a crisis hits, your team needs to know that they have the support from key stakeholders to act quickly.

Remediation is just the start

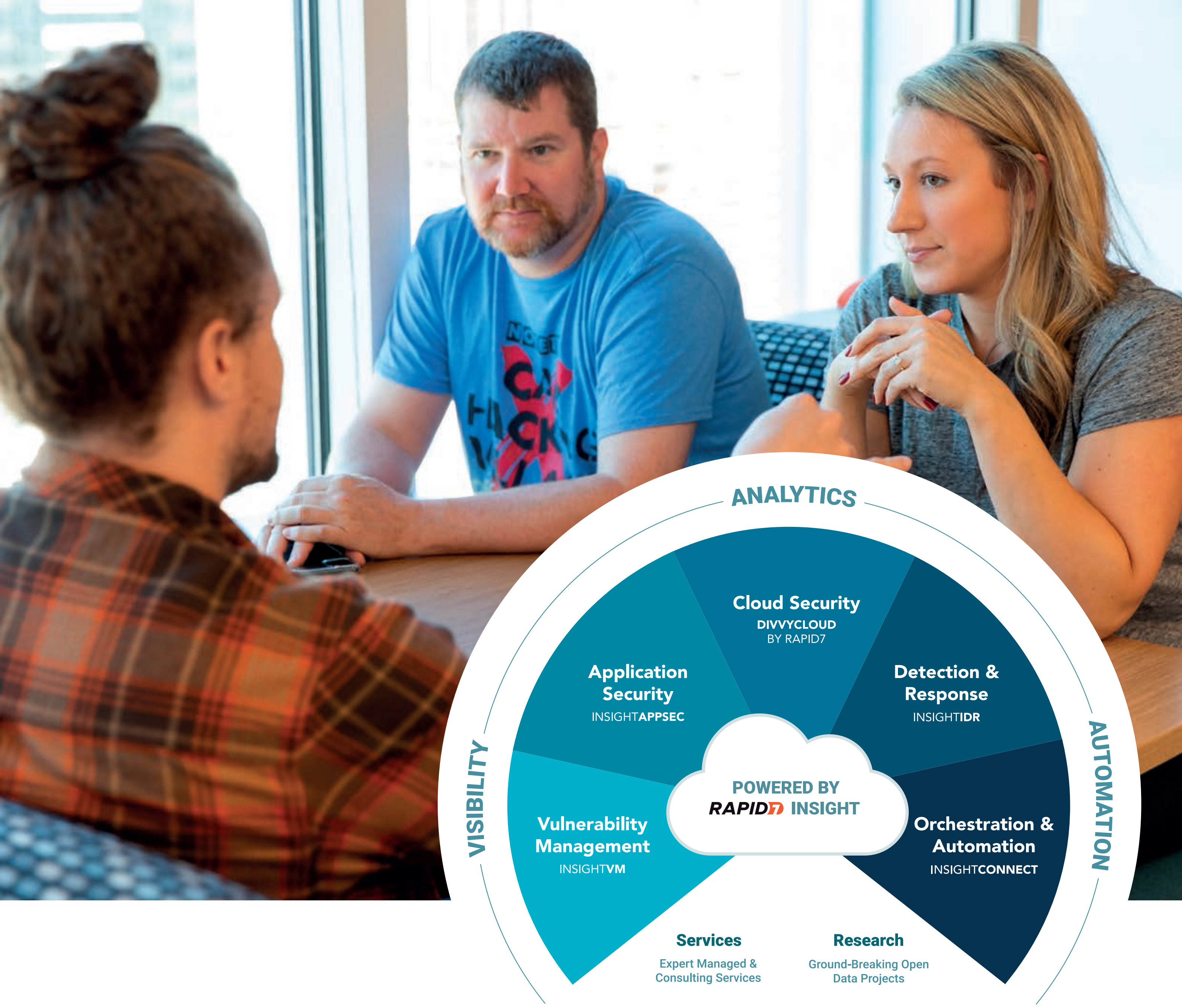
Dealing with and remediating an incident only starts once the technical aspects have been addressed. Consider how to balance the need to get systems back up and running normally as soon as possible, against the need to preserve evidence for an investigation. Depending on what the breach is, an investigation will likely need to be performed to determine what data may have been taken and whether that triggers any notification requirements. You may also want to adapt and evolve your security posture.

What did you learn?

The incident response team should conduct a post-mortem to learn from the experience. It's important to glean as many lessons as possible from responding to a real incident. Learn from your experience and understand what the attackers did. What did they manage to compromise? What worked in your response? What didn't work, and what could work better or faster?

Ensuring that a post-mortem process is available to capture critical intelligence and recommendations to prevent breaches in the future is an opportunity to fine-tune your incident response program, as well as to retune your security program overall. It will ensure that your threat detection and incident response programs are consistently maturing. ●

For more information, visit https://www.rapid7.com/c/ANZ-IDR



Our journey with AISA

Andrew Evans *and* **Sharmila Packiaraja** *catch up over a coffee to reflect on their AISA journey.*

Andrew Evans

Sharmila Packiaraja

Andrew Evans and Sharmila Packiaraja are our recently elected Directors to the Board of AISA. Their journey began as volunteers in Melbourne and Darwin.

Sharmila Packiaraja (SP): Why AISA? Andrew, I would love to hear about your beginnings with AISA.

Andrew Evans (AE): I first became aware of AISA in October 2012. I had recently emigrated from the United Kingdom to Australia, and was seeking a professional cyber security association in which to network and seek work. AISA came highly recommended, and I attended branch meetings and spoke to Branch Chair Beverley Roche, who kindly offered to meet me for coffee and provide insights (who knew coffee was so essential for networking?). Beverley gave me great advice about breaking into the Australian market, and her only ask was if an AISA member sought advice, I would give it freely and pass on the goodwill.

SP: Wow, Andrew, that is amazing – a move from the United Kingdom to Australia.

Well, my journey with AISA began with my move from Melbourne to Darwin in 2015. Darwin bought me the right challenge for my security career, and presented me with immense opportunities to grow and expand. When I joined my new Darwin workplace, my then boss John Clelland suggested that I consider starting a Darwin AISA Branch, and the rest is history. The beauty is that John was never affiliated with AISA, but saw the value AISA would bring to the local ICT and business community across the Northern Territory. The branch was inaugurated in 2016; I gathered more volunteers and formed a strong team to deliver events across the territory.

AE: What a challenge, setting up a branch from scratch!

Melbourne had an established branch when I joined, and it undertook a variety of events in support of AISA's mission. Monthly presentations were CBD-based, often attracting between 40 and 50 members with feedback consistently requesting breakfast, lunch and/or dinner events. Through these events, I met the committees, networked and easily met my goal of gaining five new LinkedIn connections per meeting. Nowadays, as an AISA volunteer, I'm particularly fortunate to have an employer that values the work AISA undertakes, and provides staff with a volunteer day that I use with AISA.

SP: Here in Darwin, branch events differ slightly.

In a month, we would be on a plane to Nhulunbuy, delivering cyber awareness for local businesses, then back to Darwin to deliver advice on how the elderly can protect themselves from scams, and finally off on a road trip for three hours to deliver a presentation in Katherine for ICT businesses. Typically, we would have between five and 80 attendees and meet our charity status by offering other events for non-members. Our mantra is, 'It doesn't matter how many attend, if we change the view of one person in a day, it's a win!'

AE: Crikey! That's a lot of travel. A good team is essential to deliver those events, and Melbourne has one, too.

We recently expanded the number of committee members to 10 due to membership growth, and we aim for gender balance as it's important to promote women in cyber and improve female attendance. I believe the industry needs to do more to encourage greater gender diversity, and AISA's student membership is trending positively in this direction.

SP: I am not going to say anything new on this topic. Throughout my career, most businesses I was part of were not balanced. The representation of women in tech across the Northern Territory is healthy; however, cyber is less mature. To increase numbers, I mentor female students and advocate female participation at Darwin ICT events. There are no magic bullets! It's critical that we all drive this with intensity and want a genuine change in people's mindsets. It is important that business and organisation leaders realise that teams with diversity of thought will create greater business outcomes.

AE: I agree, and have seen many requests for mentors, career advice, cyber education and certification.

Cyber is a fast-moving field, and it's important to remain relevant and qualified. I'm currently instructing the online AISA-ISC2 CISSP course to members, and have seen a number of recent students successfully passing the CISSP exam – thus adding to the number of cyber-certified professionals in the workforce. It's refreshing to see ambitious people improving themselves through AISA.

SP: Cyber career pathways are limiting in Darwin. The ICT industry is mainly Northern Territory Government–led, with a majority of small businesses. Small businesses have limited cyber roles, and most of them remain within government. In saying that, from 2015, I have witnessed growth in our sector, opening doors for a few locals, but largely to other state and territory candidates (I was one of them!). COVID has recently forced many businesses to adapt to a remote-working model, allowing people in Darwin and regional towns to be viable candidates, and providing viable cyber pathways. This would enable places like Darwin to grow and retain their cyber workforce.

We both enjoy that feeling of euphoria when giving something back to the community. In our new roles, how do we maintain our passion and carry this to the broader association?

AE: Great question! I'm keen to ensure that AISA remains the primary Australian group for cyber security. I'm passionate about education, and am keen to create and promote opportunities for all members. At board level, we shape strategy, provide leadership and assist the frontline branches. As a motivated and positive professional, I see myself contributing to the great work of AISA. For an association of four full-time staff and volunteers, to deliver what AISA delivers is impressive.

SP: I will continue to be an advocate and a change-maker in the lives of senior citizens, children, Aboriginal communities and regional businesses through cyber security initiatives, and will amplify this at all levels of the association. Through my passion and drive, I will seek to strengthen our integrity through communities by leading activities and widening the membership variety. ●

PARTNER CONTENT

SASE: redefining the cyber security landscape

BY NICK SAVVIDES, SENIOR DIRECTOR OF STRATEGIC BUSINESS, FORCEPOINT, ASIA PACIFIC

Nick Savvides

Cyber security has always been a challenging area of technology because it affects all aspects of business operation. While tools, techniques and processes changed and evolved, the core model that lasted the longest was where you built a perimeter around your data – and the people accessing it – to keep your critical information in and bad actors out.

This traditional approach has been challenged and, in today's new world of business collaboration where more employees than ever are accessing systems and data from outside an office environment, the 'castle and moat' approach is now a model of the past.

When the pandemic struck, the need for rapid systems transformation caused organisations to scramble to deploy new cloud-based technologies, open internal systems to much larger remote-user populations, and allow bring your own device where it was previously unthinkable. The result for many organisations was the implementation of new cloud technologies and security tools without a joined-up, holistic deployment or management strategy.

This is where Secure Access Service Edge (SASE) – a converged security and networking architecture model for the digital-first world – streamlines network, web, data and cloud application connectivity with security to be delivered via the cloud. SASE isn't just for the cloud; it reaches back into on-premises environments, taking security to where the applications and data reside, and equalises security outcomes by ensuring all users – regardless of their location or access method – have the same level of security and protection.

This is achieved by combining the necessary security and connectivity technologies, and making them available as a comprehensive cloud service sitting between the users and the applications – from secure web gateway, firewall as a service, cloud access security broker, data loss prevention or remote browser isolation, to zero trust network access and SD-WAN.

Furthermore, SASE provides an opportunity to easily adopt advanced new tools as they become available, such as user activity monitoring and real-time risk-based data protection without the traditional complexities.

SASE's true cloud-native approach paves the way for simplified network and security administration through a centralised management hub. This approach improves performance as users and branches connect directly to the cloud through a single converged security layer. Even for organisations that still have significant on-premises technologies, with a hybrid-enabled SASE they can cover their old and new worlds with the same protections.

As organisations further embrace the opportunities that a digital-first world offers, a fragmented approach to security simply doesn't work anymore. Businesses need an agile security architecture that can act as the foundation of digital transformation and swiftly adapt to changing business needs. The SASE model marks an age-defining leap in cyber security, which is bound to change how we view, secure and interact with data. •

For more information, visit www.forcepoint.com

Humans are the New Perimeter.

Cybersecurity solutions that safeguard human potential, creating safety and trust in a world where people are the new perimeter.

forcepoint.com

Is AI going to help cyber?

BY SCOTT BARNETT AND RAJESH VASA, APPLIED ARTIFICIAL INTELLIGENCE INSTITUTE, DEAKIN UNIVERSITY

Artificial intelligence is being used to revolutionise industries, from health care to manufacturing.

Scott Barnett

Rajesh Vasa

Industries yet to experience the artificial intelligence (AI) rush will soon, with a report by PwC predicting that the global economic impact of AI will reach US$15.7 trillion by 2030. Cyber security vendors have eagerly embraced AI in their products and services, but is AI really going to improve security?

AI is vulnerable

New technology presents both new opportunities and attack vectors for organisations, and AI is no different. Malicious actors use poison attacks and attacks on a system, while AI learns from data or input attacks and modifications to data used during system operation. The purpose of these attacks includes sabotage (render the AI useless), espionage (learn how the system works for future attacks) and fraud (fool the AI). Cyber security firms looking to leverage AI in their products must develop custom solutions without using open-source implementations as a foundation to ensure that attackers cannot reverse-engineer the algorithms used. Creating custom AI solutions presents unique challenges for companies.

AI is hard

AI is in fashion and hip – there is the promise of self-driving cars, and any day now a Siri chatbot will answer questions beyond today's weather; however, these solutions take large teams and many years to build, while overcoming many failures along the way. Simply hiring a couple of data scientists is not enough for a company to build an AI solution. An experimental friendly culture is also needed to learn how to build AI systems. Companies also generally collect as much data as they can with the idea that later they can extract insights using AI. While this is true to some extent, data is often missing, incomplete, incompatible, poorly maintained and not labelled.

Addressing these data quality issues requires supporting AI infrastructure and systems. Building AI solutions involves designing architectures using patterns and idioms that are not typically used when building run-of-the-mill software solutions. These techniques are not well understood or documented as the AI hype has only recently started. Learning these techniques requires either an experienced team who has built many of these solutions before, or a company prepared to invest in the trial-and-error approach to upskill its people.

Due to the scale and complexity of an AI solution, the risk of failure due to not understanding these techniques is a lot greater than building other software. The tools used for building AI solutions are also different from traditional software engineering tools. This requires upskilling the right people. Many of the techniques are described in research papers and do not have industry-grade implementations that can be used. To take advantage of this, companies need people who can translate sophisticated mathematical descriptions into working software, which is time-consuming and expensive to do.

Skills shortage

Building AI solutions is significantly different from building traditional technology systems, and companies are still learning the skill sets that they need. In addition to raw engineering capabilities, companies need people who can manage data pipelines and take a scientific approach to problems; have strong mathematical skills; understand the benefits of their findings to the business; are capable of designing and maintaining AI infrastructure; stay up to date with the current research; understand and apply complex techniques on the appropriate data; design and maintain data pipelines, from collection to warehousing; understand distributed and parallel systems; and are willing to experiment and communicate deep technical concepts in a clear and concise manner.

Many of these skills are scientific in nature and cannot be developed overnight; and it is not merely a case of putting senior engineers through a course, as their perspective is focused on a construction-based approach rather than on exploration and experimentation. Many of the people who have the necessary skills to perform AI work are based in a university, where they are not familiar with the pressures and demands of a commercial environment. These people often lack the necessary skills, experience or exposure to deliver industry-grade solutions. Hiring the right kind of people requires an expensive training period to build people up, which raises additional concerns.

When a specialised skilled team is assembled, new challenges arise. Managing a team of AI specialists is different from managing a traditional engineering team. These differences include ways of working together, approaches to the problems that arise, measures of productivity, and evaluation of quality output and budgeting requirements, especially if the team isn't experienced in the AI field. Scientists also have different motivations, desires and goals that need to be considered.

