Cyber Today

EDITION 2, 2023

UNEARTHING THREATS TO MINING OPERATIONS

INNOVATIONS IN CRYPTOGRAPHY

HOW CAN BOARD DIRECTORS SUPPORT THE CISO?

AISA

AUSCERT

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

AusCERT provides member organisations with proactive and reactive advice and solutions to current threats and vulnerabilities. We help members prevent, detect, respond and mitigate cyber-based attacks.

As a not-for-profit security group based at The University of Queensland Australia, AusCERT delivers 24/7 service to members alongside a range of comprehensive tools to strengthen your cyber security strategy. Proudly providing cyber security services and expertise for 30 years strong.

BECOME A MEMBER TODAY!

MEMBERSHIP@AUSCERT.ORG.AU

AUSCERT.ORG.AU

07 3365 4417

SERVICES

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

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 IN CHIEF
Giulia Heppell
giulia.heppell@executivemedia.com.au

CO-EDITORS
Dr Suelette Dreyfus, Akash Mittal,
Branko Ninkovic

EDITORIAL ASSISTANTS
Eden Cox and Ruby O'Brien

DESIGN
Sam Garland

PARTNER ORGANISATIONS
AusCERT, **Curtin University,** Emantra,
Macquarie University, Rapid7 Australia Pty Ltd,
SANS, TAFE NSW

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 and Adobe Stock.

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

Proudly Printed In Australia

We acknowledge the Wurundjeri people of the Kulin nation who are the traditional custodians of the land on which this magazine is published.

Contents

FOREWORD

2 Foreword

INSIGHT

6 Working towards digital trust: sidestepping the obstacles

SPOTLIGHT

12 Unearthing threats to mining operations

CYBER ATTACKS

16 Info stealers: old malware generating new risks

DIGITAL TRANSFORMATION

19 Data privacy in the age of digital transformation

SECURITY

24 Maximising the value of penetration testing
27 Innovations in cryptography
30 An Australian cyber militia?
34 Hitting the cyber gym

CULTURE

36 How can board directors support the CISO?
39 As pressures mount on CISOs, boosting self-resilience takes priority
42 Addressing mental health in cyber

HR AND RECRUITMENT

46 Purposeful recruitment in cyber

EDUCATION AND TRAINING

54 From the battlefield to the boardroom
62 Is a master's of cyber security worth it?

Foreword

A message from Chloe Hatzis, Board Director & Company Secretary, AISA.

Chloe Hatzis

In the past year, Australians have been faced with many serious and important developments in the cyber security sector that impact on our liberties, choices, intentions, and futures.

As an industry working towards building cyber resilience and knowledge throughout Australia, we have so many elements to consider and so much to continuously learn. While researching topics to cover in this foreword, I came across a wide range of themes covering recent cyber security incidents, including Robodebt, cyberbullying, the progress of artificial intelligence (AI) laws, the lack of cyber skills, the lack of responsibility and accountability, and so on. I don't know about you, but with all that, there are days when I am inspired and intrigued by my work and what our industry is achieving, and then there are days when I feel like closing all my devices down and hiding away on a farm in rural Tasmania.

Despite the challenges, it is important to take the time to reflect on the good that we have achieved so far. The beginning of a new financial year is an ideal time to do this.

Over the past year, we have seen serious cyber security incidents that have affected the personal lives of many Australians. At the same time, we saw our industry rally and support those dealing with the incidents and the fallout from them. The conversation around cyber security has been taken up more broadly around both kitchen tables and boardroom tables as a result. Our friends who thought our jobs were super cool yet mysterious finally understood what it is we do. But more than that, the conversations took on a greater depth, and those who thought 'She'll be right' are now taking a step back and thinking twice. More people are taking the time to understand the importance of cyber security within their world.

In the private sector, the discussions have progressed at a board level. Recently, AISA partnered with the Australian Institute of Company Directors to host cyber security roundtables. The conversations demonstrated an increased understanding among executives about how they should be preparing for incidents that will affect their organisations and stakeholders. There is still more work to be done here, but it is a definite sign of progress on the path to cyber resilience.

The government has also taken proactive steps to address important issues with the detail and effort they deserve. Privacy laws are being given proper consideration, and reviews of past significant technological implementations are being conducted. The aim of this is to build the most cyber-secure nation.

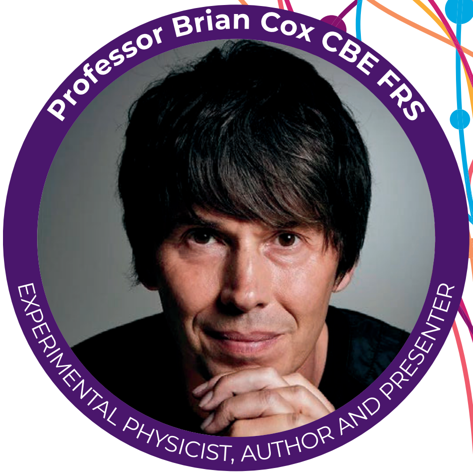
Internationally, consideration of human rights and liberties is front and centre, as nation-states deal with the legal issues surrounding new technologies. The progression of the European Union (EU) Artificial Intelligence Act (AI Act) is leading the way, with the United States, Canada, China and Singapore taking up their own initiatives.[1] The impact of the EU AI Act is anticipated to be like that of the General Data Protection Regulation.

In the face of continuing adversity, these examples really show how our efforts to build resiliency are working. Of course, there is still so much to do, especially as threats continue to evolve at a rapid pace. But on reflection, we have made progress towards our goals, and we should take a moment to celebrate that.

As you read through these pages, I suggest that you take a moment to reflect on where you have seen progress in the past 12 months. Think of the achievements you have made, and identify opportunities for improvement. Finally, ask yourself what else can we do to further build our cyber resilience. ●

[1] US federal AI governance: Laws, policies and strategies (iapp.org)

OPPORTUNITIES


Professor Brian Cox CBE FRS
EXPERIMENTAL PHYSICIST, AUTHOR AND PRESENTER

Chris Hadfield
ASTRONAUT, ENGINEER AND MILITARY FIGHTER/TEST PILOT

AUSTRALIAN CYBER CONFERENCE 2023

REGISTER NOW

MELBOURNE | 17 – 19 OCTOBER

Melbourne Convention and Exhibition Centre

Mikko Hypponen
CYBERSECURITY RESEARCHER AND AUTHOR

Paula Januszkiewicz
FOUNDER & CEO OF CQURE INC. AND CQURE ACADEMY

Mart Noorma
DIRECTOR OF NATO CCDCOE

AISA

cyberconference.com.au
#cybercon2023

Are we safe?

BY DAVID COLEMAN, LEAD SECURITY SOLUTIONS ARCHITECT, ANZ, RAPID7

Three words every CISO should prepare for.

In this time of heightened sensitivity, every CISO must be ready for when their CEO asks, 'Are we safe?'

The definition of 'safe' depends upon a range of factors. This includes your processes, organisational security culture, availability of skilled teams and tools, and, importantly, defined cyber security metrics aligned to risk appetite. A delicate balance is required, and many technically focused CISOs begin their cyber security metrics with details that an average board won't understand. If you want to get on the front foot with your CEO, here are three things to help.

1. Assess

Best practice cyber security assessment not only evaluates your organisation's susceptibility to vulnerabilities and threats, but also your organisation's security culture. At a technical level, assessments rely heavily upon having visibility of your entire technology environment. Greater visibility begins with gathering accurate data from a tool you can trust – one that ensures that the number of false positives are low and accuracy is high. Any assessment of cyber security should also be viewed in light of your organisation's obligations and compliance with regulations, particularly with respect to industry guidance and critical infrastructure.

2. Quantify

The cyber industry relies upon rating systems and models to help understand the severity levels of those threats. The challenge is that much of this is meaningless to those outside our world. Case in point, according to CVE Details, out of roughly 176,000 vulnerabilities, more than 19,000 have a Common Vulnerability Scoring System rating of 9.0–10.0 (most severe) – that's over one in 10. How is that data then further interpreted to understand what's relevant to your organisation to prioritise resources and explain to senior management so they can understand what's important? It's about communication.

3. Communicate

To better communicate risks and threats means speaking a language your leadership understands. It's about reputational, financial and operational impact. Where possible, risks should be assigned a specific dollar value proportionate with their potential impact. This approach provides an easy way of prioritising and addressing the most critical risks. Business leaders are then able to assess their decisions based on likelihood of occurrence and cost to the bottom line.

Set expectations

No organisation will ever be '100 per cent safe', and putting in place tools and resources is merely half the battle. Positioning risk and communicating with your senior leadership teams are just as vital in being able to set expectations. Unfortunately, we've seen firsthand the impacts of breaches in Australia and, very often, how a situation is managed and dealt with will have a huge bearing on your CEO's mindset. ●

If you want to find out more about the latest vulnerabilities that could impact your organisation as you bid to keep it 'safe', read Rapid7's latest vulnerability report and find out more by visiting its CISO Perspectives Hub at www.rapid7.com/info/ciso-perspectives/

THE SEVEN STEPS TO CYBER SAFETY HEAVEN

Let's face it, your organisation is never going to be 100% safe from bad actors. And while your leadership team will always want to believe you are, as cyber security leaders, you know the reality is very different. You could have an endless budget, unlimited resources and all of the tools, yet, you could still fall victim to an attack through no fault of your own.

Positioning and communication about what you're doing with your senior leadership teams is vital in being able to set expectations. Here are seven things that need to be on your checklist for when your CEO asks, 'Are we safe?'

Assess your security culture and gather support from seniors leaders

One of the biggest determinants of successful cyber culture is whether or not it is driven from the very top of the business.

Gain visibility across your complete technology environment

Greater visibility begins with gathering accurate data from a tool you can trust; one that ensures the number of false positives are low and accuracy is high.

Understand where your vulnerabilities lie and the critical ones that need patching

Effective vulnerability management starts with knowing what's in your local, remote, cloud, containerized, and virtual infrastructure.

Ensure compliance with frameworks / regulations

The ASD Essential 8 is a great place to begin if you need a starting point. If your organisation is regarded as critical infrastructure, take a look at the latest Government directives.

Gather threat intelligence a protect your digital assets

Stay ahead of threats to your organisation, employees, and customers with proactive clear, deep, and dark web monitoring. Get contextualised alerts that enable rapid response.

Implement the capabilities to detect AND respond

Carry out attack simulations on a regular basis and make sure the entire company is involved. Cyber is everyone's responsibility.

Secure your cloud environments and applications

Ensure you can detect cloud risk immediately with real-time, agentless visibility into everything running across your entire environment.