Operational assumptions

AI systems that are trained on historical data assume that yesterday, today and tomorrow are more or less the same. Consider a retailer that has trained a demand prediction model using data from before a pandemic; this model will perform poorly once the pandemic hits customer behaviour. Although pandemics are an extreme example, AI models struggle when the world changes, unless additional work is done to continuously learn new information – this adds to the expense and limits areas in which AI can be used.

The use of AI by attackers is also on the rise; the future with AI versus AI in the battle to defend computer systems is just around the corner; however, the implications and decisions made by AI in the cyber world have real-world consequences, which require human oversight. For instance, was shutting down that hospital sub-network an ethical decision? Cyber security vendors need to add human controls and interfaces that uncover decisions made by the AI while simultaneously providing protection against attack.

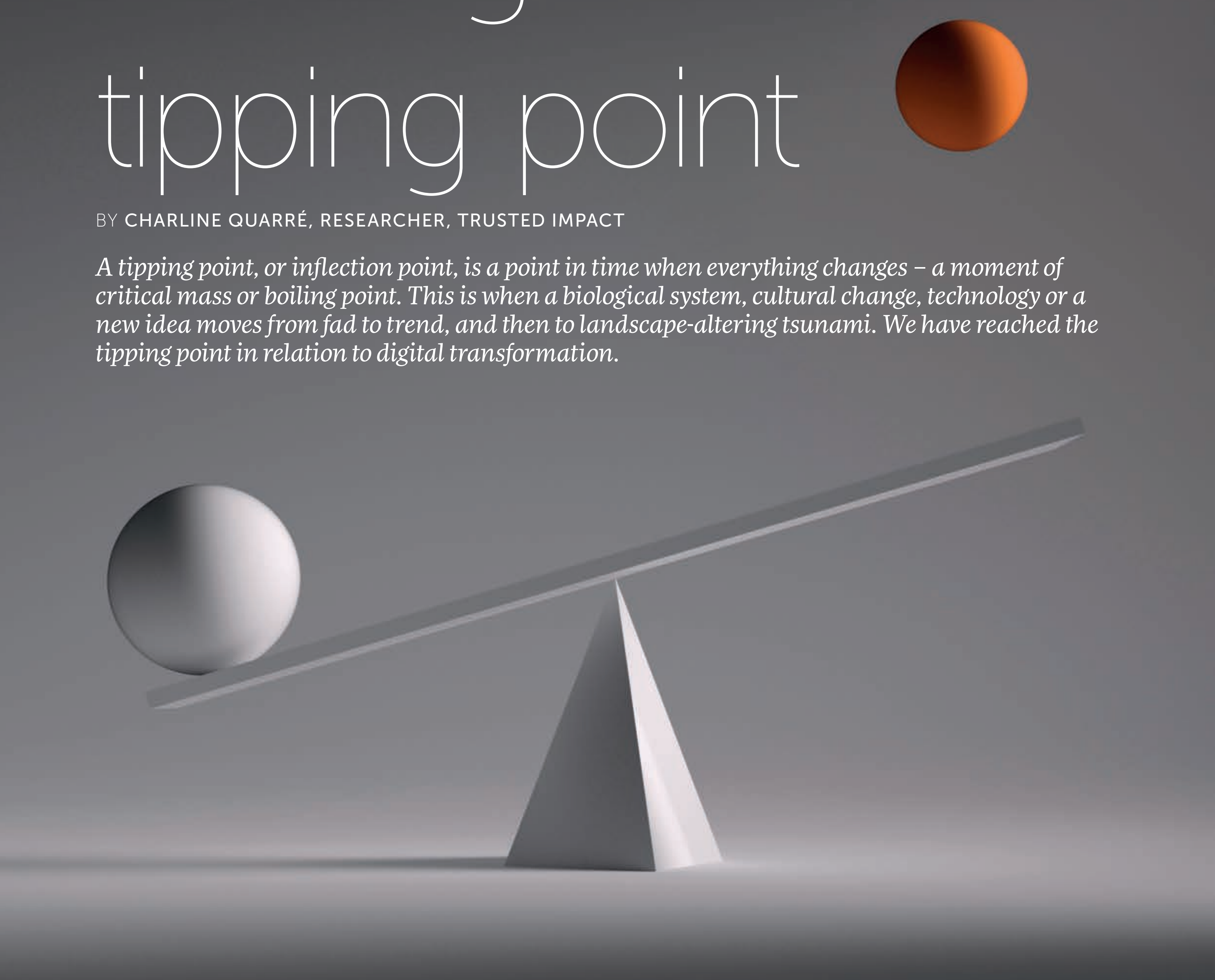
AI is coming, ready or not

The rise in AI presents new challenges for cyber security, as well as new opportunities for companies that learn to leverage this new technology. Companies seeking to leverage AI in cyber security should be wary of basing their solutions on off-the-shelf or open-source applications, as these solutions are readily available for attackers to compromise. Re-using pre-trained AI systems is also extremely risky and should be avoided; however, a new collaborative AI–human-centric world is coming, whether companies are ready or not. ●

The digital tipping point

BY CHARLINE QUARRÉ, RESEARCHER, TRUSTED IMPACT

A tipping point, or inflection point, is a point in time when everything changes – a moment of critical mass or boiling point. This is when a biological system, cultural change, technology or a new idea moves from fad to trend, and then to landscape-altering tsunami. We have reached the tipping point in relation to digital transformation.



We now live in an interconnected world where more than half of the world's population – nearly five billion global consumers – can transact wherever and whenever they want. To meet this opportunity, organisations of all types are transforming the way they engage with their stakeholders by digitally intertwining customers, citizens, employees, partners, suppliers and shareholders into a tightly woven global digital supply chain with the 'battle cries' of new markets, accelerated innovation, increased speed to market, lowered costs and improved service. And just when we thought digital transformation couldn't accelerate much faster, the global COVID-19 pandemic has been that 'landscape-altering tsunami' – there is now both the urgency and overwhelming need to engage digitally for nearly every aspect of our daily lives.

Enter the cloud

One of the cornerstones of digital transformation has been cloud computing. Cloud computing is indeed very attractive, which explains why so many organisations are eager to transfer everything they have to the cloud. Providing data access from anywhere, at any time, is one of the top reasons for cloud adoption. Disaster recovery, flexibility, cost optimisation and relieving IT staff's jobs are among the top answers, as well; however, while the shift to the cloud represents an exciting opportunity for scalability, availability and cost-optimisation, it also opens the door to new kinds of threats.

For every positive, a negative

As the digital web becomes more intertwined and complex, the threats to security also grow in both number and sophistication. The new oil of the digital machine is data – its confidentiality, integrity and availability. Well-equipped and persistent state-sponsored actors are targeting critical infrastructure and stealing intellectual property. Cyber criminals are also doing great harm, infiltrating systems from anywhere in the world, stealing money, identities and data from unsuspecting Australians.

Cloud-based assets are attractive targets because they are:

- easy to get to (with no geographical or physical distance limitations)
- easy to access (due to weak access control)
- easy to exploit (due to technical and configuration exposures and vulnerabilities)
- easy to avoid apprehension (due to cross-country jurisdictional constraints)
- easy to monetise (thus increasing motivation)
- easy to learn (limited barriers to entry, with free tools and training).

Finding Yin-Yang

As organisations 'jump to the cloud', often without even blinking, it was crucial to address security concerns for Australian organisations, and, more precisely, regarding the protection of sensitive data. As a result, the aim of our Leadership Series Paper was to have meaningful conversations with a number of Australian leaders involved with technology, cyber security and/or cloud computing to better understand what is being done in Australia to achieve the Yin-Yang[1] counterbalance of these interconnected and opposite forces.

[1] Yin-Yang 'represents the idea that nature is made up of opposing yet complementary forces and energy' (https://simple.wikipedia.org/wiki/Yin_and_yang)

Participants were chosen from a diverse range of large to small commercial and government organisations, and from various sectors, including financial services, education and health care. We also chose to base the questions broadly around the NIST Cybersecurity Framework and its five main 'functions': identify, protect, detect, respond and recover. The NIST Cybersecurity Framework is a contemporary and comprehensive set of best practices in relation to helping organisations improve their cyber security maturity. The end goal was to capture practical insight from various perspectives, to identify significant maturity gaps, and to formulate constructive recommendations regarding what could be done to help Australian organisations 'shift to the cloud' in the safest way possible.

> The NIST Cybersecurity Framework is a contemporary and comprehensive set of best practices in relation to helping organisations improve their cyber security maturity

Conclusions

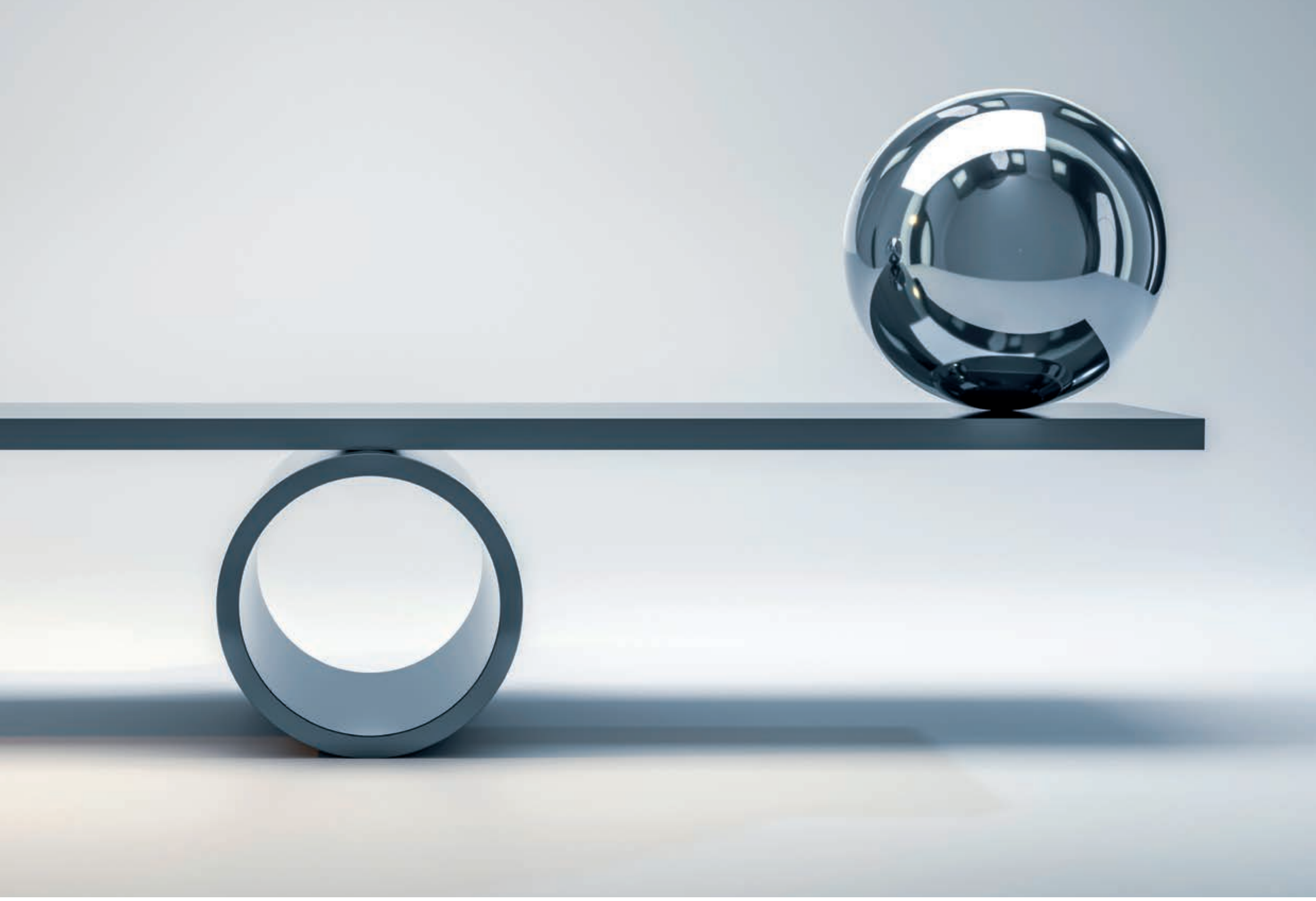
Four main conclusions were identified from the synthesis of the survey inputs and results.

1. Information security is a leadership challenge. Boards and executive suites need to 'lift their game' by adjusting and realigning their organisations' investments, priorities, policies and processes to be more reflective of the use of cloud technology and its unique risks.
2. Organisations must accelerate their security and cloud-specific risk-awareness programs to improve ineffective policy compliance so that the organisation can more sensibly adopt cloud technology.
3. It is essential that organisations go beyond the simple response of 'yes' to critical questions on essential security processes or controls and begin to seek evidence that controls not only exist, but are also effective.
4. Even when organisations know that the measures implemented by their cloud providers are effective, they should not always only rely on cloud providers' measures, especially for disaster recovery.

What to do?

As a result of our discussions, we also developed a quick checklist of our 'cloud nine' recommendations that can be used by any organisation that wishes to strengthen its cloud security posture.

1. Create an asset register and assess whether any of that information resides in cloud environments. Knowing what you have, and where, is the first step towards being able to protect it. Don't forget to also include any 'development or test' environments if they hold sensitive information.
2. Consider creating a 'cloud protection matrix'. First, rank your cloud providers in order of importance (i.e., those who hold sensitive information, or whose function is essential to your organisation) in the rows. Then, for each column, enter the five NIST functions and go through each cell in that matrix to make sure you've got them appropriately addressed.



3. Assess your high-priority cloud providers (from number two and above) and ensure that multi-factor authentication (and similar logout/lockout functionality) is enabled for all users.
4. Obtain evidence that key cloud security measures (in particular, disaster recovery) are effective/tested.
5. Review your risk registers to make sure you have clearly articulated cloud-related risks around confidentiality, integrity and availability of your systems, and the information that resides there. Make sure these risks are elevated and discussed at the board of directors' level.
6. With the insight of your asset register (step one), assess useful technology solutions (i.e., cloud access security brokers) that can manage and monitor access to these assets. Don't just have these systems generate 'logs', but define a number of 'abuse cases', and set up monitoring and alerting for triggered events.
7. Develop clear employee policies and processes around the use of cloud assets. Don't simply define the policies – actively engage staff via an ongoing and iterative education/awareness program that highlights their role in protecting the organisation's assets and use of cloud resources.
8. In our experience, one of the weakest areas of the use of sensitive information and cloud resources is at the board of directors' level – make sure policies, processes and awareness are tailored explicitly to this key audience, and ensure that they aren't storing and/or emailing sensitive information (for example, by using public email services).
9. Ensure that your Incident Response Plan reflects your ability to respond and recover cloud-based assets, and make sure the plan addresses confidentiality and integrity issues, not just availability. Most importantly, practice an incident to ensure the plan is practical. ●

Addressing security concerns

Firma FX is a global payments specialist with more than 250 employees across three continents. As a foreign exchange business, Firma FX holds sensitive customer data, customer financial data, and its own financial data all on its premises. As a result, its two major security concerns are data exfiltration and loss of the ability to process payments – the core of its business.

Challenges

Firma was planning the next steps to mature its security posture. The company had no dedicated security staff, and lacked the time and resources to gain genuine insight and visibility into the security side of its infrastructure. Initially, Firma planned to address this all in-house. It intended to procure a SIEM and hire a security manager to manage it. From there, the company wanted to build a full team. Once Firma learnt of Secureworks® Taegis™ ManagedXDR, the conversation changed completely.