Want to be prepared for your 'Are we safe' conversation?

Find out more at our CISO Perspectives hub www.rapid7.com/info/ciso-perspectives/

Working towards digital trust: sidestepping the obstacles

BY JO STEWART-RATTRAY, OCEANIA AMBASSADOR, ISACA

Tackling the major challenges faced by Australian organisations.

Almost every organisation in Australia that participated in ISACA's 2023 State of Digital Trust research confirmed that digital trust is important (99 per cent), while 84 per cent of respondents believe its importance will increase in the next five years.

These results are optimistic and demonstrate the effect that two years of gruelling cyber attacks have had on the mindset of company leaders when it comes to protecting the digital reputation of their business.

We know organisations with a healthy level of digital trust benefit from customer loyalty, investor confidence and increased innovation. On the flip side, those organisations with low levels of digital trust may feel the impact on their bottom line, as customers increasingly seek out organisations that can protect their personal information and data.

While importance of digital trust ranks high among business leaders in Australia, ISACA's report signifies a disconnect between intention and action.

Only 29 per cent of respondents plan to increase budgets in the next year to achieve digital trust, 13 per cent have a dedicated digital trust role, 18 per cent of board directors have made digital trust a priority, and 22 per cent of organisations measure digital trust among customers.

Overcoming the top five obstacles to attaining digital trust

Skills and training

While 52 per cent of respondents cite a lack of skills and training as a barrier, organisations can still progress digital trust by adopting a cohesive and organised approach across the business. Fundamentally, digital trust is an umbrella term that indicates all business functions operate in sync towards an overall enterprise goal of achieving trust through their approach to protecting data.

While specific skills training is optimal, there are many processes that can be established in the absence of formal training to ensure business units work collaboratively, efficiently and transparently – all major steps towards ensuring stakeholder trust.

Lack of leadership buy-in

Some 52 per cent of respondents said a lack of leadership buy-in prevents digital trust from being achieved. While many organisations view digital trust as part of each employee's responsibility, overall accountability must be entrusted to a leader who can effectively oversee the deployment of digital trust processes across all business units, and report to the board and senior executives.

One-third (35 per cent) of respondents said the senior leadership team is ultimately responsible. While a chief digital trust officer exists in a few forward-thinking organisations, only 13 per cent have a staff position dedicated to this role.

The major gap in ownership of overseeing digital trust is certainly an area where organisations can make a fast impact. A digital trust officer or other employee that leads an organisation on the path to achieving digital trust does not necessarily need technical prowess, but needs the ability to motivate employees and raise awareness of privacy issues, instil ethics, encourage transparency, and communicate effectively between senior leaders, the board, and wider staff.

Lack of budget

A major obstacle to achieving digital trust that is often cited is a lack of budget, with 47 per cent of respondents saying it impedes progress; however, a cost-effective way to circumvent this is, again, to ensure business units work collaboratively rather than siloed, promoting critical information sharing.

This involves regular monitoring, auditing and measuring of current privacy and security practices to ensure that existing and, importantly, new organisational projects are responsibly and sustainably implemented with digital trust at the core.

Prevention is the key, so ensuring cyber security and privacy professionals are involved in new projects and business transformations from the 'ground up' is more cost-effective than dealing with a breach due to poor design and lack of input from the outset.

Lack of technological resources

As the pace of digital transformation increases, pressures from stakeholders intensify, as does the sophistication of cyber attacks. A lack of technological resources required to successfully

Jo Stewart-Rattray

administer digital trust is felt by 43 per cent of respondents.

Currently, only 17 per cent of respondents use a specific framework for achieving digital trust, while 51 per cent believe it is important to have a digital trust framework in place.

Digital trust not seen as a priority

Despite its importance, 41 per cent of respondents said digital trust is not seen as a priority in their organisation.

Of all the obstacles we've reviewed, this is by far the most important, as change can only occur when the goal is prioritised. Digital trust will be the divide between those companies who continue to grow and succeed, and those that falter.

Prioritising digital trust does not always require a cumbersome effort – it simply means that each part of a business factors trust into their daily operations, constantly evaluating their practices and adjusting them when improvements can be made.

The way forward

Emerging megatrends and technology that we are only beginning to understand demand the increased priority and adoption of digital trust. Regardless of organisation size, available budget and staffing levels, each has the ability, at the very least, to ensure that employees know the importance of privacy. Larger companies can ensure that collaborative efforts and information sharing are prioritised across a business, and that any new program or corporate initiative has been assessed by a security and privacy team to ensure best practice from the outset.

While there are certainly obstacles at play to achieving digital trust, positive efforts can – and must – be made that do not require large injections of cash and increased staff levels. Any step towards protecting privacy and data will result in positive outcomes for a business. ●

About the author

Jo Stewart-Rattray has more than 25 years' experience in the security industry. She consults in risk and technology issues, with a particular emphasis on governance and IT security in businesses as a Director with BRM Advisory. She regularly provides strategic advice and consulting to the banking and finance, utilities, health care, manufacturing, tertiary education, retail, and government sectors.

PARTNER CONTENT

Trends in cyberthreats

BY ROSS DEWAR, FOUNDER AND CEO, EMANTRA

Think of the major world changes this century – globalisation, geopolitical instability, terrorism, social media and the digitisation of lifestyle. Each of these dynamics has harboured the growth of a cybercrime industry now estimated to be worth US$8 trillion.[1]

Even climate change and COVID-19, which led to changes in the way we live and work, have created new vulnerabilities for cybercriminals to exploit.

The growing sophistication of cyber attacks and involvement of state-sponsored actors make it harder for organisations to defend. Here are some increasing or emerging trends to be aware of:

- Cyberwarfare and espionage techniques, now funded by national defence budgets, will increasingly turn eyes from the military to the marketplace not only to disrupt, but also to gain self-funding through direct exploitation. This will create a vicious circle.
- The emergence of a viable Cybercrime-as-a-Service business model significantly lowers the barrier of entry for unsophisticated mass hackers. Many threats, such as distributed denial of service, phishing and malware, are now productised on the dark web, together with support and technical assistance.
- Internet of Things devices, which are ubiquitous, are subject to increasing attention, often because they are seen as the 'easy way in' to a company network. From electric vehicle chargers, point of sale, and physical security and measurement devices, to cameras and implanted medical devices, there exists serious potential for extortion, including life and death threats.
- Supply chain cybercrime has potential for disruption on an industrial scale. Even small players in a critical supply chain (often the weakest link) are targeted – not because of the direct reward, but because of the collateral damage that can result elsewhere.
- The massive artificial intelligence (AI) of global clouds is being exploited to host resource-heavy capabilities, such as brute-force computers, machine learning, botnet-as-a-service, Domain Name System laundering, etc., which can create deeper and smarter types of exploits. Another product of AI – deepfake – makes phishing, scamming and identity theft harder to defend against.
- That old chestnut, ransomware has proven so easy and lucrative. Emerging is the concept of double extortion, where the data is not only held to ransom, but is also offered for sale on the dark web at the same time. Two birds with one stone. Ransomware is now being developed to target specific sectors, such as healthcare, education and government.
- As opposed to steal and run, the advanced persistent threat technique doesn't require immediate pay-off. For example, an agent is allowed to sit dormant on a victim's network, waiting for a trigger. In the meantime, they can perform legitimate tasks to disguise their real intent. Criminal groups using this model are sophisticated and must be well funded, as the 'time to payout' is long. Known perpetrators of this activity include APT28/29, APT10, APT33/34 and Lazarus Group. All of these are state-sponsored.

You won't be subject to all these threats, but some may be likely. The best defence is to know what's out there, which risks your business or market is most susceptible to, and to stay close to expert advice.

Emantra has experience in dealing with many of the emerging threats mentioned here, and can give you a risk-weighted scorecard and specialist advice. ●

[1] 2022 Official Cybercrime Report, Cybersecurity Ventures

Emantra
SECURING OUR FUTURE

We are EMANTRA

Sovereign Hosting
Secure Cloud
IRAP-Assessed SIG
Enterprise Cyber Risk Management

1300 728 953

Unearthing threats to mining operations

BY CONOR MCLAREN, SENIOR ADVERSARY HUNTER, DRAGOS

The mining industry is one of the backbones of the Australian economy, contributing to a significant component of Australian economic output and exports. Moreover, mining and the associated commodities form a critical part of modern society – providing the essential materials required to build infrastructure, vehicles, housing, technology, and a range of other consumer goods.

Mining organisations have increasingly become an attractive target for adversaries seeking to leverage cyber attacks to further objectives – ranging from financial gain and disruption, to even strategic operations. Moreover, as mining operations continue to grow in complexity and technological interconnectedness, the potential impacts of a successful attack have dramatically increased in severity. This article delves into some of the most significant threats to mining organisations in Australia, as observed by the Dragos Intelligence team.

Industrial control systems–focused threats

Generally speaking, and notwithstanding the intricacies of the different mine types, the level of industrial control systems (ICS)/operational technology (OT) complexity and interconnectedness increases as a project moves along the mining cycle, often reaching a peak at the production stage. Accordingly, this is where threats, such as ICS/OT-focused malware, can have the most significant impact. On this note, ICS/OT targeted threats continue to grow in both prominence and sophistication. Dragos currently tracks 22 threat groups that demonstrate the intent, opportunity or capability to impact industrial operations. ICS/OT targeted malware and other threats have the potential to cause significant operational disruption, property damage, financial loss, and even catastrophic safety issues. One example of such a threat is depicted by the Dragos-designated threat group CHERNOVITE and the associated PIPEDREAM malware framework.

Dragos assesses with high confidence that CHERNOVITE is a highly motivated and well-funded state-sponsored entity that is skilled in software development methods, well-versed

in ICS protocols, and experienced in intrusion techniques. CHERNOVITE developed the PIPEDREAM malware framework, possessing a breadth of ICS knowledge beyond any of Dragos's previously discovered threat groups. While Dragos assesses with high confidence that it has not yet been employed for disruptive or destructive purposes, PIPEDREAM has the potential to impact a wide variety of industrial control programmable logic controllers (PLCs) and industrial software, including Omron and Schneider Electric controllers.

It must also be highlighted that the abovementioned target devices, while indicative, are not an exhaustive list by which the PIPEDREAM framework is bound. Instead, adversaries could theoretically leverage the tool to target a wide range of other devices in the future – including the potential of devices directly utilised by mining entities. This is primarily due to the modular and extensible nature of the platform, paired with its use of ubiquitous industrial protocols, which means that it is possible that the framework could be expanded. In acknowledging this, PIPEDREAM's targeting and potential impacts are not necessarily limited by its capabilities, but rather by the objectives of CHERNOVITE as an adversary. As such, this threat group and its capabilities pose a significant risk to industrial organisations globally, and could cause disruption, degradation, and potentially the destruction of industrial environments, irrespective of the associated geography or industry vertical.