> ‘For the current year, it saved us over half of what we were planning to spend on an in-house solution’
> – Mike Rue, Director of I.T. Infrastructure and Operations at Firma

Why Secureworks MDR stood out

Once the Director of I.T. Infrastructure and Operations at Firma, Mike Rue, realised that there was no need to build a team in-house, he decided to compare different solutions. Secureworks Taegis ManagedXDR stood out for one clear reason: machine intelligence was paired with human expertise.

Rue found Secureworks Taegis ManagedXDR to have a broader scope than other solutions. Two things were particularly appealing:

1. monthly threat hunts conducted by Secureworks experts
2. quarterly security-based line reviews conducted by Secureworks experts.

‘These two factors were huge in the decision,’ says Rue. ‘Other solutions didn’t have the extra human element.’ The fact that Secureworks Taegis ManagedXDR also includes an Incident Management Retainer (IMR) was a bonus. The inclusion of the IMR meant that Firma could simplify and consolidate its security portfolio.

The decision to use Secureworks Taegis ManagedXDR saved money, increased security productivity, and enabled Rue to help the rest of the organisation understand the specifics of what the security function handles. The experience for Rue has been overwhelmingly positive.

‘I have trouble finding any faults, and new features mean it’s constantly improving. It’s one of the best decisions we’ve made in a long time,’ says Rue. ●

To learn more about Secureworks Taegis ManagedXDR, visit secureworks.com

Secureworks®

The Economic Numbers You Need

Secureworks commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study. The analysis revealed that an investment in Secureworks Taegis ManagedXDR led to the following impact over a three-year period:

FORRESTER

The Total Economic Impact™ of Secureworks Taegis® ManagedXDR™

Cost Savings And Business Benefits Enabled By ManagedXDR

December 2020

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY SECUREWORKS

What Customers Say

ManagedXDR

Trusted Experts

"We wanted to maximize the budget that we have and level up the skills on my team. So, we just made a decision to take that Level 1, Level 2 SOC analysis out of the organization."

— Information Security and Compliance Leader, Retail

ManagedXDR

Superior Tools

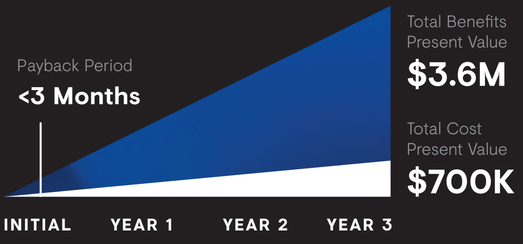
"Using [ManagedXDR], we're not doing it all ourselves, but we have a superior tool set and the ability when we need to."

— VP, Corporate and Information Security

Key Benefits*

ROI	PAYBACK
413%	<3 mo.
BENEFITS PV	NET PV
$3.6M	$2.9M

Financial Summary

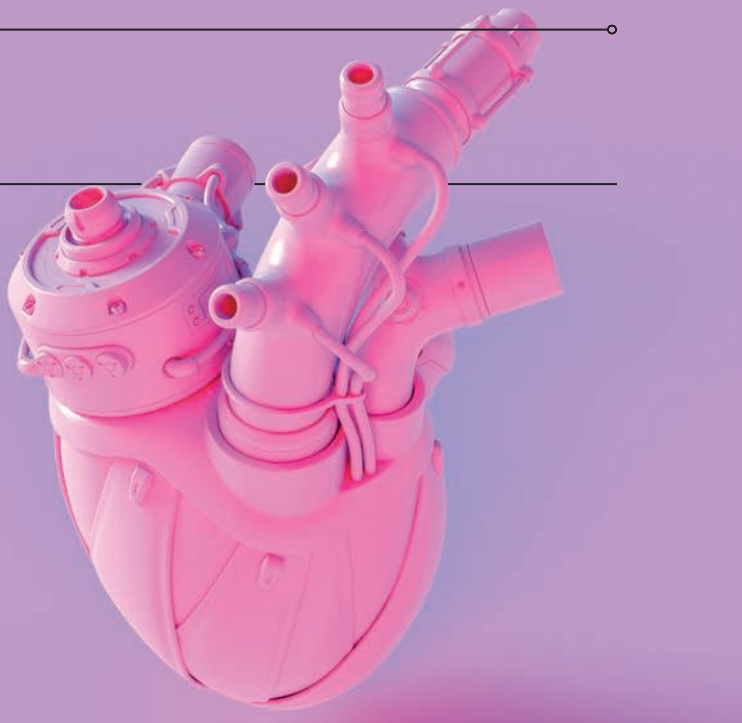


Download the Full Study

by visiting secureworks.com

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

*This advertisement is an abridged version of a full case study (Forrester Total Economic Impact of Secureworks Taegis™ ManagedXDR, December 2020). The study is commissioned by Secureworks and delivered by the Forrester Consulting group. Forrester makes no assumptions as to the potential return on investment that other organizations will receive. Forrester strongly advises that readers should use their own estimates within the framework provided in the report to determine the appropriateness of an investment in Secureworks Taegis™ ManagedXDR. Secureworks reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study. The customer names for the interviews were provided by Secureworks. Forrester does not endorse Secureworks.



The ethics of smart devices

BY PROFESSOR SENG W LOKE, SCHOOL OF INFORMATION TECHNOLOGY, DEAKIN UNIVERSITY

The challenge of achieving ethical algorithmic behaviour in connected smart things.

The Internet of Things (IoT) involves connecting things, people and places to the internet. People talking about IoT devices might be referring to smartphones, smart watches, smart TVs, smart appliances, smart cars, connected urban delivery robots, smart drones, sensors and devices with LoRaWAN, Sigfox or NB-IoT connectivity (among the many IoT networking protocols), as well as everyday objects with built-in networking capabilities.

With developments in IoT, we can expect greater cooperation among IoT devices, such as machine-to-machine collaborations. Also, as things, places and people can get connected to the internet in different ways, using a range of technologies from cameras to electronic tags, more data can be collected than ever before.

With developments in artificial intelligence (AI), we can expect increasing autonomy in smart things. Recently, there has been much thought on infusing IoT devices with AI – not just applying AI learning algorithms to IoT data, but also enabling IoT devices to make decisions and take action autonomously. Hence, there is convergence of greater connectivity with autonomy. The internet of sensors is then complemented with the internet of actuators. From IoT, one envisions the Internet of Robotic Things.

Devices trackable over the internet, however, might also be controllable via the internet, which means that they are susceptible to (remote) hacking, similar to how a computer on the internet might be hacked, but with potential cyber-physical impacts. Sensing and data collection can cause issues for the privacy-conscious (e.g., data from an internet-connected light bulb could indicate when someone is home or not) and analytics on IoT data might reveal too much.

IoT devices deployed over a long time (e.g., embedded in a building or urban furniture) might need to be upgraded over the internet with improvements, bug fixes and security patches, with consequent interruptions. An IoT device might interact and share data with another device beyond what is originally intended, or a collection of IoT devices might interact in unexpected ways not anticipated at design time. Public IoT devices – such as urban delivery robots, connected cameras and automated vehicles with cameras – might capture information beyond the original intention or be used in an unanticipated manner. Users might be burdened with the effortful set up and maintenance of IoT devices, and may be unaware of the security or privacy implications of their deployment. Users might feel a loss of control

Prominent computer scientists have noted the need for ethics in IoT, particularly in the areas of privacy rights, accountability for autonomous systems and promoting the ethical use of technologies

if they cannot stop devices from taking actions, supposedly on their behalf.

From the aforementioned, the convergence of connectivity and intelligence in IoT offers tremendous opportunity but raises a range of ethical concerns. Prominent computer scientists have noted the need for ethics in IoT, particularly in the areas of privacy rights, accountability for autonomous systems and promoting the ethical use of technologies.[1,2]

Among the ethical concerns with IoT devices and systems are the following:

— **The need for consumer IoT devices to employ adequate security measures.** Will there be a need for regulations, beyond market forces and guidelines, to 'force' manufacturers to build their devices with proper security (e.g., to include encrypted communications)?

— **Ethical data handling by IoT systems.** Will a system comprising IoT devices and their supporting cloud services manage collected and shared data in an ethical manner?

— **Right behaviour of automated behaviours (e.g., automated vehicles) in normal usage and dilemma situations.** The philosophical 'trolley problem' can be recast into a situation of whether an automated vehicle should swerve to avoid killing a pedestrian (but killing its passengers in the process) or not swerve to avoid killing the passengers (but killing the pedestrian instead). One could contrive similar situations for other devices (e.g., should a robot/device injure someone to save another person's life? Should a fire door open to let someone out, potentially also allowing the fire out?).

— **Ethical robot behaviour in public.** How should urban robots (e.g., robots doing delivery or cleaning the street) behave? Should an urban robot be polite as it goes about its business and always give way to humans? How persistent should an advertising robot be in getting a passer-by's attention?

— **Algorithmic bias could seep into AI algorithms running within IoT systems.** AI algorithms, if biased and embedded into IoT devices, might cause IoT device behaviours to be biased (e.g., a facial recognition–based door lock that fails to recognise people of a certain race more often than people of other races).

— **User choice restrictions or loss of control with automated IoT systems.**

What are possible solutions to ensure that these IoT devices behave ethically, given that they will proliferate? There have been myriad proposals, including:

— developing processes for designing and creating such ethical devices – i.e., the notion of ethical by design (similar to privacy by design or security by design)

— introducing suitable industry or government guidelines, and even legislation

— methods and tools to make it easier for developers to program ethical behaviour into devices, and to mathematically validate such behaviours

— encouraging and inculcating the right professional conduct and values in the people who make things so that ethics is a main consideration

— certifications that require a trusted party to verify that devices satisfy certain minimal standards.

The solution would likely be multi-pronged and the aforementioned is not a complete list. A variety of trade-offs might need to be navigated, such as:

— the privacy-utility trade-off – e.g., the sharing of more personal information could improve services received, but at the cost of reduced privacy

— the convenience-control trade-off – e.g., delegating tasks to a machine could be convenient, but one might lose some control.

Emerging AI ethics guidelines might be considered for smart things.[3] ●

A more extensive discussion is available at https://arxiv.org/abs/1910.10241

References:

1 Francine Berman and Vinton G. Cerf. 'Social and ethical behavior in the Internet of Things', *Communications of the ACM*, 60(2):6–7, January 2017

2 Fritz Allhoff and Adam Henschke. 'The Internet of Things: Foundational ethical issues', *Internet of Things*, 1-2:55–66, September 2018

3 Jobin, A., Ienca, M. & Vayena, E. 'The global landscape of AI ethics guidelines,'*Nature Machine Intelligence* 1, 389–399 (2019). https://doi.org/10.1038/s42256-019-0088-2

Cyber security 2021: What it means for SMEs

BY PROFESSOR MATTHEW WARREN, DIRECTOR, CENTRE FOR CYBER SECURITY RESEARCH AND INNOVATION, RMIT UNIVERSITY

The threat of cyber security attacks on governments, businesses and individuals is real, and this is something that the Australian Government recognised in its release of Australia's Cyber Security Strategy 2020.

Matthew Warren

On 6 August, Australia's Cyber Security Strategy 2020 was released, highlighting Australia's cyber security vision into the future. The strategy describes an investment of $1.67 billion over 10 years, and shows how seriously Australia is taking cyber security – some of these funding initiatives were even announced before the official launch of the strategy.

Australia's first national cyber security strategy was released in 2016, and was criticised for the lack of assistance for small and medium-sized enterprises (SMEs). The only assistance for SMEs was that they could have their cyber security tested by certified penetration testers. This is not the case with the Cyber Security Strategy 2020. One of the key aspects of the 2020 strategy was the recognition of the importance of SMEs.

The SME aspect of the 2020 strategy covered a number of different areas, and it focused on government and large businesses being able to assist SMEs to grow, and to increase their cyber security awareness and capability. This assistance will take the form of offering SMEs information, training and toolkits in relation to areas such as threat blocking, antivirus and cyber security awareness training.

The Australian Government will offer a dedicated 24/7 cyber security advice hotline for SMEs, where they can obtain advice about cyber security and how to deal with incidents. The role of the Joint Cyber Security Centres (JCSCs) will be expanded to include SMEs as part of their remit, which includes the placement of outreach officers to help SMEs. These new outreach officers will help SMEs in capital cities to improve their cyber security ability; hopefully, these roles will also cover SMEs in regional areas. There will also be a new tailored Cyber Security Business Connect and Protect Program to offer SMEs specialised cyber security advice from trusted sources (such as chambers of commerce and business associations) when it is needed to raise cyber security awareness.

The Australian Cyber Security Centre (ACSC) will also support the JCSCs by providing new materials for SMEs aimed at helping them improve their cyber security by offering a new range of focused cyber security step-by-step guides, and updated SME-focused cyber security training materials. The ACSC will also offer new online cyber security training courses specially for SMEs.

A key aim of the 2020 government approach was to help SMEs uplift their cyber

security abilities and practices through the new cyber security awareness and training programs.

But 2020 brought many changes for everyone. The COVID-19 pandemic has impacted people worldwide and provided challenges to all aspects of life, including the way we work. The economic and social disruption caused by the pandemic is devastating in terms of people being in lockdown, people losing their jobs, and organisations ceasing to trade.

Throughout the pandemic, we have seen a dramatic change in the cyber security landscape for all organisations, including SMEs. Some common cyber security issues include the following:

— Corporate data being held on employees' computers away from corporate systems, and data being held on home computers without appropriate corporate security controls or governance processes in place in order to protect the data. In many cases, we have seen that SMEs have developed ad hoc solutions and systems to deal with cyber security, and with such ad hoc solutions come major vulnerabilities.

— SMEs moving data, including sensitive customer data, into cloud storage or cloud-based system without considering the potential security risks or privacy implications.

— The change in attack vectors from threat actors focusing on individual staff members in their home environment rather than corporate systems. We have seen an increase in cyber incidents, including phishing attacks and ransomware attacks.

— Organisations trying to manage and protect corporate systems and data with employees in a remote-working environment, especially a challenge for SMEs, which may not ordinarily have patching process in places, let alone the ability to patch systems in a remote situation.

During 2020, a project was conducted by Cynch Security, Deakin University and RMIT University, funded via Austcyber. The project focused on the cyber security challenges that Australian SMEs and microbusinesses faced during 2020, including during COVID-19. In February 2021, a discussion paper of the results of the cyber security survey will be made available via Cynch Security's website (https://cynch.com.au/).

A key takeaway in light of 2020 and COVID-19 is that the Australian Government should revisit the Cyber Security Strategy 2020 and reconsider the needs of Australian SMEs in 2021. It should refocus the support and training requirements based on the new environment that Australian SMEs now find themselves in. The Cynch Security, Deakin University and RMIT University SME cyber security study would be a good starting point to identify the key cyber security requirements of SMEs in the new COVID-19 world. •

AusCERT in 2021

Celebrating its 28th anniversary by optimising and elevating its services.

As a not-for-profit information security group based at The University of Queensland, AusCERT delivers 24/7 service to its members alongside a range of comprehensive tools to strengthen their cyber security strategies.

While there are many unknowns to come in 2021, here are some key issues on the AusCERT agenda this year.

Expanding and enhancing its delivery of threat intelligence

AusCERT aims to form and publish a Cyber Threat Intelligence (CTI) strategy document to align with its members' needs. To complement this initiative, the team is looking to introduce some enhanced functionalities within the AusCERT Member Portal.

And last but not least, in tandem with the CTI strategy and existing Information Sharing and Analysis Center initiative, the team aims to launch a malware information sharing platform for all members.

Remaining a trusted incident response partner, both locally and globally

AusCERT aims to broaden its incident response capability with consistent training and drills – especially through its strong relationship with the APCERT community, as well as maintaining its standing within the worldwide CERT community through FIRST, the global Forum of Incident Response and Security Teams.

AusCERT will also continue to foster a strong relationship with the local Australian cyber security sector's key players.