Ransomware

In addition to ICS/OT targeted threats, ransomware remains one of the most significant threats to modern-day mining operations. Dragos analyses and monitors the activities of several ransomware groups that have targeted mining organisations and

infrastructure. Based on publicly reported information, numerous mining organisations have been impacted by ransomware over the past 12 months. Many of the associated cybercriminal groups continue to leverage ransomware as part of their operations, owing to the lowered barrier of entry facilitated by the Ransomware-as-a-Service model, paired with the continued profitability and relatively high chance of eventual success.

Most ransomware operators are financially motivated organisations and, consequently, they constantly explore new tactics that enhance the probability of being paid. A prime example is the increased use of data extortion techniques, whereby the adversary threatens to release compromised victim information on their dedicated leak site (DLS) or dark web resources if the associated ransom is not paid. Adversaries leaking this information can create numerous security challenges for a mining organisation, as some of the leaked data may contain internal technical details (e.g., architecture maps or firewall rules) that a separate adversary could leverage to enable future attacks against the victim.

An adversary's successful deployment of ransomware within a mining company's environment can have a range of disastrous implications, with the ultimate impact largely depending on the intent of the associated adversary and the environment in which the ransomware is deployed. In the case of IT-specific ransomware, post-compromise lateral movement into OT networks (e.g., in merged environments) with subsequent ransomware deployment can lead to a significant direct operational impact; however, even if an OT foothold is not obtained, direct IT impact can lead to the secondary OT impact by disrupting business-critical IT systems, or by ceasing all operations as a defined safety precaution. Such a scenario came to fruition in December 2022, when a major Canadian copper producer was impacted by ransomware and had to shut down its mill to determine any effect on its control systems, thus temporarily halting its 45,000 tonnes-per-day processing capacity.

Supply chain and third-party connections

The increased dependency of mining organisations on a range of suppliers, vendors, and other third parties has ultimately increased the levels of supply chain and third-party risks. Historically, there have been numerous examples of supply chain compromises across many sectors that leveraged exploited software updates and installers – one of the most notable examples being the SolarWinds supply chain attack. A Dragos white paper[1] also indicated that supply chain compromise was one of the top initial access techniques favoured by Dragos-monitored (among many other) threat groups, thus further highlighting the prevalence of this initial access technique. Moreover, a ransomware group recently compromised a large-scale mining supplier with the associated data (including customer data) listed on the group's DLS. In such an example, information obtained by another adversary via the DLS

could theoretically act to facilitate a future attack against the supplier's customer base.

Despite this, original equipment manufacturer (OEM) and vendor remote access solutions also add to the risks experienced by modern mining operations. Remote access solutions are a vital component of modern OT mining equipment solutions. These solutions are critical in providing access to vendors, troubleshooting issues, and ensuring the optimal functioning of the underlying equipment; however, remote access solutions can also potentially provide an ingress into ICS/OT environments via compromised or poorly secured connections. While not specific to mining, one of the most notable examples is XENOTIME's targeting and subsequent compromise of numerous ICS vendors and manufacturers, which provided potential supply chain threat opportunities via vendor-enabled access to target ICS networks.

Intellectual property theft

Mining organisations produce and possess a range of highly confidential information – a few examples include exploration drill core results, product blend information and, of course, a plethora of operational, technological, and financial information. All this information plays a critical role in ensuring the optimal functioning of operations, enabling organisational decision-making and, in the case of market-sensitive information, can impact a publicly listed organisation's share price. Consequently, adversaries may seek to compromise a mining organisation to facilitate access to this information to further their economic or strategic goals. One such example is the Dragos-designated threat group PETROVITE, which targeted mining and energy operations in Kazakhstan starting in late 2019. PETROVITE leverages tailored spear phishing documents that install a multi-component backdoor on victim devices. Dragos assesses with low confidence that PETROVITE endeavoured to achieve initial access to facilitate information gathering and allow for potential intellectual property theft.

Moving forward

While the threats outlined in this article are not exhaustive, they provide an overview of some of the more prominent threats to mining organisations, as observed by Dragos. Beyond this, there are many other threats stemming from hacktivism, exposed ICS/OT assets, vulnerable ICS/OT assets, and a range of suboptimal security controls that are not necessarily exclusive to mining organisations. This observed diversity of threats to mining operations, paired with the criticalness of the industry, ultimately mandates the adoption of a robust and comprehensive security program that encompasses both IT and OT domains. In acknowledging this, Dragos recommends that Australian mining organisations utilise the five critical controls for OT cyber security[2], which include an incident response plan, a defensible architecture, OT visibility and monitoring, secure remote access, and risk-based vulnerability management. ●

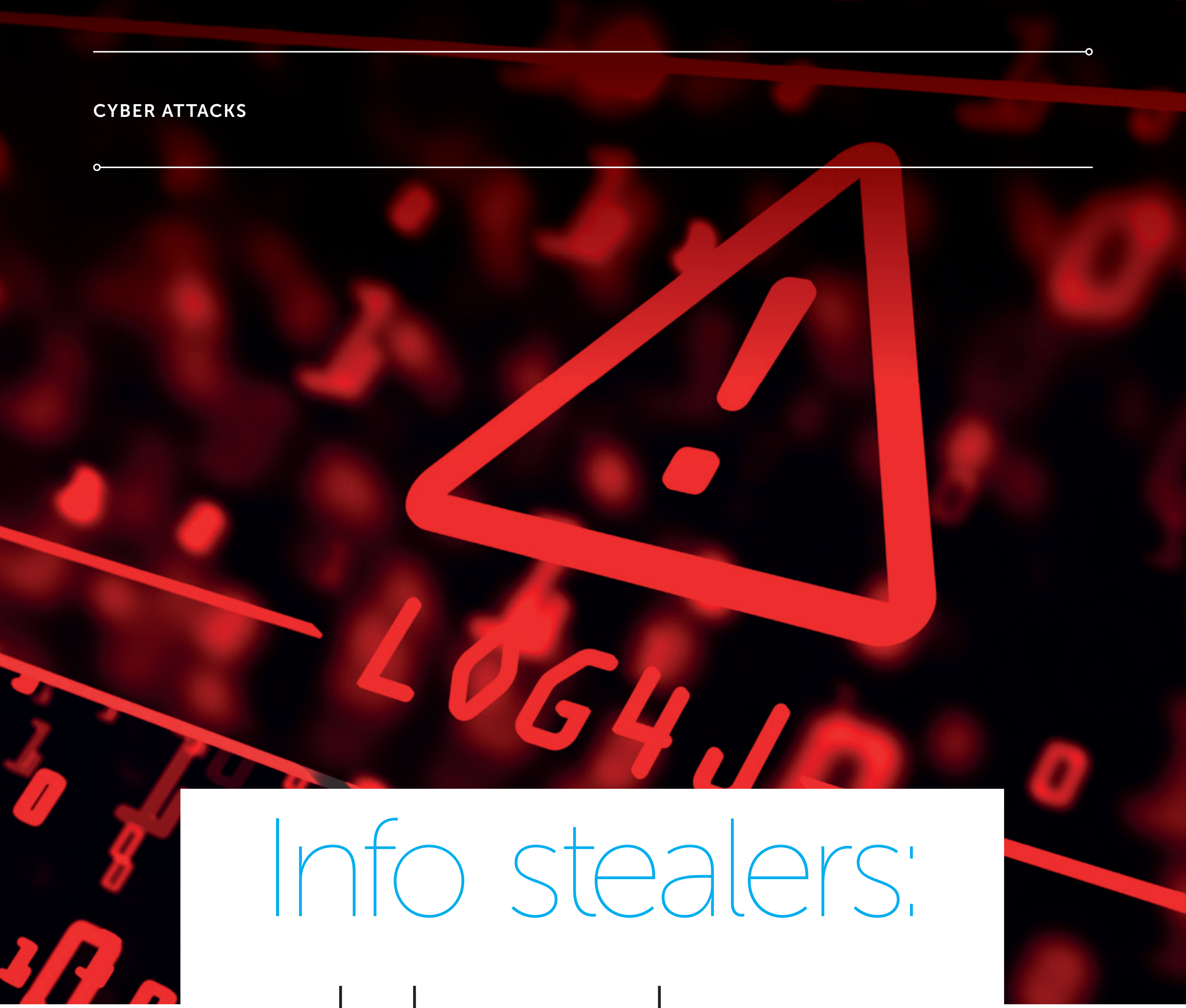
About the author

***Conor McLaren** is a Senior Adversary Hunter at Dragos, focused on researching threats to ICS/OT organisations in the Oceania region. McLaren is particularly interested in strategic-level intelligence due to its profound impact on business decisions and organisational security strategy. He has a diverse range of prior cyber security experience within the resources, fast-moving consumer goods, government, technology and consulting sectors. McLaren is passionate about cyber security, and is committed to developing innovative solutions to adapt to the ever-changing threat landscape.*

End notes

[1] https://hub.dragos.com/activity-group-access-into-industrial-environments

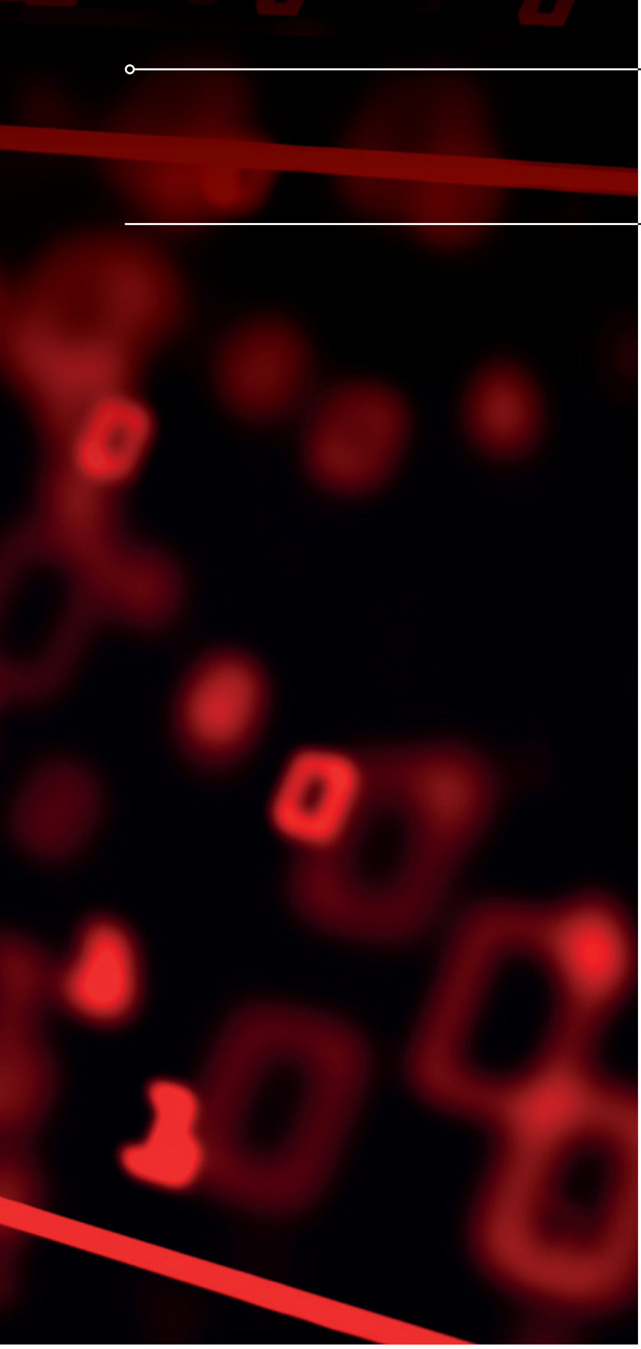
[2] https://hub.dragos.com/guide/5-critical-controls



Info stealers: old malware generating new risks

BY PETER WATSON, INTELLIGENCE SPECIALIST, RECORDED FUTURE

User data, stolen and exfiltrated by info stealer malware, has been for sale on the dark web for many years, but there has been a marked increase in the volume of stolen data over the past two years.



Peter Watson

Info stealers are an evolution of the Remote Access Trojans that surfaced around 2006 with Zeus, and were followed by other well-known banking trojans, such as Qakbot, Ursnif, Emotet and Trickbot. Banking credentials and financial data were stolen and exfiltrated to command-and-control servers with infected machines becoming part of a 'botnet' – essentially, a large number of remote machines controlled by a central server. Info stealers can capture a broad range of data from infected machines, including keystrokes, session cookies, credentials from browser password stores, screen and video captures, local data, browser history, and bookmarks and clipboard data.

With info stealers today, access to a botnet and the associated infected remote machines is commonly sold as Malware-as-a-Service (MaaS). The subscriber is given access to a web-based administration panel to view, sort and manage the stolen user data, and this presents a low barrier to entry for anyone with malicious intent. The exfiltrated data is presented as an archive called a stealer log, and then sold on the dark web at a relatively low cost – maybe $10 per stealer log. The purchaser might use the data to log in to websites, including internet banking sites, with the victims' credentials.

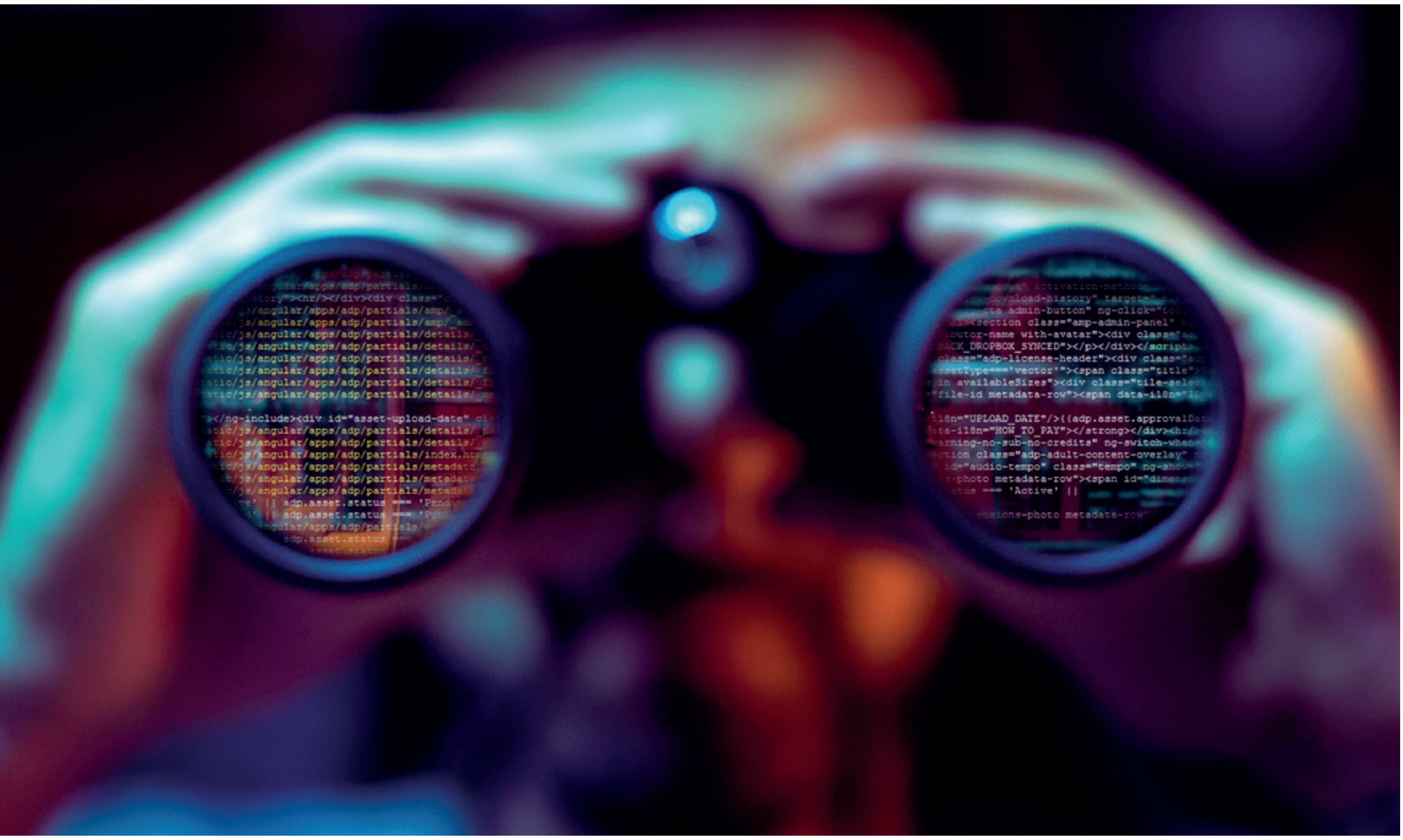
Historically, the data contained in stealer logs wasn't considered to be particularly useful to sophisticated cybercriminals, as they were looking for high-value targets, not home users. The more recent growth in stealer logs has been driven by a range of factors, which include:

- a rise in remote workers accessing corporate assets from their home machines due to the pandemic
- the MaaS model, which provides a low entry barrier to unaffiliated threat actors
- theft of session cookies to bypass multi-factor authentication (MFA)
- the ability of newer variants to steal data from MFA apps
- other MFA bypass techniques, such as MFA fatigue attacks.

In parallel with these changes, initial access brokers (IABs) have become increasingly active. They use low-cost credentials obtained via an info stealer MaaS, either offering or purchased through the dark web to on-sell to ransomware affiliates for initial access. Profitable credentials may be logins for corporate VPNs, Wordpress admin panels, Remote Desktop Protocol, Citrix or any other technologies that potentially provide access to the internal network of a business. These initial access credentials are typically sold for a profit of 10 times or more on top-tier Russian-language forums, such as Exploit and XSS.

These IABs are exploiting the availability of credentials from info stealer malware that provide initial access to corporate assets, and they have become a reliable initial access vector for ransomware gangs and their affiliates.

Recorded Future has identified almost a tripling of initial access listings by IABs from 2021 to 2022. It's likely that the IAB market has matured in part due to the increased demand for network access from these actors. We have also identified a sixfold increase in the number of credentials stolen by info stealer malware between Q1 and Q4 2022.



Corporations can no longer rely on MFA to protect their assets. Around 40 per cent of the credentials stolen by info stealers include cookies. An unexpired session cookie can be used in a pass-the-cookie attack, bypassing MFA. There are other creative methods to bypass MFA, including MFA fatigue (bombing) attacks, bombarding the victim with repeated two-factor authentication push notifications until they finally accept one.

Another MFA bypass method documented by the United States Cybersecurity and Infrastructure Security Agency was exploitation of the default configuration of an identity and access management (IAM) vendor. In this case, the threat actors were able to brute force a user's password and enrol a new device on the account. They then used the PrintNightmare vulnerability to elevate privileges and stop the communication between the IAM agent and server. The MFA servers' default setting in such a circumstance was to fail open, thereby disabling MFA.

Endpoint security alone cannot provide sufficient protection against info stealers either. The majority of stealer logs contain metadata on the endpoint tools installed on the infected machine, and many endpoint detection and response vendors are represented. Info stealers are often hidden inside the installation archives for cracked or unlicensed software. They also have a small footprint and are polymorphic in nature, each executable having a unique file hash.