Consistent and useful engagement with members

AusCERT will be celebrating the 20th anniversary of its annual cyber security conference, Australia's oldest and premier cyber security event. The AusCERT2021 conference theme will be 'SOARing with Cyber', and this annual event will once again provide members with the optimum opportunity for professional development and upskilling.

AusCERT also aims to increase the number of blog articles and publications it publishes. These will be aimed at senior to mid-level members.

AusCERT is one of Australia's only computer emergency response teams (CERTs), and is one of the oldest CERTs in the world. This legacy has given AusCERT an extensive body of cyber security research and knowledge that it shares with members and other CERTs around the world.

Its collaboration with global peers enhances its ability to identify, monitor and report on the latest threats. AusCERT has hundreds of members, ranging from private corporations to government departments, local councils, not-for-profits and small enterprises, and is especially prominent in the education sector.

Thinking of pursuing training this year?

AusCERT continues to provide its training workshop offerings to members and the wider information security community by providing the following options:

- Cyber Security Risk Management
- Incident Response Planning
- Introduction to Cyber Security for IT Professionals.

The team can offer each of these sessions either in-person (under COVID-safe restrictions) or virtually. ●

Submit an expression of interest to our team and email training@auscert.org.au for further details. The cyber security landscape is ever-changing, and AusCERT continues to be passionate about engaging its members to empower your people, capabilities and capacities.

SolarWinds a sobering wake-up call for the Australian Government

BY TIM WATTS MP, SHADOW ASSISTANT MINISTER FOR COMMUNICATIONS AND CYBER SECURITY

The SolarWinds hack has been described by WIRED as the 'biggest espionage hack on record', and according to Sergio Caltagirone, Vice President of Threat Intelligence at Dragos, the hack 'could be the biggest ever'.

Tim Watts

The SolarWinds exploit was downloaded up to 18,000 times by its corporate and government clients, allowing further compromise of networks belonging to organisations including the US Department of Homeland Security, US Treasury and Microsoft.

The more we learn of this attack, the more it seems that these targets were not merely random.

While there hasn't been any publicly released evidence suggesting that Australian Government entities were targeted with further compromise, we know that they are using SolarWinds software, and are therefore potentially vulnerable. These include the Departments of Home Affairs, Defence and Finance, and the Australian Signals Directorate.

'Making the job of a hostile state hacker extremely onerous by very strong defences is much less interesting than the idea of covert digital combat. But it can be very effective. Cyber security is fundamentally attritional. Hardening defences doesn't immunise against attack, but over the long haul it yields results'

This attack is a sobering reminder of the importance of cyber security to the effective functioning of governments, and how much more work there is to be done.

When considering how governments should respond to SolarWinds, Ciaran Martin, former Director of the UK's National Cyber Security Centre, put it best: 'Making the job of a hostile state hacker extremely onerous by very strong defences is much less interesting than the idea of covert digital combat. But it can be very effective. Cyber security is fundamentally attritional. Hardening defences doesn't immunise against attack, but over the long haul it yields results'.

But a lack of accountability means that these incremental efforts haven't been made in our public service. Last year, the Government's Commonwealth Cyber Security Posture report offered little comfort, stating that implementation of the ASD's Essential Eight 'improved [security] slightly' in Commonwealth agencies, but it 'still requires further improvement to meet the rapidly evolving cyber security threat environment'.

I recently joined with my fellow members of the government-controlled Joint Committee of Public Accounts and Audit (JCPAA) to issue an alarming report on the Australian Government's failure to ensure the cyber security of its departments.

The report calls for a new and unprecedented oversight regime after years of shockingly high rates of noncompliance from the Australian Government with its own cyber security framework.

Despite the Australian Signals Directorate's 'Top Four' mitigations being mandatory since April 2013, the most recent Auditor-General's report in 2019 found that nearly four in 10 Australian Government entities had still failed to implement these basic cyber security measures six years later.

Extraordinarily, of the 25 Commonwealth entities that were prioritised for improvement as part of the Morrison Government's 'Cyber Uplift', none were assessed by the Australian Cyber Security Centre to have achieved their recommended cyber security maturity level.

As a result, the report concluded that 'these entities are vulnerable to current cyber threats targeting the Australian Government'.

JCPAA's report indicated that a lack of accountability was to blame for the failing of implementing basic cyber security controls. In response to the SolarWinds attack, US Congressman Representative Jim Langevin, a Cyberspace Solarium Commission member, said, 'In all of the different departments and agencies, cyber security is never going to be their primary mission'.

The JCPAA report demonstrates that this has been especially true of Commonwealth departments; each individual department is responsible for its own cyber security but there are no consequences for noncompliance. Given this finding, and with Representative Langevin's words in mind, it's clear that departments can't be left to mark their own homework on cyber security.

The SolarWinds hack should be a wake-up call to the government when it comes to the reality of the threats against government networks and the information they hold.

The bipartisan final report of JCPAA's Cyber Resilience inquiry includes a series of recommendations, supported by both government and opposition committee members, of how to improve the cyber resilience of Australian Government entities in the face of these growing threats.

One of the most significant of these recommendations is Recommendation Four, an annual review by the Australian National Audit Office (ANAO) into the cyber resilience of Commonwealth entities. This recommendation addresses the frustrating lack of transparency across government that has allowed departments to hide their cyber security failings for years.

The limited assurance process would enable the ANAO to look across the entirety of the Commonwealth to identify areas of noncompliance, to find systemic problems, empower the ANAO to do deeper dives into specific entities and issues, and then report to Parliament.

This oversight and scrutiny will help to drive a culture change within the Australian Public Service, shifting the focus to enhanced cyber security through greater accountability for cyber resilience, which has previously not existed.

In December, the Morrison Government introduced legislation that would impose significant new cyber security obligations on a wide range of critical infrastructure operators. This legislation has been met with serious concern from Australian industry, citing a lack of consultation.

At a time when it is trying to impose significant new cyber security obligations on the private sector, the government must heed its own warnings and, at a minimum, hold itself to the same standards it seeks to impose on the private sector.

In an era of constantly growing cyber threats and in the wake of the SolarWinds attack, the government must begin to prioritise the national interest through its own cyber security, starting with proper transparency and accountability about the current state of the Australian Government's cyber resilience.

The best way to do this is by accepting and implementing the bipartisan JCPAA recommendations, starting with establishing a new cyber security accountability regime led by ANAO that will drive the cultural and technical changes we need to create a genuinely cyber-resilient Commonwealth. ●

Threat intelligence and collective defence

Connecting Australian businesses to protect our digital borders.

In 2020, COVID-19 saw an unprecedented rise in the use of digital technologies for everyday activities. Australian businesses of all sizes shifted to digital interactions and operations, boosting our already formidable digital economy. With increased online adoption, however, came increased cyber risk. Cybercrime and malicious actors continue to take advantage of the situation by targeting Australian organisations with phishing attacks, ransomware and supply chain compromises.

While malicious cyber actors are increasingly sophisticated and often coordinate their attacks, the majority of Australian companies are defending themselves in insolation – fighting back while trapped in silos. Cybermerc believes that there is a smarter approach to collaborate in a way that leverages our strengths to identify cyber attacks early, share actionable intelligence and disrupt malicious cyber operations. In essence, we can overcome the attackers' advantage by working together.

AUSHIELD is a digital ecosystem of cyber threat intelligence (CTI) solutions that connect Australian businesses and protect our digital borders from cyber attacks. Members of the AUSHIELD network benefit from CTI generated from data sourced through Australian participants, contributing real-time telemetry of emerging attacks, malware samples, and optionally participating in analysis and investigations. Rather than defend in isolation, participants of AUSHIELD work together to harden our digital borders by producing and sharing intelligence that is used to detect attacks early, and protect everyone. The resulting intelligence can be ingested into firewalls and security tools to alert or block emerging threats in environments without the need for dedicated security staff. Through this, Cybermerc enables small businesses to access a level of protection traditionally only accessible to enterprise and government clients.

Cybermerc is 100 per cent Australian-owned. We hold the conviction that our thriving digital economy is best protected against the scale and sophistication of cyberthreats by forging partnerships across industry, research, enterprise and government.

Our technologies and services are designed to underpin the collaborations needed to defend our digital borders. Cybermerc's CTI is Australia-specific, generated to address the increasing attacks specifically targeting Australian businesses.

We are all in this together, and Cybermerc is on a mission to prove that together we can elevate our cyber maturity and capability. At the heart of our mission are two key goals:

— Lift the cyber security capability of all Australian organisations by providing a community platform to consume, share and collaborate on Australia-specific CTI.

— Provide defence-grade cyber security detection and protection to Australian small and medium-sized enterprises at an affordable pricepoint.

We can defend our digital borders effectively by working together. In achieving our mission, we will elevate the cyber capability of organisations big and small, government and non-government. We can be secure together. Join Cybermerc today. •

Ransomware has gone from bad to worse

New attacks and bigger demands made 2020 'the worst year for every CISO'. **David Braue** *reports.*

As if the rapid shift to remote working hadn't already made 2020 hard enough for security professionals, cybercriminals' eagerness to capitalise on the disruption – and their success in targeting already scrambling firms with vicious ransomware – made it an *annus horribilis* for many.

Analysis after analysis has come to one conclusion: although 2019 was a bad year for ransomware, 2020 was even worse.

A pre-COVID survey of 5000 IT managers, conducted in early 2020 by Vanson Bourne on behalf of Sophos, clarified the baseline from which organisations were already working before the pandemic spurred the creativity of cybercriminals.

Fifty-one per cent of respondents said that they had been hit by a ransomware attack during 2019, with their precious data successfully encrypted in 73 per cent of the attacks.

Although 94 per cent of affected organisations got their data back, 26 per cent did so by paying the ransom – the remainder used other strategies, with 56 per cent simply restoring data from their backups.

Yet, no matter how widespread ransomware already was when the year began, things only got worse as the pandemic dragged on.

In June, for example, the New South Wales State Transit Authority was forced to revert eight bus operators to manual processes after a ransomware attack took down its dispatching system. Cleaning and facilities management firm Spotless was hit by ransomware in October, while cruise operator Carnival Corporation suffered a ransomware attack in August, and appliances company Fisher & Paykel was hit in June.

The list goes on and on – and, at a time when they could least afford downtime or unexpected expenses, even healthcare operators were particularly affected by ransomware during the course of the year. In fact, 46 per cent of all data breaches in the sector were caused by ransomware attacks, according to Tenable's recent 2020 Threat Landscape Retrospective.

Yet, they were far from alone. By year's end, a CrowdStrike survey found that 67 per cent of Australian organisations had suffered a ransomware attack in just the previous four months – well ahead of the global average of 57 per cent, cementing Australia as the world's second most-attacked ransomware target.

Easy access to cryptocurrencies – which provide the anonymity that helps the ransomware model to thrive – has been credited with driving a ransomware industry that surged to be worth $1.8 billion (US$1.4 billion) last year, with the average cost of the Australian attacks pegged at $1.25 million.

Yet, even that can be a low-ball figure. Media monitoring company iSentia, for one, announced in November that it had been hit by a ransomware attack that would cut its net profit by up to $8.5 million.

Many other companies keep quiet about their ransomware struggles, engaging middlemen to negotiate a payment or calling on technical experts to help them get back up and running.

The tendency of many companies to keep ransomware incidents in-house means that even the significant figures in customer surveys are likely 'under-reported', CrowdStrike Chief Technology Officer Mike Sentonas says, adding that there was so much demand for the company's incident response services during 2020 that the company was 'struggling to manage the resource requirement'.

'It's one of the reasons I say that the traditional approaches [to ransomware recovery] don't work,' he adds. 'If they worked, we wouldn't be that busy.'

Investigations often turn up patterns of infiltration that suggest that by the time the ransomware rears its head, cybercriminals may already have been listening quietly on the network for days or months

Feeling the pain

Heaped on top of the already formidable security challenges that 2020 threw at security professionals, the added burden of ransomware attacks pushed many companies – and their CISOs – to breaking point.

Kevin Mandia, CEO of cyber security firm FireEye, said during a recent Aspen Institute webinar that the year was, without a doubt, the worst year for every CISO he had seen in 27 years, 'and that was driven by ransomware'. He noted that FireEye's 500 security specialists were currently helping customers with 155 different security investigations worldwide.

Those investigations often turn up patterns of infiltration that suggest that by the time the ransomware rears its head, cybercriminals may already have been listening quietly on the network for days or months.

'It's not just about the email that you get with the link that tricks the user,' Sentonas explains. 'It's about adversaries that use stolen credentials or brute force attacks to find a way in – and then sit there preparing the environment for maximum damage. We've seen a very, very methodical, well-structured process to go through all the stages of the attack.'

Some companies had successfully increased their resistance to the initial phishing compromise by deploying strategic screening platforms – but, he adds, 'just because [successful compromise] is getting harder for criminals doesn't mean that it doesn't work. It's just getting harder'.

Making the bad even worse

Much of this groundwork is not only about locking systems until the ransomware is paid. As if it wasn't already bad enough during

2020, ransomware extortionists also ramped up 'double extortion' attacks – in which they pressure companies to pay the ransom by threatening them with having their sensitive data published online for anyone to read or buy.

Cybercriminals 'are putting pressure on organisations, and [that's] how they ask for a higher amount of money,' Sentonas says. 'If you don't pay, and you ever want to see your data again, you're basically going to have to download it from the public source where everyone else has it, as well.'

Extortionists' threats to publish or sell company data are more than empty promises: logistics giant Toll Group, for one, admitted in May that the perpetrator of a Nefilim ransomware attack 'has now published to the dark web some of the information that was stolen from the server', and that it was investigating 'the specific nature of the stolen data that has been published'.

Electronics giant Canon was also in damage control after its data was leaked online in the wake of its refusal to negotiate with a ransomware group.

Such incidents became more common in 2020. Tenable, for one, identified 18 different ransomware groups using name-and-shame attacks to pressure victims into paying their ransom demands.

More than 22 billion data records, the firm says, had been exposed in 730 publicly disclosed incidents between January and October in 2020 alone.

The fact that 259 of those breaches were attributed to ransomware – two-and-a-half times more than email compromise, the next most-common vector – confirms that malware 'remains the most disruptive global cyberthreat', Tenable Staff Research Engineer Satnam Narang says, adding that it 'reflects a new normal, and is a clear sign that the job of a cyber defender is only getting more difficult as they navigate the ever-expanding attack surface'.

All indications are that 2021 will be another bumper year for online extortionists, who are likely to have been emboldened by their success with double extortion attacks last year.

BlackBerry security researchers, for one, identified a Ransomware-as-a-Service (RaaS) offering called MountLocker that had been operating through a network of affiliates, and had quickly expanded its reach and effectiveness.