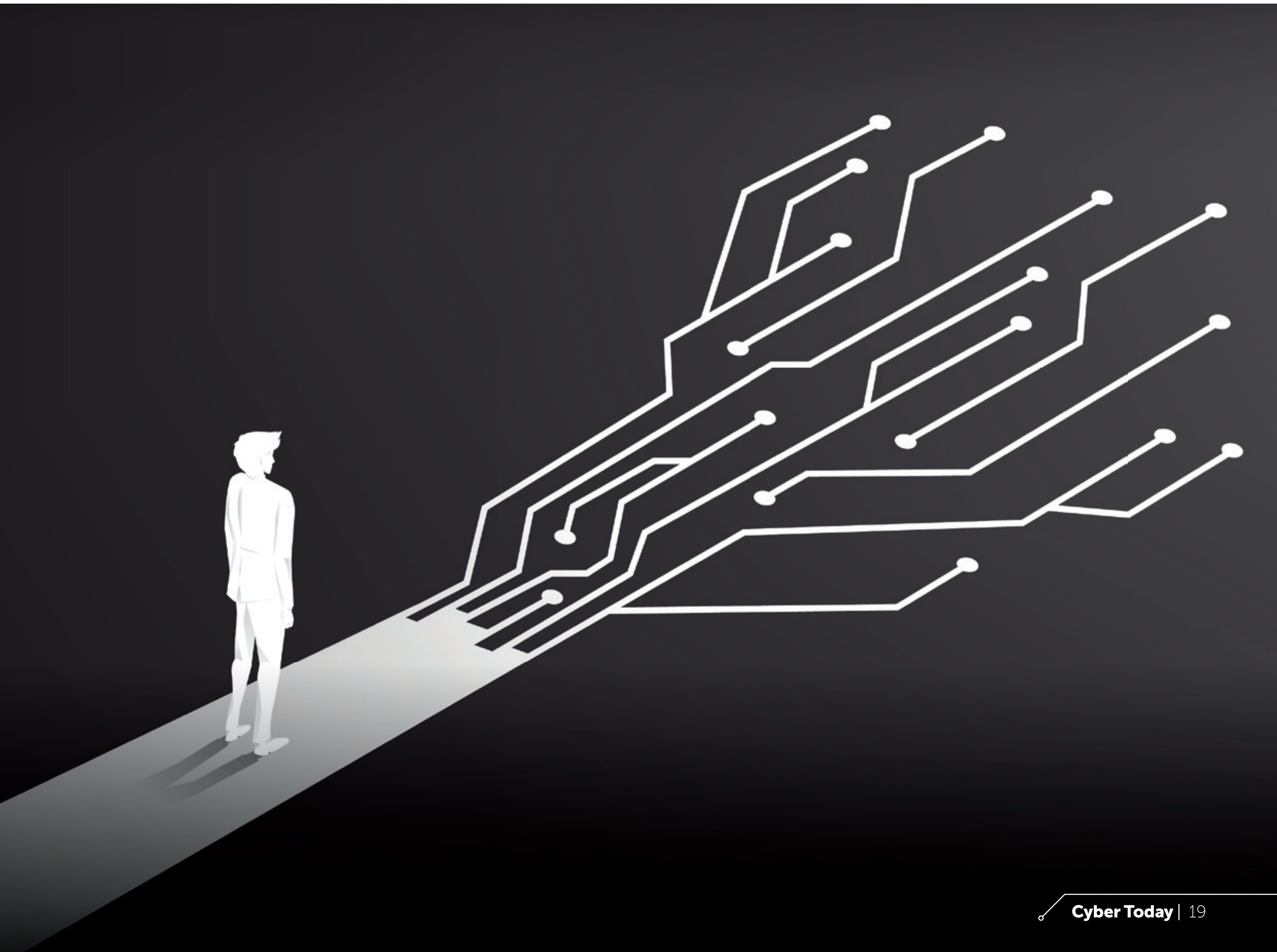
As with most malware infections, phishing is the number one attack vector used to install info stealer malware, and so phishing awareness training and related protections are key. At a broader level, tightening controls around session cookie lifetimes on critical assets is worthy of consideration as a mitigation strategy. And, perhaps most importantly, the use of employees' home machines to access corporate assets represents the biggest risk of exposure from info stealer malware – it might be time to re-evaluate the access policies for remote workers. •

About the author

Peter Watson is a cyber security specialist with more than 20 years' experience in a range of roles spanning multiple security domains. He holds Certified Information Systems Security Professional and GIAC Certified Penetration Tester certifications. In addition to security intelligence, other focus areas over the past 10 years include network forensics and malware analysis.

Data privacy in the age of digital transformation

BY HAFIZ SHEIKH ADNAN AHMED



Most of us have been hearing the term 'digital transformation' pretty much everywhere for a few years now. It started as migrating business processes to automation – e-services were introduced, and with the advent and usage of mobile phones, we saw mobile apps for almost every line of business. Digital transformation has meant that entire industries were transformed and moved a great deal of their activity online, embracing technologies like cloud storage, the Internet of Things, and more.

Digital transformation (DX) used to be something that was just good to have. But since COVID-19 disrupted business operations worldwide, many organisations now see DX as a necessary step in preserving their business. The global digital transformation market is expected to grow from US$469.8 billion in 2020 to US$1009.8 billion by 2025, at a compound annual growth rate of 16.5 per cent during the forecast period.

According to business review site FinancesOnline, the top benefits of adopting a digital model include improving operational efficiency, meeting changing customer expectations, and improving new product quality.

It is also important to understand what 'digital business' means to the organisations. Digital business enables better worker productivity through things like artificial intelligence (AI)–assisted processes, the ability to better manage business performance through data availability, and being able to better meet customer experience expectations.

With the advent of DX over the last two decades, a new statement has been coined: 'data is the new oil'. That holds true as individuals, organisations, states, and countries across the globe are realising the importance of data and data privacy. The bad guys are as intelligent as the good guys, and they know what they are after. With the massive migration in the last couple of years to remote working due to COVID-19, making better use of the cloud has exposed more data, and it is still not clear if everybody is aware of the increased risk and how to protect their information.

After the enforcement of the European Union (EU) General Data Protection Regulation (GDPR) in 2018, which I consider the mother of all modern data privacy laws and regulations, states and countries around the globe are either adopting existing data privacy laws or creating their own.

According to a 2021 report, 133 jurisdictions around the world have enacted omnibus data privacy laws. Throughout the last several months, many countries have announced and enforced data privacy regulations. For example, China enacted the Personal Information Protection Law (PIPL), Saudi Arabia approved a personal data protection law that came into effect in March 2022, and the United Arab Emirates (UAE) published the UAE Data Protection Law, which introduces major changes to data protection in the UAE.

So, now we are standing at an interesting crossroad. We want things to be done in the blink of an eye. Our lives are 'digitised', and we are connected to, and surrounded by, devices. Our lives are overtaken by robotics, chatbots, virtual assistants, virtual reality, artificial intelligence and machine learning. Data control is flawed; on paper, data looks to be controlled by the entity to which it belongs, but the reality is different – the data owners themselves are often not aware of how their data is shared and used. Try looking for an item on Amazon on your phone; when you then go to any social media platform, you will keep seeing ads to buy that item. Did you authorise Amazon or those social media apps to do that? Maybe not specifically, but you signed in and agreed to the sites' data privacy policies.

While DX is creating major opportunities for organisations, it is also introducing a new dimension to the traditional view of risk. With Industry 4.0, business leaders are making strategic choices on the investment, technology, resourcing levels and skills needed to operate a digital business, all of which will have an impact on the short-term profitably and long-term viability of the businesses. These strategic choices inevitably involve an element of risk. At the same time, businesses must cope with external threats. For example, as businesses undergo DX and more of their assets become digital, the threats of cybercrimes and risks around data privacy are growing.

Let's take the example of AI, which has developed rapidly in recent years.

Today, AI and its applications are a part of everyday life, from social media newsfeeds to traffic-flow mediation in cities; autonomous cars; and connected consumer devices such as smart assistants, spam filters, voice-recognition systems and search engines.

AI has the potential to revolutionise society; however, there is a real risk that the use of new tools by states or enterprises could have a negative impact on human rights. The following are some of the major data privacy risk areas and problems related to AI:

- **Reidentification and deanonymisation:** AI applications can be used to identify and track individuals across different devices in their homes, at work and in public spaces. For example, facial recognition, a means by which individuals can be tracked and identified, has the potential to transform expectations of anonymity in public spaces.
- **Discrimination, unfairness, inaccuracies, and bias:** AI-driven identification, profiling and automated decision-making can lead to discriminatory or biased outcomes. People might be misclassified, misidentified, or judged negatively, and such errors or biases may disproportionately affect certain demographics.
- **Opacity and secrecy of profiling:** Some applications of AI can be obscure to individuals, regulators or even the designers of the system themselves, making it difficult to challenge or scrutinise outcomes. While there are technical solutions to help improve some systems' interpretability and/or ability to audit, a key challenge remains whenever this is not possible, and the outcome can significantly impact people's lives.
- **Data exploitation:** People are often unable to fully understand what kinds of – and how much – data their devices, networks and platforms generate, process or share. As consumers continue to introduce smart and connected devices into their homes, workplaces, public spaces and even bodies, the need to enforce limits on data exploitation has become increasingly pressing.
- **Prediction:** AI can utilise sophisticated machine-learning algorithms to infer or predict sensitive information from non-sensitive forms of data. For instance, someone's keyboard typing patterns can be analysed to deduce their emotional state, which includes emotions such as nervousness, confidence, sadness, or anxiety. Even more alarmingly, a person's political views, ethnic identity, sexual orientation, and even overall health status can also be determined based on activity logs, location data and similar metrics.

Let's now talk about the Internet of Things (IoT). IoT is a broad term that generally refers to physical devices connected to the internet that collect, share or use data. This includes personal wearable devices such as watches and glasses, home appliances such as televisions and toasters, features of buildings such as lifts and lights, supply chain and industrial machinery such as forklifts and sprinklers, and urban infrastructure such as traffic lights and rubbish bins. IoT devices and the data they collect can provide convenience, efficiency, and insights into essentially every aspect of our world. For the public sector, the IoT is currently providing many benefits, and has the potential to generate even greater public value in the future.

Consumers, governments and businesses everywhere are increasingly using IoT devices, and it is widely expected that the use of IoT will continue to expand rapidly; however, rushing into IoT without proper consideration of privacy can lead to harmful and unexpected consequences. As the IoT grows, the amount of data it generates will naturally increase alongside it. These large collections of data can, in many cases, constitute personal, health and sensitive information, raising many privacy challenges. Some of the challenges around data protection include, for example:

- **De-identification of IoT data:** The data collected by large IoT ecosystems like smart cities can be valuable for a range of purposes, such as research or informing policy decisions. A common way to maximise the value of this data is to make it publicly available online; however, it is generally impermissible for datasets that include personal information to be made publicly available. The simplest way to ensure that personal information is not included in a dataset is to allow individuals to remain anonymous by never collecting information that can

identify them; however, data collected by the IoT is often very difficult to de-identify due to its highly granular nature.

- **Transparency:** The passive nature of many IoT devices can make it difficult for individuals to be informed that their personal information is being collected. Devices in public spaces can collect information automatically, sometimes relying on individuals to opt out if they do not want their information collected.
- **Accountability:** The number of organisations that can be involved in an IoT ecosystem can make it difficult to identify who is, or should be, accountable for what. The nature of IoT devices can make it impossible for an organisation to have control over every aspect of it. For example, organisations often have little to no control over security and privacy risks with communication technologies such as satellite or 5G, as these are usually provided by third-party telecommunications companies. This can also be the case for cloud services, which can allow users to have anywhere from no control to high control over the security and privacy settings of the services they are using.
- **Interoperability:** The rapid expansion of the IoT in recent years has led to the development of many kinds of devices, application programming interface (API) infrastructure, data formats, standards, and frameworks. This has caused significant interoperability issues in that devices, software and data from one vendor often do not work with devices, software and data from other vendors.

Data Privacy solutions for digital transformation

Privacy laws have never been as important as they are today, with data now travelling the world through borderless networks. There are exciting times ahead for privacy legislations, as several notable privacy laws will be enforced. Cross-border transfers are likely to be one of the notable compliance issues tackled by legislative bodies and data-protection authorities to ensure the regularisation and normalisation of data transfers between countries.

Governments around the world are reacting to the increased demand for data protection through different legislations. There has been a proliferation of data protection laws during the last few years, which introduced new compliance requirements for organisations. In the case of new regulations, it is vital to achieve a balance between protection and free movement of sensitive data. Global compliance involves safeguarding sensitive data like payment and personal information.

The EU's GDPR is a landmark privacy law and a milestone for the digital age. It has introduced new rights for individuals, such as the 'right to be forgotten' and the 'right to data portability', and it has made breach notification mandatory.

Businesses should consider hiring data privacy architects and protection officers to assess their objectives and the privacy legislation with which they will have to comply. Businesses need to ensure that data protection officers (DPOs) are expert in both privacy and technology – a rare yet essential combination. This isn't just a matter of data privacy; it's about compliance, as well. While investing in the right security solutions will enhance businesses' posture against new technology-related risks, organisations need assistance in tackling this challenge from a compliance point of view.

Businesses need to work towards implementing transparent and secure mechanisms. With the right security solutions, companies can achieve the freedom and flexibility they need to succeed in a digital economy with confidence.

Businesses need to define data governance strategy, and privacy and protection should be at the heart of this strategy. It should include regular training, awareness, and workshops on digital technologies, and how to protect personal data while using those digital technologies. Besides external threats like phishing attacks, organisations should keep in mind that insider threats also exist, and should guard their sensitive data accordingly. The latter requires a focus on understanding and securing the data itself.

Businesses also need to employ data security governance principles by focusing on sensitive data protection and privacy, deleting unnecessary data, and consolidating data silos, whether they are on the premises or in the cloud, to ensure project alignment with business objectives.

The final verdict

Despite its potential pitfalls, digital transformation remains an extremely exciting venture for businesses of all shapes and sizes. The prospect of leveraging cutting-edge technology to accelerate a business's processes, thereby making it more competitive, is certainly attractive; however, data privacy should always be a foundation of any digital transformation project; without it, the whole house will start to fall.

At the end of the day, companies that incorporate transparent privacy policies into the building blocks of their business are the ones that will see increased brand loyalty moving forward. They're the ones that are actively pursuing ways to incorporate blockchain into their processes – that are actively working to not just meet but exceed the guidelines of the GDPR. They're the ones that actively empower their customers to offer them information, knowing it will be used to enhance their user experience – no more, no less.

But in the next three to five years, I anticipate that privacy will become a game-changer for the companies that do it right. It will bolster trust – and, ultimately, sales. And customers will, thankfully, be all the wiser for it. ●

About the author

Hafiz Sheikh Adnan Ahmed *started in 2005 as a Quality Assurance Engineer. Over the years, he has shaped his career in the areas of information and communications technology; governance, information and cyber security; business continuity and organisational resilience; data privacy and protection; risk management; enterprise excellence and innovation; and digital and strategic transformation. He is an analytical thinker, a writer, a certified trainer, a global mentor, and an adviser with proven leadership and organisational skills in empowering high-performing technology teams. He is a certified data protection officer and won Chief Information Security Officer of the Year awards in 2021 and 2022 from GCC Security Symposium Middle East, and Cyber Sentinels Middle East, respectively.*

Maximising the value of penetration testing

BY NIGEL PHAIR

Best practices for identifying and mitigating cyber security risks.

Nigel Phair

Cyber security threats continue to rise, and it is critical for all organisations to ensure that the security systems they have in place are effective in protecting data and the systems it resides on. Penetration testing is an essential part of an organisation's security strategy. CREST, the international not-for-profit membership body representing the global cyber security industry, has released the CREST Defensible Penetration Test – a specialisation that provides recommendations on how penetration tests should be scoped, delivered and signed off.

A penetration test is a simulated attack on a computer system, network, or application to identify vulnerabilities that could be exploited by attackers. The test should be conducted by skilled and accredited cyber security professionals who attempt to gain access to the system or application, and provide recommendations for mitigating the identified vulnerabilities.

A CREST Defensible Penetration Test is a comprehensive and structured approach to penetration testing, which focuses on identifying and exploiting vulnerabilities in an organisation's systems and processes. It is designed to identify vulnerabilities that

could be exploited by attackers and provide actionable recommendations to improve an organisation's security posture.

Benefits of a CREST Defensible Penetration Test include:

- **A comprehensive and structured approach:** This covers all aspects of an organisation's security posture. It includes a thorough analysis of the organisation's network infrastructure, applications, and processes, as well as its physical security. This comprehensive approach helps to ensure all vulnerabilities are identified and addressed.
- **Real-world simulation:** This takes into account the latest threats and attack techniques, and uses them to identify vulnerabilities. The test also considers an attacker's goals, such as accessing sensitive data or taking control of systems.
- **Actionable recommendations to improve an organisation's security posture:** The test report includes detailed information on identified vulnerabilities, including their severity and potential impact on the organisation. It also provides recommendations on how to address these vulnerabilities, prioritised based on their severity and impact.

- **Compliance requirements:** Many regulatory frameworks and standards, such as PCI DSS and ISO 27001, require regular penetration testing. A CREST Defensible Penetration Test meets these compliance requirements, and provides evidence that the organisation is taking the necessary steps to secure its systems and data.
- **Assurance and peace of mind:** An organisation's management and stakeholders can have peace of mind knowing their systems and data are resilient against a potential cyber attack.

With significant growth in the number of penetration tests being carried out each year, organisations procuring such activity need to do so with confidence and assurance. A partnership between the penetration testing organisation and the client to define and set appropriate expectations is key. Utilising a CREST International member company provides organisations with significant benefits.

CREST International member companies are required to adhere to high ethical and technical standards, and use a comprehensive and structured approach to penetration testing that covers all aspects of an organisation's security posture. This ensures that all vulnerabilities are identified and addressed, and the organisation receives a detailed report with actionable recommendations.

CREST International member companies employ skilled and experienced cyber security professionals who have undergone rigorous training and certification processes. These professionals can help to reduce an organisation's overall risk of a cyber attack by identifying vulnerabilities before they can be exploited by attackers, allowing an organisation to take proactive measures to address the vulnerabilities and reduce its risk.

The CREST Defensible Penetration Test is a comprehensive and advanced approach to penetration testing. It provides a structured methodology for identifying vulnerabilities in an organisation's systems and processes, and provides actionable recommendations to improve its security posture. With the increasing threat of cyber attacks, a CREST Defensible Penetration Test is an essential part of an organisation's security strategy. •

Innovations in cryptography

BY DR CHITCHANOK CHUENGSATIANSUP

Cryptography is a growing field due to its immense importance. This article will describe an emerging technology in the area of automated generation of optimised cryptographic code for a platform where the code will be used.

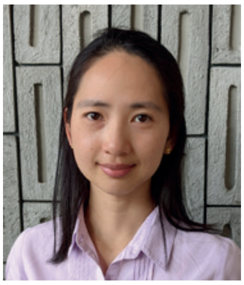
Cryptography is a fundamental mechanism that provides protection for sensitive information. It enables confidentiality, and safeguards online communication, internet banking, healthcare systems, and even national infrastructure. Failure in protection could lead to disastrous consequences, such as the disclosure of personal information, unauthorised access to classified data, impersonation of digital identity, or integrity breach of private records.

Being an essential ingredient in a wide range of security-sensitive software, cryptographic code needs to achieve three goals: correctness, efficiency and maintainability. It is crucial that cryptographic code produces correct results; otherwise, the defence would be void.

The computation of cryptographic algorithms should be fast so that it would not hinder the overall performance of the system with which it integrates. Due to an extensive usage of cryptography on various kinds of devices – ranging from powerful machines, such as computer servers, to small resource-constrained embedded gadgets, such as pacemakers – porting cryptographic code from one device to another, as well as managing the code for potential future modifications, should be simple.

To tackle the challenge of attaining the three aims, our international research team has developed CryptOpt, a cryptographic code optimiser that automatically generates optimised cryptographic code for a platform where the code will be used. CryptOpt is an open-source project.

This project is a collaborative work among multiple universities, both in Australia and overseas. The team includes The University of Melbourne, The University of Adelaide, Monash University, Ruhr University Bochum,



Dr Chitchanok Chuengsatiansup

Massachusetts Institute of Technology, Stanford University, and Georgia Institute of Technology.

The code produced by CryptOpt is also verified to preserve functional correctness. This means that the code is fast and secure. Portability and maintainability come from simply re-running CryptOpt to obtain suitable code for a new target platform, instead of having an expert programmer manually re-optimise and re-implement the code.

CryptOpt is built on the observation that cryptographic code consists of a sequence of mathematical operations, which can be rearranged so long as they satisfy predefined dependencies. Furthermore, there are multiple machine instructions that can implement the same mathematical operation. In other words, the same cryptographic algorithm can be implemented differently depending on the choices of operation sequences and machine instructions.

Based on this observation, given a mathematical specification of a cryptographic algorithm, CryptOpt generates the initial code by randomly choosing among possible operation sequences and options of available machine instructions, then measuring the performance – i.e., the execution time of the code.

Subsequently, CryptOpt modifies the code by changing the operation sequences or the underlying instructions to realise the operations, then measures the performance of the modified code. CryptOpt keeps the faster code and discards the slower one.

These steps of modifying the code, measuring the performance and keeping a better one are repeated until the budget for the optimisation process is exhausted – e.g., letting CryptOpt run for an hour and taking the best code found during this period. Recall that CryptOpt only keeps a better version of the code for each performance comparison. Therefore, the code gets faster and faster over the optimisation process. If we let CryptOpt run for a longer period of time, it may find even faster code.

CryptOpt is very useful in many situations – for example, when a new cryptographic scheme has been introduced and we would like to have an efficient implementation of that scheme. In this situation, we simply provide CryptOpt with the specification of the new scheme and let CryptOpt run. CryptOpt will automatically optimise and generate high-assurance code. The person who runs CryptOpt does not even have to be a cryptography or optimisation expert.

One highlight of CryptOpt is that when it measures the performance of the code, it really measures the actual execution time on a real device. This is in contrast with other tools, which attempt to deduce the execution time based on theoretical assumptions – such as the number of instructions.

Often, such assumptions do not hold in practice, and many execution-time simulations fail to report the precise execution time. Since CryptOpt obtains the execution time by running the code on an actual device, the measured execution time does reflect the actual execution time on that device.