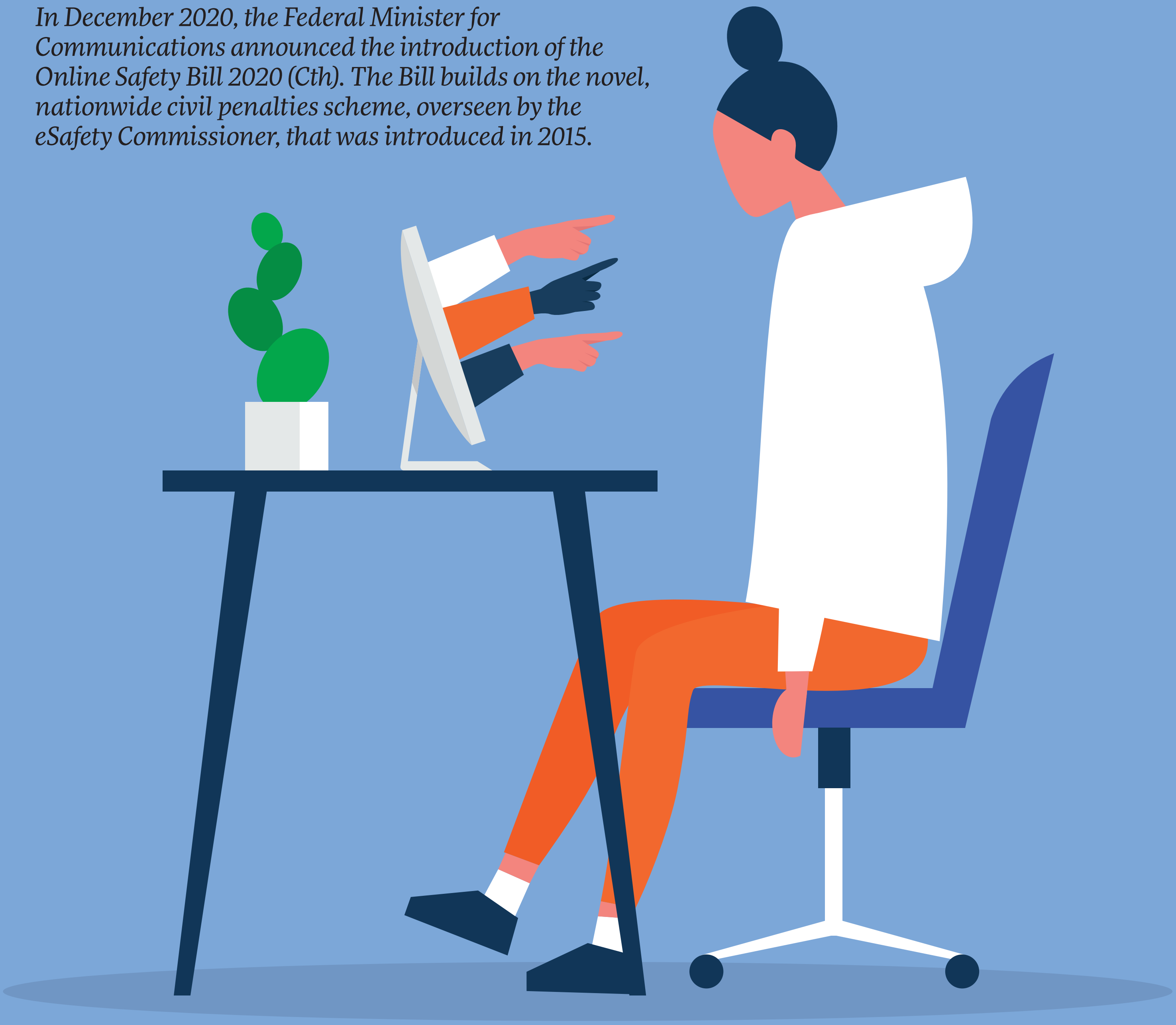
By pairing technologically devastating tools with time-tested business models, ransomware authors are continuing to expand their footprint – and the effectiveness of a threat that no CISO wants to have to deal with, but most will have to manage anyway.

'A complex threat landscape, highly motivated threat actors and readily available exploit code translate into serious cyber attacks,' Narang says. 'This threat affects virtually every industry and stems from a variety of root causes, all of which security teams must account for in their defender strategy.' ●

The Online Safety Bill 2020: Protecting adult victims of cyber abuse

BY MARILYN MCMAHON, PROFESSOR OF LAW; AND DR VICKI HUANG, DIRECTOR OF CYBER LAW STUDIES; DEAKIN UNIVERSITY

In December 2020, the Federal Minister for Communications announced the introduction of the Online Safety Bill 2020 (Cth). The Bill builds on the novel, nationwide civil penalties scheme, overseen by the eSafety Commissioner, that was introduced in 2015.



The 2015 civil penalties scheme was limited to dealing with the online safety of children and, in 2018, it was amended to regulate image-based abuse of adults and prohibited/illegal online content. If the current Online Safety Bill is passed, it will bestow the eSafety Commissioner with a new power to act upon the cyber abuse of adults. It will also consolidate the existing regulatory framework by adding instant messaging services, in-game communications, and conduits – such as search engines – to the social media services and ISPs who currently may be required to take down or block access to abusive or prohibited material.

What is the cyber abuse of adults?

Under current law, victims of online harassment, threats to cause harm, cyberstalking and similar behaviours are largely restricted to seeking redress through federal or state/territory criminal laws; however, evidentiary standards ('beyond reasonable doubt') and thresholds for liability are high, and obtaining a remedy can take a long time. The Bill proposes a simpler avenue for adult victims.

The Bill distinguishes the online abuse of children and adults; the former is referred to as 'cyberbullying', while the latter is termed 'cyber abuse'. Unsurprisingly, there is a higher threshold for cyber abuse when compared with cyberbullying.

Cyber abuse material is defined in clause 7(1) of the Bill as involving material provided on a social media service, a relevant electronic service or a designated internet service where:

(b) an ordinary reasonable person would conclude that it is likely that the material was intended to have an effect of causing serious harm to a particular Australian adult

(c) an ordinary reasonable person in the position of the Australian adult would regard the material as being, in all the circumstances, menacing, harassing or offensive.

If the Bill passes into law, adult victims of cyber abuse (as defined above) will be able to complain to the Commissioner. If a complaint is substantiated, the Commissioner has a range of powers, including ordering the service provider to remove 'seriously harmful' content within 24 hours. Civil penalties of up to $550,000 for companies and $111,000 for individuals can also be applied.

Benefits

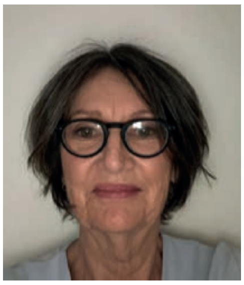
The impact of this new scheme is likely to be considerable. Although the Commissioner has not previously had the power to investigate complaints of cyber abuse involving adult victims, a reporting service existed. In the 2019–20 financial year, the Commissioner received 1064 reports of cyber abuse from adult complainants. When compared with alternatives, such as the criminal prosecution of cyber abusers, this is a noteworthy number of reports. It is, for example, significantly more than the 137 prosecutions in the same time period for the Commonwealth offence most commonly relied upon in these circumstances ('using a carriage service to menace, harass or offend'[1]).

There are many benefits of the new scheme. It offers a much faster and more accessible means of redress for adult victims of cyber abuse than current criminal remedies. It may also avoid some of the jurisdictional problems that have bedevilled criminal prosecutions. Additionally, because the scheme can require social media services, ISPs and other services to take down material, it can facilitate the removal of abusive material even when the identity of the original poster is not known – something that is not available under the criminal law.

Limitations

Although the Bill offers novel safety initiatives, limitations and concerns exist.

It appears that 'online scams, identity theft and other online security issues'[2] will not be captured by the new scheme (although they can be reported to the Commissioner).[3] Thus, romance scams or 'catfishing' (where a perpetrator creates a fake online identity, and emotionally controls and manipulates a victim without engaging in financial fraud) may fall outside the scope of 'cyber abuse' because the conduct is not overtly 'menacing', 'harassing' or 'offensive'. But the damage can be profound,


Marilyn McMahon

Vicki Huang

[1] *Criminal Code Act 1995* (Cth) s 474.17

[2] Department of Communications and the Arts (Cth), Fact Sheet—Online Safety Reform Proposals—Adult Cyber Abuse Scheme (11 December 2019) <https://www.communications.gov.au/have-your-say/consultation-online-safety-reforms>. ('DCA 2019 Discussion Paper')

[3] Ibid.

as was illustrated in the recent coronial inquest into the death of Renae Marsden, a young woman who took her own life after being the victim of protracted catfishing.[4]

There is also concern about restricting free speech. Some fear that the Commissioner may censor material that represents 'robust differences of opinion'[5] or expressions of unpopular but legitimate views. The test for what constitutes 'abusive material' is whether the 'ordinary reasonable person in the position of the Australian [victim] would regard the material as being, in all the circumstances, menacing, harassing or offensive'. This test incorporates community standards ('ordinary reasonable person'), but also allows some subjectivity ('in the position of the Australian [victim]'). It is unclear how much the personal qualities of the victim – particularly any special sensitivities and vulnerabilities – will inform the determination of what constitutes 'abusive material'.

It is also uncertain how the Bill fits into the Australian regulation of cyber space more generally. Ongoing reviews of the laws of defamation[6] and privacy[7], following closely on recent government reviews of digital platforms[8] and cyber security[9], and the release of the Safety by Design principles[10] and the Online Safety Charter[11], present a complex environment for the operation of the proposed new laws.

Conclusion

If the Online Safety Bill 2020 (Cth) becomes law, the Commissioner will have the power to deal with both cyber and image-based abuse of adults. This world-first initiative promises to offer unique safety protections and means of redress for victims. While risks relating to over-regulation and the restriction of free speech have been identified, they have been subordinated to the greater goal of protecting adult victims from these cyber harms. ●

[4] Coroners Court New South Wales, Inquiry in the Disappearance and Suspected Death of Renae Marsden (20 May 2020) <https://coroners.nsw.gov.au/coroners-court/download.html/documents/findings/2020/Marsden_findings_20_May_20.pdf>

[5] DCA 2019 Discussion Paper above n 2, 34

[6] Department of Communities and Justice (NSW) 2020, Review of Model Defamation Provisions (Web Page) <https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/review-model-defamation-provisions.aspx>

[7] Attorney-General's Department (Cth) 2020, Review of the Privacy Act 1988 (Web Page) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>

[8] Australian Competition & Consumer Commission, Digital Platforms Inquiry 2019 (Web Page) <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>

[9] Department of Home Affairs (Cth), Australia's Cyber Security Strategy 2020 (Web Page) <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/>

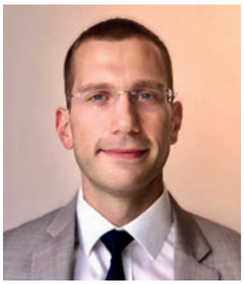
[10] eSafety Commissioner (Cth), Safety by Design 2019 (Web Page) <https://www.esafety.gov.au/about-us/safety-by-design/>

[11] Department of Infrastructure, Transport, Regional Development and Communications (Cth) 2019, Online Safety Charter (Web Page) <https://www.communications.gov.au/documents/online-safety-charter-0>

The future use case of blockchain for cyber security

BY JULIEN LEGRAND, SECURITY GOVERNANCE LEAD, NEAT

It is a challenging time for businesses that operate on digital network platforms. Cyber attacks and breaches continue to haunt online activities at even more sophisticated and damaging levels. As this nightmare continues to escalate, it is not only the small businesses that fall prey to the attacks, but also the large IT companies like Siemens, Facebook, Yahoo, Microsoft and LG, just to name a few.



Julien Legrand

Ransomware attacks and other forms of data breaches have now become a day-to-day challenge for companies. A successful cyber attack can be the downfall of any well-positioned entity. Data breaches not only cause significant financial losses, but are also the leading cause of bad reputation to victim companies.

Recent analysis and statistics indicate that even sacrosanct state procedures like elections are not safe from these attacks. This shows that cyber security is no longer an issue only for companies, but also for governments and other agencies.

For the development of viable cyber security protection strategies, it would be prudent to analyse the recent cyber attack trends and statistics. According to Juniper Research, the damages caused by cyber attacks in 2019 amounted to $2 trillion. With such tremendous financial impacts, companies continue to increase their investment in cyber security. It is estimated that by 2030, the global cyber security spending will be $2 billion in a bid to mitigate these malicious attacks. To stay well-protected, the following are some attention-catching cyber security trends and stats.

Bitcoin involved in almost $76 billion of illegal activities

Unlike other currencies, bitcoin offers a fantastic form of quick transaction with anonymity and safety. The cryptocurrency is unregulated by legacy government currency rates. This has quickly transformed it into the most preferred mode of anonymous operation in illegal activities like the cybercrime and drug trade. According to a study by the University of Sydney, bitcoin facilitated $76 billion of illegal business transactions around the world.

Ransomware attack every 14 seconds

It is estimated that an individual or company falls prey to a ransomware attack every 14 seconds. This is according to the 2019 Official Annual Cybercrime Report (ACR) that also indicated that most of these attacks go unreported. With a new person joining social media platforms every 15 seconds, the ransomware vulnerability scope continues to expand.

Small businesses are the primary targets of cyber attacks

Most small businesses consider themselves ‘unlikely’ to fall victim to cyber attacks. According to reports by Cybint, two-thirds of companies have experienced attacks such as social engineering incidents, phishing and distributed denial-of-service (DDoS) attacks in the past three years. Small businesses continue to be the smallest investors in cyber security, despite making up 13 per cent of the cybercrime market.

Cyberthreat costs

As per Security Intelligence’s 2019 Cost of a Data Breach Report, the average cost of a cyber attack data breach is $3.92 million. The cost of hacking is almost insignificant, with cyber attack tools now available on the dark web for as low as $1, with other complementary services being offered for free. It becomes more alarming that it takes an

A successful cyber attack can be the downfall of any well-positioned entity. Data breaches not only cause significant financial losses, but are also the leading cause of bad reputation to victim companies

average of five minutes to hack an Internet of Things (IoT) device.

The future of cyber attacks and malware

The current fast-paced advancement in technology allows cyber attacks to become increasingly sophisticated and executable. The rolling out of the game-changing 5G networks that offer 10 times faster download speeds will inevitably create more opportunities for hackers. Faster speeds will increase the chances of more devices being hacked and enable the execution of larger cyber attacks. There is a huge commercial appetite for IoT. Almost everything, from furniture to utility equipment, is being fitted with internet-connected sensors. According to research company Gartner, in 2021 there will be an increase in the number of IoT devices from 14 billion to 25 billion. Most of these new technologies have patchy security features that tend to attract hackers. Moreover, home automation features could lead to more homes being vulnerable to cyber attacks by criminals.

Use of blockchain for cyber security

Blockchain technology is a distributed and decentralised ledger system that can record transactions between multiple computers. Blockchain started as the technology behind bitcoin, but has popularly grown into a promising mitigation technology for cyber security.

Notably, human error remains the leading cause of data breaches. Blockchain fully automates data storage, reducing the human element in these data storage systems.

The popularity of blockchain technology

Blockchain can be utilised in any sector or industry. This is because any kind of digital asset or transaction can be inserted in the blockchain from any industry. The new technology is considered a reliable cyber security protocol due to its ability to detect foul play and provide certainty in the integrity of transactions.

Blockchain technology was designed to be transparent; therefore, blockchain does not offer any privacy or confidentiality for any transactions made through it. Its description as 'secure' simply describes the integrity of the transactions, not its privacy.

Blockchain for cyber security

Although not unbreakable, blockchain has evolved to become one of the most foolproof forms of transacting in the digital realm. As designed and intended, the technology has been credited for its information integrity assurance. If well-utilised, many sectors can benefit from it.

Blockchain has the potential to be used in many ways, including in the assurance of integrity for building cyber security. The following is a list of some future beneficial uses of blockchain to strengthen cyber security.

Securing private messaging

With the internet shrinking the world into a global village, more and more people are joining social media. New social media platforms are also on the rise, and more social media apps are being launched every day as conversational commerce gains popularity. Huge amounts of metadata are collected in the course of these interactions. Most of the social media platform users protect the services using weak, unreliable passwords.

Most messaging companies are warming up to blockchain for securing user data as a superior option to the end-to-end encryption that they currently use. Blockchain can be used to create a standard security protocol. For enabling cross-messenger communication capabilities, blockchain can be used to form a unified API framework.

In the recent past, numerous attacks have been executed against social platforms like Twitter and Facebook. These attacks resulted in data breaches, with millions of accounts being breached and user information falling into the wrong hands. Blockchain technologies, if well-implemented in these messaging systems, may prevent any future cyber attacks.