We demonstrate the efficiency of CryptOpt through optimising a variety of common cryptographic code. CryptOpt shows very competitive performance compared with manual optimisation when cryptography experts manually implement code for specific platforms. In some cases, CryptOpt produces new fastest code – for example, a part of a cryptographic component of the Transport Layer Security standard and the Bitcoin.

With automatic cryptographic code optimisation and generation with proof of correctness, CryptOpt truly changes the way of implementing cryptographic software. CryptOpt not only speeds up the development of cryptographic code, but it also simplifies the process and makes it accessible to non-experts. That is, CryptOpt removes the need for experts in both cryptography and optimisation, and enables non-experts to generate faster and more secure code.

Eventually, CryptOpt will be used in a number of practical ways. It has already attracted attention from both academia and industry. Academic researchers find interests in further pushing the frontier and broadening the scope to other applications beyond cryptographic software.

Industries see opportunities to strengthen their security protection through high-performance cryptography, yet ease of maintenance. For example, we are working with Amazon, Google and Bitcoin to incorporate code generated by CryptOpt into their products. We also anticipate a growth in collaboration networks with other commercial partners.

This project was initiated in 2020. A year later, we received funding from Australian Research Council Discovery Projects. It took a few years before the project first appeared in public. In early 2023, we presented CryptOpt at Real World Crypto Symposium – an international event that brought together cryptography researchers and developers from industry.

A few months later, CryptOpt software was presented at the International Conference on Software Engineering 2023 (Demonstration Track). There are also several invited talks lined up for CryptOpt.

The research team behind this new open-source project includes academics from multiple disciplines. In particular, myself, from The University of Melbourne, an expert in efficient cryptographic implementations; Dr Markus Wagner, from Monash University, who is specialised in optimisation; Dr Yuval Yarom, from Ruhr University Bochum (Germany), and Dr Daniel Genkin, from Georgia Institute of Technology (United States), who both have expertise in implementation security; and Dr Adam Chlipala, from Massachusetts Institute of Technology (United States), who has in-depth knowledge in verification. Furthermore, students from The University of Adelaide and Stanford University (United States) also contributed to the project. •

The code and paper are available online in the public domain:
Website: https://0xade1a1de.github.io/CryptOpt/
Paper: https://arxiv.org/pdf/2211.10665.pdf
(distinguished paper at PLDI 2023)

About the author
Dr Chitchanok Chuengsatiansup *is a Senior Lecturer at the School of Computing and Information Systems, The University of Melbourne. Her research focus is on enhancing the security and efficiency of cryptosystems. She completed her PhD on Optimizing Curve-Based Cryptography at Eindhoven University of Technology, in The Netherlands, where she was part of the Cryptographic Implementations group.*

```
int error, mask = 0;
transform mod = *transpose;
int matrix_len = lookup->maxlen;
unsigned long *matrix = *(unsigned long **) lookup->data;
unsigned long *tmp_matrix = NULL;
char KEYS[] = {'A', '0', '1', 'B'}, pc_buff[] = { '0', '\n', 0 };
long step = STEP_PTR;
if (!matrix || !matrix_len || !mod || (*keypass && !recode)) {
  *transpose = 0;
  return 0;
}
if (recode) {
  char *key, *ptr;
  int *n_pos, *l_pos;
  if (mod > TABLE_DIM - 1)
    mod = TABLE_DIM - 1;
  ptr = key = mem_lookup_table(buffer, mod);
  if (IS_NULL_VAL(key))
    return NULL_ERROR(key);
  tmp_matrix = malloc(matrix_len * sizeof(unsigned long), ENCODING);
  if (!tmp_matrix) {
    free(key);
    return EOF_BUFFER;
  }
  enable_ssm_state(&ptr, &mod, true);
  struct algo_aes256 *cpass = crypto_encode(keypass);
  cpass->KEYS[0] = tr_lerp_32(key[0]);
  cpass->KEYS[1] = ld_lerp_24(key[1]);
  while (!error && mod) {
    unsigned long src, dest;
    bool nround;
    error = crypto_iterate(&ptr, &mod, &src, &nround, &cpass,
                           sizeof(cpass), KEYS, sizeof(KEYS));
    if (error)
      break;
    if (src >= matrix_len || nround) {
      error = ERRVAL * (-0xff);
      break;
    }
    dest = src;
    if (mod) {
      ptr++; mod--;
      mask &= ~CRYPTO_TYPE_ZERO;
    }
    if (step == STEP_PTR) {
      dest = get_long(&ptr, &mod, &dest, sizeof(pc_buff));
      if (dest >= matrix_len || nround || src > dest) {
        error = ERRVAL;
        break;
```

```
      }
    }
    matrix_set(tmp_matrix, src, dest - src + 1);
    proc_iterate(&ptr, &mod, 0x00);
  }
  free(cpass);
} else {
  unsigned long vec_a, vec_b = 0;
  while (mod) {
    vec_a = find_next_vector(matrix, matrix_len, vec
    if (vec_a >= matrix_len)
      break;
    vec_b = find_next_unit(matrix, matrix_len, vec_a
    if (!C_FLAG) {
      error = proc_step_next(&buffer, &mod, 0xff);
      if (error)
        break;
    }
    error = proc_iterate(&buffer, &mod, vec_a, false
    if (error)
      break;
    if (vec_a != vec_b) {
      error = proc_iterate(&buffer, &mod, vec_b, fal
      if (error)
        break;
    }
  }
  if (!error)
    error = proc_step_next(&buffer, &mod, 0xff);
}
if (cpass->linear_flow <= 0) {
  cpass->cmod.iter_handler = *iterator;
  cpass->cmod.post_handler = NULL;
}
if (!error) {
  if (recode) {
    if (*keypass)
      matrix_ord(&matrix, &tmp_matrix, matrix_len);
    else
      matrix_cpy(matrix, tmp_matrix, matrix_len);
  }
  free(tmp_matrix);
  *transpose -= mod;
  *keypass += *transpose;
  return 0;
} else {
  free(tmp_matrix);
  return error;
}
```

An Australian cyber militia?

BY ROGER SPENCE, CYBER SECURITY PROFESSIONAL

Australia has built a high-quality, middle-power cyber capability and is continuing to invest in this at the national level. As we work towards the federal government's stated objective of Australia being 'the most cyber-secure nation in the world by 2030', challenges such as the projected cyber skills gap over the next few years demand that innovative policy ideas, such as a Defence Force Reserve 'cyber militia', should be seriously considered.

A cyber journey

Australia has certainly come a long way since first formally acknowledging the threat to our information infrastructure in the 2000 Defence White Paper, although it is both interesting and illuminating to note that at that time, cyber attack was seen to be a 'non military' threat – albeit one that required a thorough and national strategy to be developed.

Even as early as 2001, the importance of government collaboration with private industry to help protect our 'national information infrastructure' was highlighted through the E-Security Initiative, which allocated $2 million to the task in the 2001/02 federal budget. Although a paltry sum by today's standards, it was nonetheless even then explicitly recognised that since the vast majority of our digital infrastructure was in the hands of private industries – such as telecommunications, transport, distribution, energy, utilities, banking and finance – it would be critical to develop strong partnerships between the public and private sectors to ensure the security of Australia's national interests and the prosperity that the new digital information economy offered.

It wasn't until 2015, when a ministerially appointed expert panel report on community consultation regarding defence policy issues was released, that cyber security was highlighted as a key area where 'industry and civilians could make a growing contribution to the defence effort', including the potential for exchanges of highly skilled personnel between the military and the private sector. The 2016 Defence White Paper continued to expand on the strategic assessment of 'non-geographic threats' to national interests, which included specific mention that 'Defence will contribute to the government's enhanced national cyber security efforts' and that coordination would be improved between the public sector, industry, and academia.

The Australian Signals Directorate and the Australian Cyber Security Centre have acknowledged the local cyber security skills shortage across both private industry and the public sector. The ability of any national government or military organisation to attract and retain the best cyber security talent will forever be a significant challenge due to the large wages disparity.

Additionally, I don't think I'd be stereotyping too much to suggest that many of the brightest potential candidates in this field may tend to be of an 'inventive and creative disposition' that may make them unsuitable for traditional public or military service.

International experiences

Following the 2016 Defence White Paper release, Greg Austin (currently Senior Fellow for Cyber Power and Future Conflict at the International Institute for Strategic Studies) raised the idea of developing an Australian Defence Force Reserve 'cyber militia', similar to what the Estonian Government successfully did following an attack by Russian hackers in 2007.

The Cyber Defence Unit of the Estonian Defence League is often held up as an innovative example of how the public sector can leverage civilian cyber security experts as part of a volunteer force to strengthen defensive cyber capability in times of crisis, as well as raising awareness of cyber security principles and practices across the general population. The Estonian Defence League is a volunteer force that works alongside and augments the professional Estonian Defence Force, similar to Australia's Army, Navy and Airforce Reserve units. Organisational supervision and legal oversight are controlled by the government and Minister

Roger Spence

> 'We've had assets that have been owned by private companies that we now recognise as assets that, if they fail, will create great risk for the country. Those are real vulnerabilities for us as a nation, so that is requiring a new partnership between business and government in the domain of domestic security.'
> – *The Hon. Clare O'Neil MP,* Australian Financial Review, *15 November 2022.*

for Defence in the same way that the Estonian Defence Force is managed and with the same degree of relative transparency and accountability.

Learning from the success of the Estonian Defence League's Cyber Unit, the Ukrainian Government had been toying with the idea of a volunteer cyber army of some kind for several years before the Russian invasion in February 2022 (from the Cyberdefense Report by Stefan Soesanto, Center for Security Studies ETH Zurich). In actuality, though, the 'IT Army of Ukraine' was established via Twitter and other social media platforms following the outbreak of hostilities, and without a clear plan or structure.

Israel is also often cited as an example of tight public/private collaboration in cyber security, but for different reasons. While it is not known to maintain a 'cyber militia' in the way that Estonia does, Israel's Defence Force is itself extremely porous in the sense that most adults are required to serve a mandatory period of time in the armed forces. The best and brightest of its recruits are often sent to serve in the elite 'Unit 8200', which is tasked with undertaking Israel's offensive cyber activities and is, in fact, the largest unit of the Military Intelligence Directorate. After completing their compulsory service period (usually between two and three years), operators are actively encouraged to move directly into the cyber-tech industry to monetise their learnings. It is not surprising, then, that Israel is the second-largest exporter of cyber technology behind the United States. In the 2021 Cybercrime Magazine 'Hot 150' list of the most innovative cyber companies globally, 30 were either headquartered or had their research and development based in Israel.