IoT security

Hackers have increasingly used edge devices, such as thermostats and routers, to gain access to overall systems. With the current interest in artificial intelligence (AI), it has become easier for hackers to access overall systems like home automation through edge devices such as 'smart' switches. In most cases, a large number of these IoT devices have sketchy security features.

In this case, blockchain can be used to secure such overall systems or devices through decentralising its administration. The approach will allow the device to make security decisions on its own. Not relying on central admin or authority makes the edge devices more secure by detecting and acting on suspicious commands from unknown networks.

Normally, hackers penetrate the central administration of a device, and automatically gain full control of the devices and systems. By decentralising such device authority systems, blockchain ensures such attacks are harder to execute (if even possible).

Securing DNS and DDoS

A DDoS attack occurs when users of a target resource, such as a network resource, server or website, are denied access to, or service from, the target resource. These attacks shut down or slow down the resource systems.

On the other hand, an intact Domain Name System (DNS) is very centralised, making it a perfect target for hackers who infiltrate the connection between the IP address and the name of a website. This attack renders a website inaccessible, cashable and even redirectable to other scam websites.

Fortunately, blockchain can be used to diminish such kinds of attacks by decentralising the DNS entries. By applying decentralised solutions, blockchain would have removed the vulnerable points exploited by hackers.

Decentralising medium storage

Business data hacks and theft are becoming a primary evident cause of concern to organisations. Most companies still use the centralised form of the storage medium. To access the entire data stored in these systems, a hacker simply exploits a single vulnerable point. Such an attack leaves sensitive and confidential data, such as business financial records, vulnerable to theft.

By using blockchain, sensitive data may be protected by ensuring a decentralised form of data storage. This mitigation method would make it harder and even impossible for hackers to penetrate data storage systems. Many storage service companies are investigating ways blockchain can protect data from hackers. Apollo Currency Team is a good example of an organisation that has already embraced the blockchain technology in their systems (the Apollo Cloud).

The provenance of computer software

Blockchain can be used to ensure the integrity of software downloads to prevent foreign intrusion. Just as the MD5 hashes are utilised, blockchain can be applied to verify activities, such as firmware updates, installers and patches, to prevent the entry of malicious software in computers. In the MD5 scenario, new software identity is compared to hashes available on the vendor websites. This method is not completely foolproof, as the hashes available on the provider's platform may already be compromised.

In the case of blockchain technology, however, the hashes are permanently recorded in the blockchain. The information recorded in the technology is not mutable or changeable, hence blockchain may be more efficient in verifying the integrity of software by comparing it to the hashes against the ones on the blockchain.

Verification of cyber-physical infrastructure

Data tampering and systems misconfiguration – together with component failure – have marred the integrity of information generated from cyber-physical systems. The capabilities of blockchain technology in information integrity and verification, however, may be utilised to authenticate the status of any cyber-physical infrastructure. Information generated on the infrastructure's components through blockchain can be more assuring to the complete chain of custody.

Protecting data transmission

Blockchain can be used in the future to prevent unauthorised access to data while in transit. By utilising the complete encryption feature of the technology, data transmission can be secured to prevent malicious actors from accessing it, be it an individual or organisation. This approach would lead to a general increase in the confidence and integrity of data transmitted through blockchain. Hackers with malicious intent tap into data amid transit to either alter it or completely delete its existence. This leaves a huge gap in inefficient communication channels, such as emails.

No matter how it is utilised, the key component of blockchain technology is its ability to decentralise. This feature removes the single target point that can be compromised

Diminish human safety adversity caused by cyber attacks

Thanks to innovative technological advancement, we have recently seen the rollout of unmanned military equipment and public transportation. These automated vehicles and weapons are possible thanks to the internet that facilitates the transfer of data from the sensors to the remote-control databases; however, hackers have been on the job to break and gain access to networks, such as Controller Area Network. When tapped into, these networks offer hackers complete control access to vital automotive functions. Such occurrences would have a direct impact on the safety of humans. But through data verification conducted on blockchain for any data that goes in and through such systems, many risks would be avoided.

Conclusion

No matter how it is utilised, the key component of blockchain technology is its ability to decentralise. This feature removes the single target point that can be compromised. As a result, it becomes utterly impossible to infiltrate systems or sites whose access control, data storage and network traffic are no longer in a single location. Therefore, blockchain may be one of the most efficient mitigation strategies for cyber threats in the coming days. Nevertheless, blockchain, just as with any other new technology, faces many startup challenges as it undergoes the painful process of growth. ●

All strategy and no execution

Amid a wealth of options, securing digital transformation requires coherent integration and orchestration.

Reports of accelerated digital transformation have become a catchcry of the COVID-19 pandemic – but as companies launch into 2021's new normal with an eye on maintaining their momentum and a mandate around secure modern enterprise IT, it's still important to make sure the walk matches the talk.

The explosion of digital working led many employees towards ad hoc adoption of solutions for secure file sharing, file transfer and data – but delivering consistency of security every step of the way has been harder than it should be for many development teams.

Many of these solutions were designed for cloud-based file sharing but lack the auditability, traceability and manageability of a mature corporate records system. That, warns Progress Software Business Development Lead Meri Kukkonen, can turn casual choices into fatal mistakes when sensitive and regulated business files and data end up in silos that cannot be monitored or controlled.

'[Many employees] are still using their own free tools or other non-encrypted methods because the company is not offering a viable alternative that's easy to use, quick and flexible,' Kukkonen explains, noting that with such platforms, 'the company has no visibility to what its employees are sharing, as there's no audit trail, there's no trace, and you get all the performance, regulatory and other problems that come with shadow IT'.

She adds, 'There's not a single organisation that isn't looking into the security aspects of all this – but without a special solution for this challenge, you can't get away from it'.

The importance of good data governance has not been lost on the Australian Prudential Regulation Authority (APRA), which suspended policy and supervision initiatives for much of 2020 but has since resumed its supervisory activities with a renewed focus on consultations around its data collections.

Cyber security is naturally a key part of protecting those collections – and, as APRA further ramps up its surveillance and enforcement activities, its focus on data is a reminder for companies in every APRA-regulated industry that consistent security policy has become a fundamental regulatory expectation.

Security is the difference

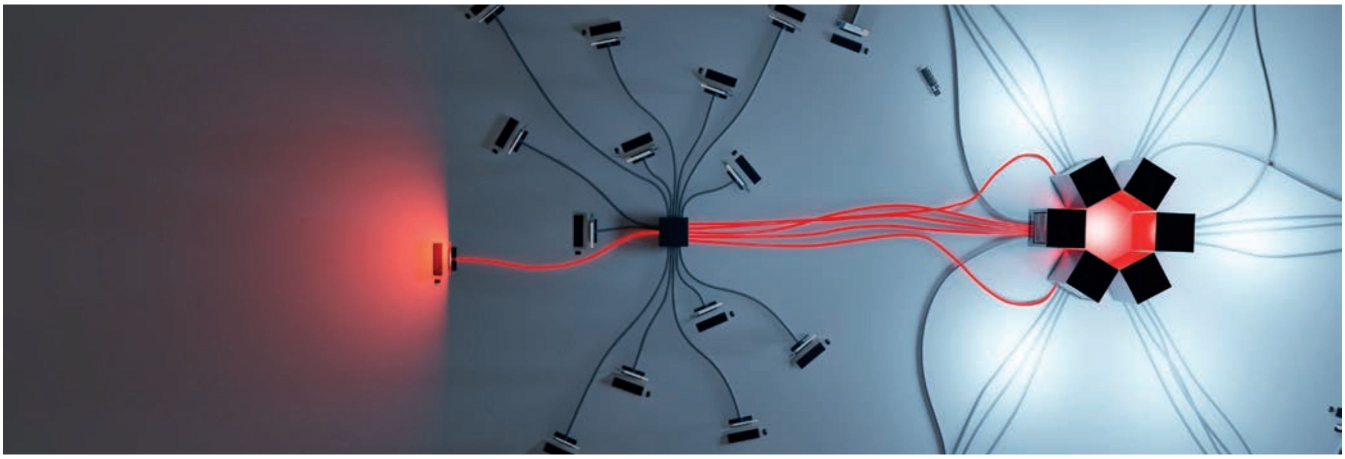
Even as employees embrace end-user file tools, companies like Progress – which has parlayed its data management nous into a cloud-native application development platform that is focused on user experiences – have been working to build secure file-exchange platforms combining enterprise-grade manageability with user-friendly design.

Progress's MOVEit, for one, borrows from decades of database expertise to provide a scalable, secure cloud-based consolidated file transfer management with full automation, auditing, traceability and high-granularity access control.

By leveraging its library of API calls, development teams can integrate MOVEit's file services deep within corporate applications in a consistent way that gives those applications a full suite of file storage and sharing capabilities.

For DevOps teams, the availability of a fully fledged file-storage system – one that meets both regulator and corporate governance requirements – offers a significant improvement over trying to keep up with the accumulation of employee-driven cloud services.

Benefits for their DevSecOps counterparts are even greater because all file-related operations can be implemented within a secure framework where access policies are continually respected and security is built in from the ground up.



'Because of the API-driven approach, you don't have to think that something only works for moving data from one source to another,' Kukkonen explains. 'It really goes across all of your corporate applications.'

Anticipating greater demand for secure data management architectures, Progress invested $283 million (US$220 million) to purchase Chef – an established development automation provider whose infrastructure, application and compliance automation capabilities dovetail with corporations' digital transformation mandate.

DevSecOps is gathering critical mass among enterprises, according to Gartner, which recently flagged market penetration between 20 and 50 per cent, and predicted that the paradigm would reach mainstream adoption in just two to five years.

'Everyone is talking about DevOps and DevSecOps, and there is a reason for that: improving and further developing a modern enterprise IT will not stop,' Kukkonen says. 'There will just be more requirements from policy creators from the business, and the pace of change will just be faster.

'If you've just met the minimum requirements this month, you're going to have to find more resources to implement even more stringent guidelines into your practices next month. Ultimately, you can't be creative [with security and governance] and get ahead.'

Taking a partner approach

Rather than just providing its tools, Progress has taken a partnership approach to ensure that its tools can integrate easily with whatever systems customers – or their employees – already have in place.

In a network of partners and customers that leans heavily towards large corporates and governments, close working relationships help clients to fully embrace the secure architecture they need.

Kukkonen and her colleagues observed this firsthand throughout the pandemic, as they were contacted by organisations pressed to transform after massive disruption throughout the year.

'Tender after tender was just cancelled, or projects [were] cancelled altogether. And our customers came to ask us, "How can you help us to meet the security guidelines?"' she explains.

Customers had different audience groups wanting to engage on new channels, but didn't have enough people to manage the phones or answer emails. On top of that, they had completely new workflows to implement.

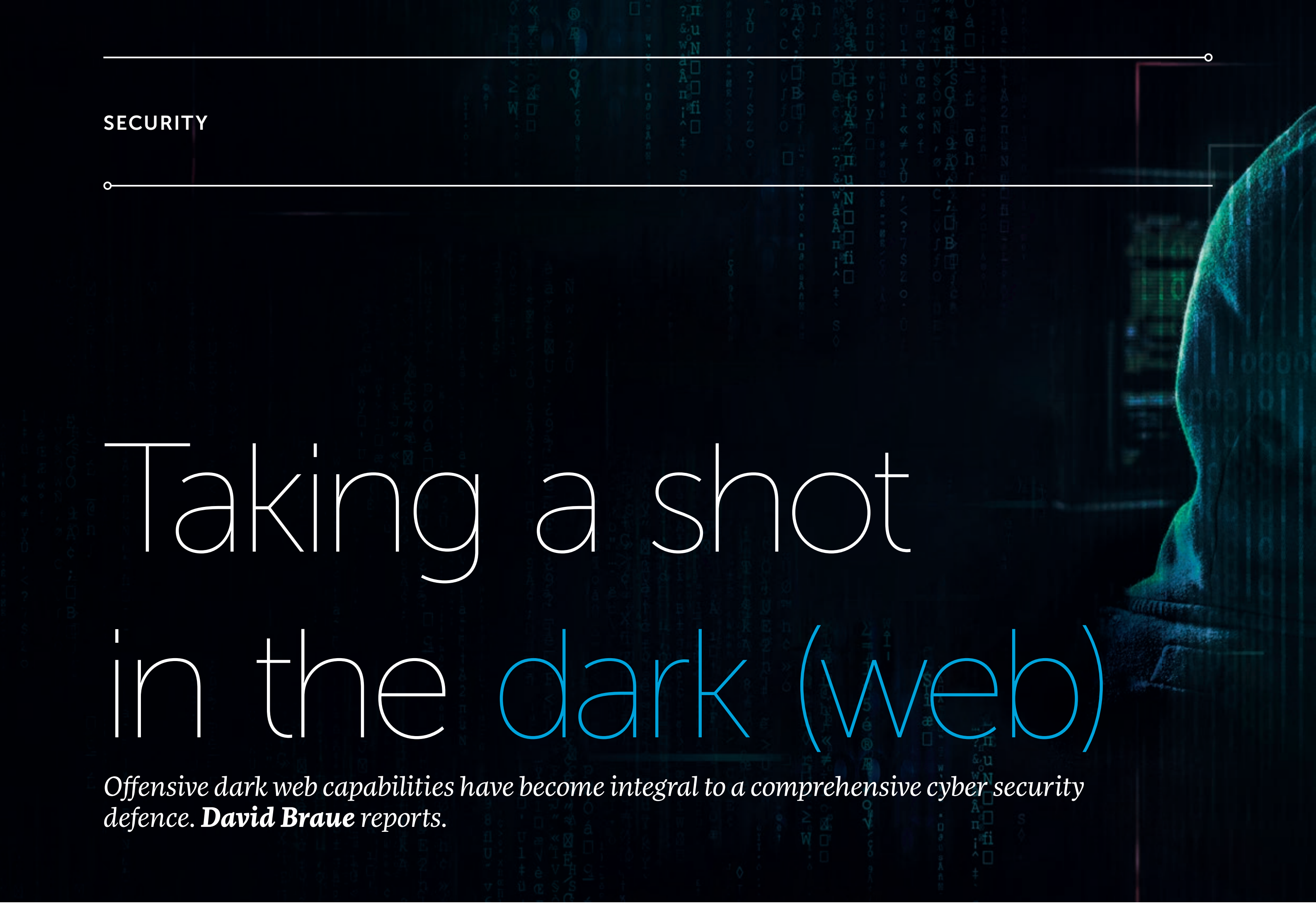
'It was a really important time for us to step in and support our community,' she says.

Out of that maelstrom of change came a concerted understanding that maintaining the integrity of corporate data and processes would require alignment of development and security processes – ensuring that security is built into everything the organisation does.

Cloud-based platforms meet this objective by providing commonly available architectures where security, visibility and other capabilities are baked into a robust, cloud-based security orchestration architecture that supports the operational security goals of DevSecOps.

'Choosing the right software is important, but nothing is secure if you don't have a cyber security strategy in place,' Kukkonen says.

'Hopefully, development leaders will take a moment to pause and consider how to build their strategy to address their organisational needs so that when the next APRA policy is released, they've got strategy with the correct scalable tools in place, and aren't just chasing their tails.' ●



Taking a shot in the dark (web)

Offensive dark web capabilities have become integral to a comprehensive cyber security defence. ***David Braue*** *reports.*

Like much of the security legislation floated by the government in recent years, the proposed Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (I&D Bill) has been mooted as a way to help the Australian Federal Police better crack down on child abuse and terrorism metastasising across the dark web.

Those powers – which include the creation of three new types of warrants allowing investigators to proactively take over suspects' online accounts 'for the purpose of gathering evidence of criminal activity' – promise a full-frontal attack on the dark web, the shadowy, anonymous and hidden anti-internet that has increasingly become the last place you'd want any of your company data to end up.

Yet, that's exactly what has happened to companies like Toll Group and Canon, whose refusal to pay exorbitant ransoms to cybercriminals led to large volumes of sensitive data being dumped into public dark web markets where they are available for purchase or download by anybody.

For profit or whimsy, cybercriminals' new infatuation with massive data dumps – last year, for example, a hacker known as ShinyHunters gave away 386 million records sourced from 18 data breaches alone – has become yet another unwelcome threat for security executives to manage.

Worse still, the dark web's very nature means that activity happens anonymously – making law enforcement efforts difficult and data recovery even harder.

'The dark web and anonymising technologies allow criminals to hide their identities and activities from law enforcement agencies,' the Department of Home Affairs explains in its discussion of the I&D Bill. 'An obstacle to investigating these crimes has been attributing criminal activity to particular individuals, organisations, premises or devices, especially on the dark web.'

The I&D Bill is currently being reviewed by the Parliamentary Joint Committee on Intelligence and Security for changes and possible ratification this calendar quarter.

The promise of stronger investigative powers, however they look once the I&D Bill has been reviewed and ultimately approved, may come as a relief for those charged with keeping corporate data safe and secure.

But they also underscore an inescapable reality: in today's cyber security climate, you must be ready to engage with dark web cybercriminals on their home turf.

A shot in the dark

Chasing cybercriminals into the depths of the anonymous dark web may sound like something best left to others – and the police will no doubt become much more adept at it once they are freed to engage more aggressively.

The growing dark web threat, particularly as data dumps become an increasingly common consequence of refusal to pay ransomware ransoms, means that any effective cyber security defence now requires some level of dark web visibility.

'It generally takes quite a while for entities to realise they are under attack,' writes Deloitte Risk Manager Adam Karl Farrugia. 'Throughout the hacking process, both clients and the targeted company are often unaware that their data has been stolen. What is left to be uncovered is what the attacker seeks to do with the stolen data.'

If cybercriminals steal and dump your user account details, after all, those credentials could open the door for other cybercriminals to simply walk onto your network and begin compromising your systems, stealing your data, or moving laterally to attack your partners and suppliers.

'In an increasingly digital operating environment, businesses will need to up their game around cyber risk,' Farrugia writes, 'especially in terms of investment in people, training and awareness, as well as infrastructure.'

> The growing dark web threat, particularly as data dumps become an increasingly common consequence of refusal to pay ransomware ransoms, means that any effective cyber security defence now requires some level of dark web visibility

Staying on top of such breaches is important, but it takes time, notes Arni Hardarson, Head of Assurance at security consulting firm Pure Security, which is one of a growing number of consultancies offering dark web monitoring services for its clients.

'You can't just roll up to the dark web and start searching for pages,' Hardarson says. 'It's not in text, so you can't really find websites unless you already know about them. And more often than not, you need to have some credibility on the dark web to get access to those forms – and this is where companies that have actually built up their threat intelligence practice become really handy.'

Last year, Pure Security joined the ranks of security consultancies sourcing intelligence gathering capabilities from DarkOwl, a US-based firm that has parlayed its dark web connections into a 'dark net database' that can be searched for keywords, such as your company name.

DarkOwl's database has also been tapped by OSINT Combine, a Sydney-based provider of open-source intelligence that will leverage the DarkOwl data to support its work training military, intelligence and law enforcement staff in information gathering.

With a growing roster of dark web intelligence companies – including IntSights, Digital Shadows, Neotas, Sixgill, Recorded Future, Kela and Sovereign Intelligence – corporations have more options than ever when it comes to monitoring dark web databases for their own data.

'By tracking the threat actor, you can understand [their] behaviour and where [they have] posted data, and whether there is going to be a second leak,' Hardarson says, citing cases where well-prepared companies 'managed to get the data down within a minute after it was exposed'.

'It can be successful, but managing it should be part of a plan to try to prevent it going out. The assumption is just that the data is going to leak – and how to manage that risk,' he says.

The new face of cybercrime

By integrating dark web intelligence into internal or third-party threat intelligence feeds, companies can meaningfully keep tabs on what MIT Sloan Cyber Security Research Scientist Keman Huang calls a 'value system' built around illegal activity.

That value system involves more than just selling or dumping data: with many dark websites hosting cyberattack-as-a-service (CAaaS) offerings that let anybody launch cyber attacks, the system creates additional economic value by selling the promise of compromising your systems and those of everyone around you.

This 'comprehensive cyber attack supply chain… enables hackers and other providers to develop and sell the products and services needed to mount attacks at scale,' Huang writes, calling CAaaS marketplaces 'a game-changing development that drastically reduces barriers and challenges in cybercrime'.

Huang adds, 'Hackers and other dark web providers don't need to perform attacks to realise benefits from their innovations, and their customers don't need to be hackers to mount attacks… Understanding how it works provides new, more effective avenues for combating attacks to companies, security service providers, and the defence community at large'.

Authorities have already chalked up wins in their fight to tame the dark web, with a high-profile take-down last year uniting Australian authorities with their peers in the United Kingdom, the United States, Germany, Denmark, Moldova and Ukraine to take down DarkMarket – the largest dark web marketplace, with nearly half a million users and 2400 sellers – and arrest 179 people.

Backed by the new investigative powers of the I&D Bill, Australian authorities will have more opportunities to repeat those successes, extending criminal investigations to even the most opaque corners of the internet.

Yet, the dark web is amorphous, continually changing in response to take-downs, and constantly reconfiguring itself in a digital cat-and-mouse game. Keeping up with those changes – no matter how you do it – is now crucial to avoid being caught flat-footed by a data leak involving your company, its employees or its customers.

'We see cybercrime evolving from a nefarious hobby into a business ecosystem and value chain with a global scope,' notes Huang.

'No wonder it is difficult, if not impossible, for the defence community to keep up.' ●

Cyber security crackdown

BY DAVID BRAUE

COVID-era attack surge pushes government towards tougher security regulations.

As a core part of Australia's financial system, the Australian Securities Exchange (ASX) has been wrestling with issues of security and business continuity since its inception – and a recent expansion of its digital infrastructure has only increased its primacy.

'Exchanges in general are very technology-centric, and most of the services that we offer are fundamentally technology,' ASX CIO Dan Chesterman explained during the recent TIBCO NOW virtual conference. 'For me, it's about making sure we have the right people, processes and capabilities in place to make sure those are being run safely all the time.'

Recent changes – such as an overhaul of its core data infrastructure, updates of core trading, clearing and settlement systems, and a secondary data centre to boost resilience – have tapped technologies such as container-based applications and a cloud-based data analytics platform to help the company reinvent itself, as well as ensuring maximum availability of its core systems.

'Our technology strategy really starts with strong foundations, and we've been investing in all of the critical capabilities and systems that allow you to be safely up all the time,' Chesterman said.

Despite their importance to Australia's financial system, organisations like the ASX have traditionally managed their

cyber security strategy outside of the direct influence and concern of government agencies whose purview, according to the *Security of Critical Infrastructure Act 2018* (SOCI), was focused on the electricity, gas, water and ports sectors.

Each faces a significant and constant flood of cyber security attacks, with US electricity operators alone blocking 'millions' of attacks last year.

This rising tide – flagged most notably by Prime Minister Scott Morrison in his June warning of attacks from a 'sophisticated state-based cyber actor' – has changed that, with the government's newly released Australian Cyber Security Strategy 2020 driving an expansion of SOCI's scope that will place data centres, financial services and telecommunications among the industry sectors considered as 'critical infrastructure'.

The reclassification comes as infrastructure operators deal with a growing cyber security threat that was, despite a widely reported COVID-era attack surge, problematic even before the pandemic.

One 2019 Siemens and Ponemon Institute survey of 1726 utility providers, for example, found that 56 per cent had had at least one shutdown or operational loss per year.

A quarter of those respondents said that they had been impacted by 'mega attacks' – often with the support of nation-state actors, as in the 2015 take-down of three Ukrainian power companies – and 54 per cent expected an attack on critical infrastructure during 2020.

Yet, just 42 per cent rated their cyber-readiness as 'high' – and just 31 per cent said that they were ready to respond to, or contain, a cyber security breach.

COVID sharpens utilities' risk focus

Amid a widespread surge in cybercriminal attacks during the COVID-19 pandemic, the dangers of utilities' unpreparedness were compounded in 2020 by accelerated organisational change that has exacerbated infrastructure operators' cyber security exposure.

'We've seen cyber security projects brought forward that we may never have seen [otherwise],' Alastair MacGibbon, Chief Strategy Officer with cyber security consultancy CyberCX, said during a Cyber Week 2020 session on infrastructure resilience.

'As the criminals have taken advantage of this stretched line of communication and the different ways that we're doing business, it has actually raised cyber security in the minds of those who run systems,' he added.

'And while it's certainly been advantageous for both nation-state and criminal actors that we have shifted the way we do our business, it has actually brought to the fore this concept of cyber risk.'

Awareness of the broader scope of today's cyber risk has become essential as utility providers' systems 'become increasingly connected through sensors and networks, and, due to their dispersed nature, are even more difficult to control,' GlobalData Senior Power Analyst Sneha Susan Elias noted in a recent analysis of pandemic-era cyber security threats.

'Increasingly interconnected, smart and decentralised' utility systems – further complicated by the growing integration of localised 'microgrids' – had made conventional centralised approaches to security 'increasingly untenable', Elias says, noting a consequent 'rising burden on edge elements and local systems to be resilient to cyber attacks, while also having the flexibility to support the resilience of the wider energy system in case of a cyber attack on the electricity grid'.

Localised support from artificial intelligence and behavioural analytics systems would help providers of all types of infrastructure – with a recent EY analysis warning that Australian water utilities 'face an urgent need to strengthen their cyber security strategies'.

Infrastructure providers can walk through six key steps to bolster their security, EY advises, including understanding 'must do' legal, regulatory and compliance actions; identifying critical assets; assessing key risks and threats; filling control gaps, such as Australia's lack of industrial control system (ICS) security standards; and developing an optimised cyber security target operating model to drive their future state road map.

Laying down the law

The federal government's formal recognition of infrastructure operators' cyber security exposure will this year push for more consistency in infrastructure cyber security, as new legislation classifies data centres and telecommunications services as 'critical infrastructure' for the first time.

Coming as part of the government's Protecting Critical Infrastructure and Systems of National Significance (PCISNS) reforms, the new guidelines are encapsulated in the Security Legislation Amendment (Critical Infrastructure) Bill 2020 – which expands the scope of critical infrastructure to include the communications, financial services and markets, data storage or processing, healthcare and medical, and other sectors.

Declared entities in these sectors will be subject to stricter cyber security reporting obligations and protections, including cyber incident reporting and risk management plans; access to government assistance to help them respond to cyber attacks on critical infrastructure; and enhanced cyber security obligations – including incident response plans, cyber security exercises, vulnerability assessments, and access to system information – for systems of national significance.

Particulars of the obligations under the expanded framework are being worked out through industry consultation this year, but with 129 submissions received during the consultation period, it's clear that the legislation has struck a chord.

CyberCX, for one, supports the reform plan and the push for 'more interventionist government action', noting that current legislation means the government 'does not have near real-time powers to compel [reasonable action or inaction], and system owners and operators can largely ignore requests from government'.

Critical infrastructure operators and their suppliers should be obligated to adopt controls, threat intelligence techniques and situational awareness capabilities to protect their assets in a 'continuous state of cyber resilience', the Active Cyber Defence Alliance notes, arguing that 'a set-and-forget approach to cyber defence, where inspection of the system is undertaken only during its introduction, is not sustainable'.

Availability of more prescriptive powers has never been more important, with cyber security consultants working at capacity, and law enforcement bodies working hard to investigate and disrupt cybercriminal enterprises.

INTERPOL notes that the pandemic has driven 'a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure', with disruptive malware – notably ransomware and distributed denial-of-service (DDoS) attacks, which surged fivefold last July and August – observed frequently, and often targeted against organisations critical to the COVID-19 response.

INTERPOL recommended that countries should build national cybercrime strategies 'to build resilience of national infrastructure and services, which can help countries counter cyber threats effectively and protect communities from data breaches during the global crisis and beyond'.

> INTERPOL recommended that countries should build national cybercrime strategies 'to build resilience of national infrastructure and services, which can help countries counter cyber threats effectively...'

Australia's efforts to expand its critical infrastructure protections represent a significant step towards these goals, with MacGibbon welcoming the 'much more muscular' Australian Cyber Security Strategy 2020 – and noting that because 'directors and officers will have to know what's happening with their supply chains, it will lead us to being a more resilient cyber nation'. ●

Leveraging neurodiverse cyber security talent

BY MARILIA WYATT, CYBER RISK ANALYST, WSJ PRO

FEATURE CONTRIBUTORS: ROB SLOAN, RESEARCH DIRECTOR, WSJ PRO; AND MICHAEL FIELDHOUSE, ADVISOR, WSJ PRO

The cyber security skills and workforce gap is driving companies to consider a different approach to the way that they recruit and develop talent: tapping neurodiverse people through programs they have established.

There are an estimated half a million unfilled cyber security positions in the United States alone, according to trade organisation (ISC)^2.[1]

Neurodiversity programs aim to recognise the variation within neurocognitive functioning and harness neurodiverse talent (people with neurological differences), particularly those on the autism spectrum – a group hitherto largely overlooked, neurodiversity experts say.

The aptitudes some neurodiverse workers possess – such as excellent pattern recognition, visual perception, creativity, hyperfocus and attention to detail – make them highly suited to some cyber security roles, according to companies that have hired them.

To leverage talent, firms will need to consider some adjustments to create an environment in which neurodiverse people can contribute to the organisation's mission. For firms willing to invest in developing new cyber talent rather than competing for a relatively small pool of established professionals, a neurodiversity program can be worthy of consideration.

Underemployed or unemployed?[2]

In 2013, neurodiversity took off in terms of talent acquisition. German business software maker SAP SE launched its Autism at Work program, followed by Microsoft Corporation, Ernst & Young, JPMorgan Chase & Co., and, in Australia, DXC Technology. Firms generally recognised that neurodiverse individuals have certain skill sets, yet remained under-utilised.

500,000
Cybersecurity Skills Gap

85%
of adults with autism are unemployed or underemployed

NEARLY HALF
of 25 year olds with autism have never held a paying job

38%
of security professionals think neurodiversity will strengthen cyber defences

44%
of neurodiverse individuals with average or above average IQ scores

Leveraging neurological differences to build cyber talent

In Australia, the strategy at IT services firm DXC Technology is to harness the whole community to find the best talent.

[1] The 2019 (ISC)^2 Cybersecurity Workforce Study

[2] Note: data from (ICS)^2, Drexel University, Autism Speaks, and a 2020 Bitdefender survey

Michael Fieldhouse, head of DXC's Social Impact Practice, says '[The neurodiverse hires] bring innovation and a different perspective to problems'.[3]

Neurodiverse workers not only include individuals with autism, but those with attention deficit hyperactivity disorder (ADHD), dyslexia and Tourette syndrome, Fieldhouse says in reference to DXC's Dandelion Program. For example, some of his current cyber teams are roughly 20 per cent neurodiverse, comprising workers with autism, ADHD and dyslexia, he says.

Since 2014, DXC's Dandelion Program has provided career and life skills training – as well as a job – to more than 120 neurodiverse people, around half of whom work in cyber security.

Fieldhouse says that their roles include fraud analysis, malware reverse engineering and threat intelligence, while attention to detail and pattern recognition are skills the neurodiverse workers provide in a data-rich cyber environment.

Caroline Wong, Chief Strategy Officer at Cobalt.io, a penetration-testing-as-a-service company, says one neurodiverse person on her team provides skills she cannot find elsewhere. For example, she can learn very technical topics quickly and apply her hyperfocus to any task. The full-time employee was up to speed in penetration testing in 12 months. This typically takes other individuals two to five years to accomplish, Wong says, adding that the neurodiverse worker also writes primary research on technical topics, and collaborates with security and IT teams on activities, such as vulnerability management.[4]

Wong adds that neurodiverse workers with attention deficit disorders are potentially suited for roles that require a quick, detailed response, like security operations centre analyst activities and those requiring a dive into cyber security datasets to extract insights, such as a data scientist.

Workplace adjustments

Firms will need to consider updates to existing processes for employee recruitment, management and retention, which may not be suited for neurodiverse talent. Making the following adjustments will be key to maximising return on investment and adopting an inclusive approach.

- **Recruitment and assessment:** Update job descriptions – i.e., 'must be good team players' – to ensure neurodiverse talent can relate to roles. Adapt recruitment communication style so that the process isn't overly reliant on interviews, psychometric testing or candidates' résumés alone. Allow them enough time to show their strengths.
- **Onboarding and integration:** Create norms around a safe environment where workers can be themselves. Some might have social, executive functioning and communication challenges or exhibit certain behaviours

[3] Emailed response to WSJ Pro Cybersecurity

[4] Emailed response to WSJ Pro Cybersecurity

– including talking to themselves. Train managers and co-workers on how to communicate with empathy and work respectfully. Managers will require special training for a broader awareness of neurodiversity issues and how to coach employees, including on social interactions and office culture, of which younger neurodiverse workers might have had little or no experience.

- **Adjustments:** Chief information security officers, managers and co-workers must consider understanding the environment needed for individuals to perform at an optimal level. This can include how workers deal with noise, communication, social experiences and even decor. Provision of equipment, such as noise-cancelling headsets, to make the office environment more comfortable should be considered, especially in open offices.
- **Retention:** Incorporate mental wellness resources into the program due to the reported prevalence of mental health challenges and higher suicide risk among individuals on the spectrum.[5] Some workers might also need life-skills training. Embed support systems – including mentorship and career progression opportunities – as well as a pipeline of suitable work.

Developing partnerships

To recruit talent, the Mitre Corporation – a federally funded, not-for-profit organisation – leverages university programs to recruit cyber-proficient neurodiverse students. In September 2019, it started its Autism at Work program, Portal Project, as a pilot. Among those who assisted them was the Autism @ Work Employer Roundtable, which includes firms that have been running their own initiatives.

John Wilson, Mitre's Chief Information and Security Officer, says that the neurodiverse interns are fast learners who have come up with innovative ideas to solve problems while working on projects for their government sponsors.[6] They work in tandem with cyber security engineers on tasks such as conducting research on monitoring software, Wilson says. 'One student found surprising software bugs that were later patched.'

Setting up a pilot program to better understand how to prepare the organisation for a broader neurodiversity program helps to identify the necessary adjustments, while also highlighting the potential benefits. Once established, a program can take a steady stream of new recruits, and the process should be smoother each successive time.

Case study: National Australia Bank

In February 2019, National Australia Bank (NAB) recruited six trainees with autism into its Neurodiversity at NAB program, working in Identity and Access Management at NAB Enterprise Security, which comprises roughly 450 employees. Four of the six trainees moved to full-time employment, says Nick McKenzie, NAB's Chief Security Officer.[7]

The trainees did the same tasks as non-program participants, but showed a 26 per cent productivity increase compared to the team's average number of requests in the Identity and Access Management function in the first two months. 'They are exceptional in that space, with acute attention to detail,' McKenzie says.

During the recruitment phase, NAB assessed the candidate's performance over several weeks, and sought to understand their autism to ensure that they were placed in suitable roles and given the right tasks. The ones selected had the aptitude to learn the required role-based skills, and all were able to identify anomalies and patterns. NAB says it plans to hire more neurodiverse staff in 2021.

> 'Our program has measured about 20 per cent to 30 per cent improved productivity between neurodiverse workers in roles managing security incidents'
>
> *– Michael Fieldhouse, Head of DXC's Social Impact Practice*

Filling the gap?

None of the neurodiversity experts interviewed for this paper felt able to estimate the numbers of cyber jobs that could be filled by neurodiverse candidates. 'Calculating exact numbers is impossible,' says Mike Spain, Chief Executive and Founder of NeuroCyber, a not-for-profit

[5] The Dandelion Program

[6] Emailed response to WSJ Pro Cybersecurity

[7] Emailed response to WSJ Pro Cybersecurity

Appendix: neurodiversity resources

Resources to help firms navigate neurodiversity questions and build programs.

- The DXC Dandelion Program Resources *https://digitalcommons.ilr.cornell.edu/dandelionprogram/*
- The Autism @ Work Playbook *https://disabilityin.org/wp-content/uploads/2019/07/Autism_At_Work_Playbook_Final_021 12019.pdf*
- The Neurodiversity Hub: Employer Resources *https://www.neurodiversityhub.org/resources-for-employers*
- Neurodiversity at Work: A guide for HR professionals and others *https://www.cipd.co.uk/Images/neurodiversity-at-work_2018_tcm18-37852.pdf*
- People With Autism Are Hot Hires for AI Jobs *https://www.wsj.com/articles/people-with-autism-are-hot-hires-for-ai-jobs-11564651804*
- Neurodiversity. How Senses Are Engaged in the Built Environment is a Large Part of Why and How We Design *https://theworkingbrain.net/wp-content/uploads/2020/01/Sensory-Processing-and-Design_LR.pdf*

based in the United Kingdom. Spain adds that doing so would be ‘attempting to answer the wrong question. Everyone is different’.

He continues, ‘One should not simply go out and recruit a large number of neurodiverse individuals to fill one’s quota without having the right understanding, knowledge, culture and ethos’.[8]

Although there is a potentially large neurodiverse talent pool, it’s not clear how many of those people are suited to cyber security or want to work in the field.

On the employer side, Fieldhouse says, ‘People find diversity and inclusion hard to commit to’. He also points out that many of those already working in cyber security may be neurodiverse, but not labelled as such, given that the nature of cyber jobs may attract people with such cognitive abilities. So, although few neurodiversity programs employ a relatively small number of people, the number of neurodiverse employees in security may already be significant.

Moving forward

A company’s long-term competitive edge requires innovation and unconventional thinking, particularly when there is a dearth of available talent. Recruiting and managing neurodiverse talent to enhance cyber strategy presents potential challenges, but also opportunities.

While the impetus behind a neurodiversity program can come from the chief diversity and inclusion officer or the HR team, support from security and IT leadership will be necessary to include the recruits in technical work. Programs aimed at bringing neurodiverse talent directly into the cyber team benefit from the CISO – or equivalent – being the driving force. Considerations for companies thinking about a neurodiversity talent program include the following.

- Identify an executive-level project sponsor, such as the CISO or chief diversity and inclusion officer.
- Seek guidance from organisations – such as DXC’s Dandelion Program or Autism @ Work – to establish a pilot program with clear requirements.
- Use publicly available resources from neurodiversity support organisations to create or adapt a suitable recruitment process.
- Understand potential adjustments to the office environment with consideration to accessibility and ongoing integration of new hires. Expect to engage workers on what adjustments they might need.
- Set out how managers and co-workers can best engage with the new hires. Procure external training expertise for managers before a program starts and to act as coaches on an ongoing basis.
- Assess mental wellness resources to see if they will adequately support the program. A manager will also need to carefully direct a neurodiverse worker’s intense concentration appropriately to proactively prevent burnout. ●

This article is an edited version of the white paper that first ran in The Wall Street Journal.

About the author

Marilia Wyatt *is a cyber risk analyst at* The Wall Street Journal*’s professional arm, WSJ Pro. Wyatt writes research and analysis, develops strategy, and creates solutions to augment executive decision-making around improving cyber security, data privacy, ethics and responsible use. Submit research ideas or feedback to marilia.wyatt@wsj.com*

[8] Emailed response to WSJ Pro Cybersecurity

Understanding CREST

The Council of Registered Ethical Security Testers is a not-for-profit accreditation and certification body that represents and supports the technical information security market. It was set up in 2006 in response to the clear need for more regulated professional services, and is now recognised globally as the cyber assurance body for the technical information security industry.

Dan Maslin

Chathura Abeydeera

Chief Information Security Officer and AISA Executive Advisory Board Member Dan Maslin chats with the Council of Registered Ethical Security Testers (CREST) Australasia Advisory Board Member (and KPMG Associate Director – Cyber Security) Chathura Abeydeera about the organisation, and what it's been up to in recent times.

Dan Maslin (DM): Welcome, Chat. Tell me a bit about CREST.

Chathura Abeydeera (CA): CREST is a global not-for-profit body that brings consistency in the global cyber security industry through an internationally recognised certification and accreditation scheme. CREST helps organisations/buying communities to identify cyber security service providers with highly skilled and qualified individuals in various technical cyber security domains. CREST provides internationally recognised accreditations for organisations and world-class certifications for individuals providing penetration testing, cyber incident response, threat intelligence and security operations centre services.

> CREST is a global not-for-profit body that brings consistency in the global cyber security industry through an internationally recognised certification and accreditation scheme

DM: What are some of the certifications/ accreditations that CREST offers?

CA: CREST qualifications are seen as being a mark of excellence, and individuals holding CREST qualifications are very much in demand. CREST provides a structured entry point for those who wish to get into the industry, as well as a structured career path for progression within the industry. CREST offers a number of certifications to individuals and accreditations to cyber security service providers. Primarily, there are three levels of certifications offered to the individuals: Practitioner, Registered and Certified. 'Certified level' sets the benchmark for senior professionals, and these are the certifications to which most aspire.

DM: What services or skills do these certifications cover?

CA: CREST certifications cover a variety of skills, such as penetration testing, threat intelligence and incident response. Each segment has specialised streams to cover individuals' expertise on infrastructure penetration testing, application penetration testing, malware reversing and simulated attacks (red teaming) domains. CREST Certified Infrastructure Tester, CREST Simulated Attack Specialist and CREST Certified Simulated Attack Manager are a few highly recognised certification offerings.

DM: What are the career paths on offer to individuals?

CA: CREST provides a well-recognised and rewarding career path, from entry into the industry, through to experienced senior professional level. The Penetration Testing career path is widely known in the Australian market. CREST Registered Penetration Tester and CREST Certified Tester certifications are highly recognised within the technical security testing market. We also have three more paths within Simulated Target Attack and Response/CBEST, Incident Response and Security Architecture domains. CBEST is one of the dominant certifications in the UK market, and CREST developed this particular certification working together with the Bank of England.

DM: What do these accreditations offer to individuals?

CA: CREST certifications are recognised by the cyber security professional services industry, regulators and governments as being one of the best indications of technical knowledge, skill and competence. These certifications enable individuals to unlock employment opportunities.

DM: What does CREST do for the buying community?

CA: CREST provides the confidence that penetration testing, threat intelligence and cyber incident response services will be carried out by qualified individuals with up-to-date knowledge, skills and competence, supported by a professional services company with appropriate data-handling processes, quality assurance policies and technical methodologies. CREST helps buyers to distinguish service providers from one another based on their skills and competencies.

DM: What type of presence does CREST have in Australia and globally?

CA: Other than our official chapter in Australia, CREST has a presence across North America, South-East Asia and Africa, as well as in the United Kingdom. CREST has a global viewpoint, and our strategy has been to arm the global cyber security industry with the skills, knowledge and competency to address what is truly an international threat. CREST currently offers penetration testing stream certifications exams, such as CREST Registered Penetration Tester and CREST Certified Tester, in Australia. We are looking to expand the onshore exam portfolio in the coming years.

DM: Personally, I have seen a boom in penetration testing in recent years – it seems that many technology companies have penetration testing offerings, and there are plenty of independent contractors offering their services, too. What should organisations look for in providers to have a level of comfort that they are engaging the right skills and experience?

CA: Organisations should look for a cyber security partner who can keep up with leading-edge tech and industry-better practices, and can employ skilful and qualified people to help their clients. CREST has built a robust standardised global framework for governments, regulators and buyers to identify capable suppliers that can deliver technical cyber security services in a competent and safe manner. CREST member companies have the appropriate standards and qualified people to meet technical security testing requirements within the industry. We feel it is important that cyber security service buyers obtain those services from an official member of the CREST Approved scheme (listed on the Accredited Companies section at www.crest-approved.org).

DM: Aside from accreditations, what types of (free) resources are available from CREST?

CA: Good question, Dan – this is something not widely known. Other than providing access to trusted service organisations utilising highly skilled, knowledgeable and competent individuals, we provide procurement support and industry benchmarks. We have a number of implementation guides and Cyber Maturity Assessment Tools available under the knowledge-sharing section of the CREST website (www.crest-approved.org).
We also have specific focus groups for members to share their war stories and offer the opportunity for them to benefit from purposeful networking opportunities.

DM: What is the role of an Advisory Board Member like yourself?

CA: The CREST Australia Advisory Board is a mix of like-minded, skilled individuals in the Australian cyber security industry, and we are working on raising industry awareness of CREST. Members of the Advisory Board provide CREST with strategic advice and guidance – on the Australian market, in particular. We are also talking with the government to tailor frameworks, such as intelligence-led penetration testing, to protect Australia's critical infrastructure.

DM: Where can readers find out more?

CA: CREST's international website (www.crest-approved.org) is a great place to start. ●

The value of cyber security certifications

The pressure is on for organisations to attract and retain the right people with the right skills and hands-on experience to best protect them from the latest threats. For individuals, that means giving current and prospective employers reassurance that they can do the job to the highest standard. For organisations, that means offering positions – both new and more – to people who can maintain and improve security. Research – like Fortinet's cyber security skills survey* – has shown that certifications add significant, career-impacting value for both practitioners and employers. There are a number of reasons to certify.

Job security

Fortinet's research revealed that 82 per cent of cyber security organisations prefer to hire candidates with certifications. If you're hoping to find a new role, that means acquiring the right certifications could be what gets your foot in the door at almost any enterprise.

Not only do certifications help you get the job, but they also play an important role in helping you to keep the job and to continue progressing in your career. More than half of the survey's respondents believe that their certifications helped them perform their duties more effectively and with confidence, and many also attribute them to faster career growth.

Enterprise security

Keeping organisations secure is critical, especially in today's threat environment. We know that bad actors don't decrease their efforts during a pandemic – in fact, they've increased. Certifications provide confirmation of the skills needed to combat breaches and mitigate threats to the enterprise. Research shows that 94 per cent of cyber security practitioners believe that their certifications better prepared them for their current role, allowing them to successfully protect their organisation.

Proven abilities

Anyone can claim that they have a certain ability or skill. But the only way to back up those assertions is to demonstrate with proof. Certifications are that verification of skill– especially in InfoSec. If they prove you've mastered a specific skill set, both employers and your industry peers know that you have what it takes. Hands-on practical testing like GIAC's CyberLive takes this skill verification a step further. Practical testing in a virtual lab environment and executing tasks found in specific job roles confirms that you could walk into a new position and get right to work on day one.

Personal validation

Obtaining certifications helps overcome imposter syndrome by showing that you have what it takes. Setting goals to learn new skills and pass a certification exam can be a challenging and rewarding internal experience. Proving to yourself that you can master skills and conquer the exam creates a sense of purpose and personal satisfaction.

The Fortinet survey reveals that there is still a significant skills gap in cyber security today. Take advantage of this moment and do your part to improve the security of our world by getting certified. •

**https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-fortinet-survey-skills-shortage.pdf*

To learn more about GIAC certifications and SANS training courses in the Australia–New Zealand region, visit giac.org/certify-AISA-21 or email Steven Armitage, Country Director, Australia, SANS Institute, APAC, at anz@sans.org

GIAC
CERTIFICATIONS
www.giac.org/certify-today