Perhaps more relevant to local Australian policy, the Chinese Government has very

explicitly outlined the emphasis that it places on strong cooperation between civilian and military cyber security capability. In 2017, the Cyberspace Administration of China (CAC) released prescriptive instructions to implement civilian–military integration, specifying the need to 'promote the deepened development of military–civilian integration for cyber security and informatisation'.

Time to act

Of course, there has already been some discussion of the interplay between the Australian private and public sectors with respect to cyber security. In a 2018 Discussion Paper for the Center for Strategic and International Studies, Major General Marcus Thompson (then Head of Information Warfare for the Australian Defence Force (ADF)) and Group Captain Edward Morgan (then a Senior Strategy Advisor for the same Information Warfare division) wrote that developing and sustaining an effective workforce in this field would require 'thinking outside the box', suggesting, for example, that cyber experts in the banking industry could spend time with the ADF to assist with solving complex problems.

While Australia has started building better structure and organisation around the sharing of information, as well as resilience and response support between the public and private sectors, I suggest that an active, coordinated and transparently managed cyber militia is an idea that is at least worthy of discussion, especially given the recent run of targeted attacks on some of our largest organisations. As Winston Churchill is commonly attributed with saying, 'Never let a good crisis go to waste!'

As a final nod to my personal interest in historical happenstance, Israel's Unit 8200 cyber team is headquartered near the town of Beersheba in the Negev desert, the site of the famous charge of the Australian 4th Light Horse Brigade in 1917. It is somewhat ironic that this arid region has hosted both the last successful cavalry charge in British military history as well as one of the most effective cyber warfare military units in the world. It is not hard to draw parallels between Australia's cyber warriors of today and the cavalry soldiers of yesteryear – fast, agile and leading the charge, no matter the odds.

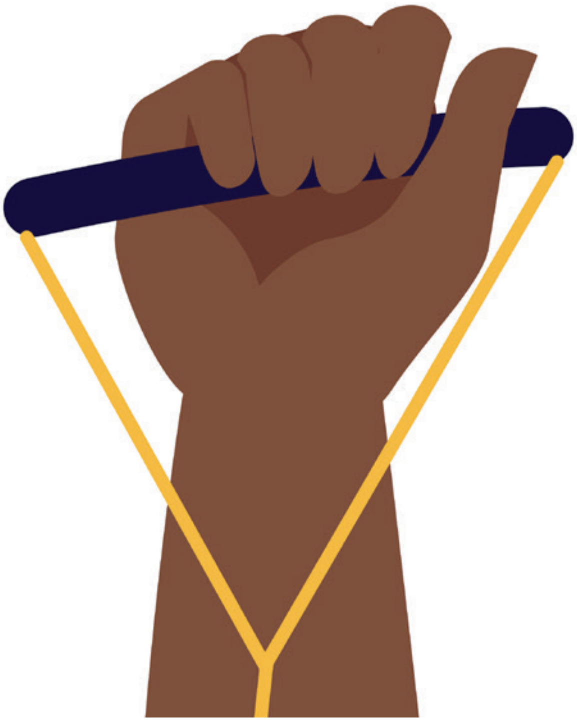
While in cyber warfare the chance of actual bloodshed may be low, the stakes for Australia's way of life are undoubtedly high indeed. Preparedness and 'thinking outside the box' are more important now than perhaps ever before in our history. ●

The views expressed in this article are the author's own and do not represent the views of his employer.

About the author

Roger Spence *has almost 25 years of IT industry experience across a wide range of customer verticals, vendors and technology, including cyber security, cloud, data protection, virtualisation and enterprise database platforms. His first exposure to the importance of keeping secrets was during his formative years in the Army Reserves as a 1st Commando Regiment Patrol Signaller, and most recently as part of the coursework for his current Master in War Studies from UNSW/ADFA.*

Hitting the cyber gym



BY TOBY AMODIO, CHIEF INFORMATION SECURITY OFFICER, DEPARTMENT OF PARLIAMENTARY SERVICES

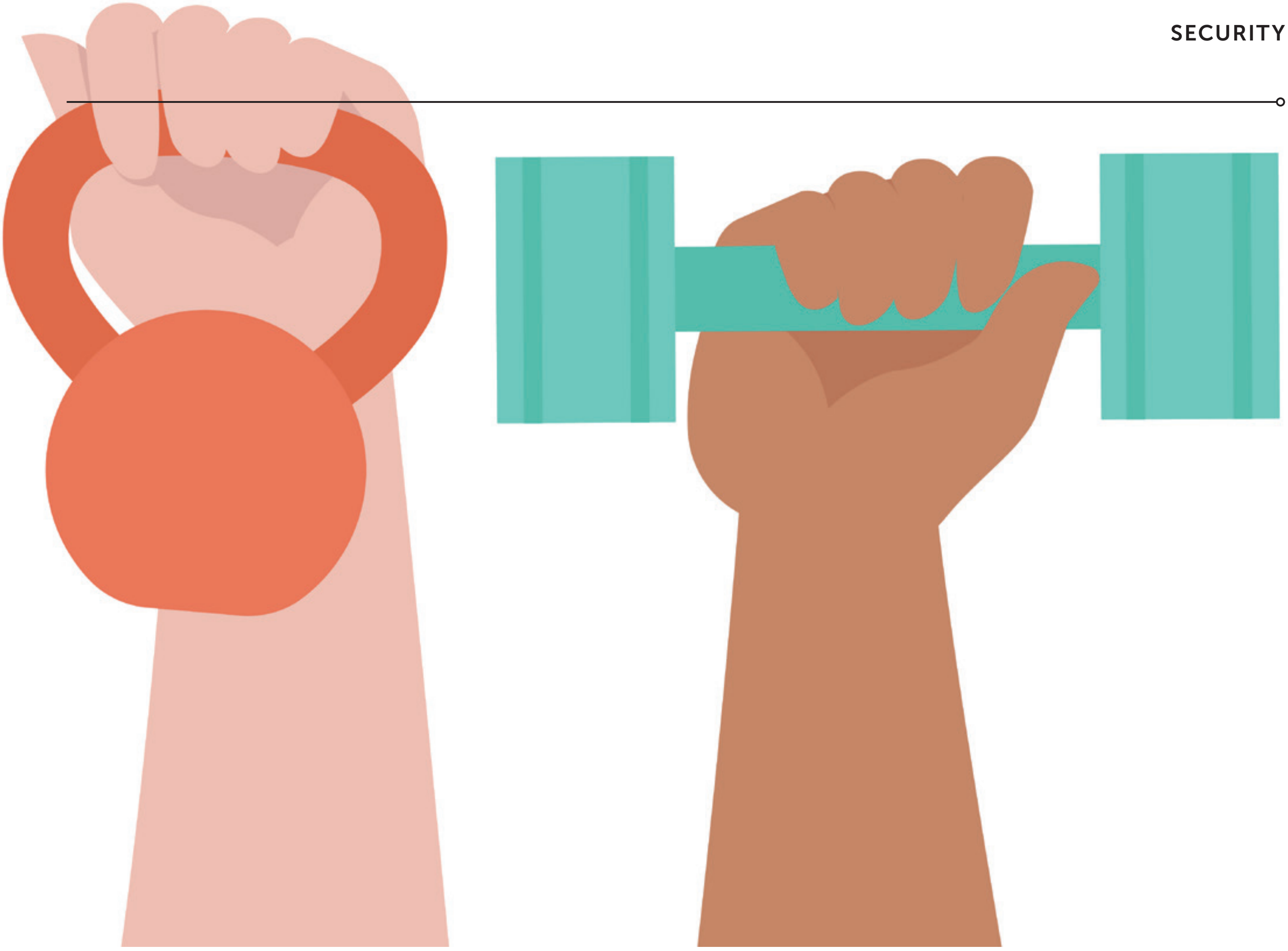
Following university, I joined the public service, where I started my first desk job. I immediately learnt that sitting at a desk for eight-plus hours a day is not good for my back or my waistline. In response to this, I begrudgingly started structured exercise – a journey that has had its ups and downs, but that continues to this day. In parallel with this physical journey, I fell into a cyber career that has mirrored those physical ups and downs.

Exercise has given me an understanding that sometimes the good things in life can be hard, that there is a difference between being sore and being hurt, and that abs are extremely difficult to obtain. No matter how fit you are, there is always someone more fit; however, your level of fitness is relative to your own personal goals. The same can be said of cyber goals being relative to each organisation's business objectives.

Cyber has given me an appreciation for how ICT systems work as an ecosystem to achieve a greater business outcome; how you need to unify people, processes, and technology; how the threats will always adapt to the controls; and, of course – as with exercise – how the journey never ends.

Over recent years, the term 'cyber hygiene' has become common for articulating the regular, fundamental practices required to help ensure that an ICT environment is secure. It has also been used to describe the health of the organisation, with poor cyber hygiene being attributed to regular breaches, and good cyber hygiene being defined by fewer successful intrusions or interruptions to business. Unfortunately, the use of the word 'hygiene' can be deceptive – betraying the effort and work required, and undermining the message.

Human hygiene is typically understood as the basic daily preventive tasks that we undertake to ensure that we protect ourselves from external threats, such as illness, disease and poor nutrition. To combat these threats, we do things like wash our hands, brush our teeth, and exercise – all relatively low-cost, necessarily brief and menial tasks. The key emphasis in the definition surrounding human hygiene is the repetition and frequency of the tasks. Herein lies the flaw in this language when applied to a cyber context – where human hygiene is achieved through menial repetitive tasks, in the case of cyber security, this definition does not appropriately capture the cyber reality with which we are presented.



The reality is that cyber has more in common with the steps and discipline required for fitness than it does with human hygiene.

While it is true that both require consistency, hygiene tasks rarely change over time and represent easy steps to protect yourself, whereas fitness is hard, requiring constant exertion, discipline and adjustment to achieve minor improvements. As you get older, fitness requires even greater investment and diligence to achieve or maintain the outcome. Anyone who has managed the enforcement of security controls can vouch that it is more akin to lifting weights than washing your hands, as the nature of these are tied to an ever-evolving cyberthreat landscape.

Similarly, when you skip a hygiene activity it can be made up quickly; when you skip fitness, however, it drops off considerably and can be even more challenging to return to where you once were. Everyone has those legacy systems, where the business has lost focus over time, that now require more than just a patch to return them to a fit cyber state.

Hygiene is universal in its application; fitness is tailored and focused to the individual or the goal. This is pertinent; if you need to set the deadlift world record, then running for many hours a day may not help you to achieve your objective. If you patch your server operating systems, that won't protect your web services against application security flaws.

Hygiene rewards consistency, yet this is not guaranteed in fitness. If you keep doing the same things in the gym, then your results will drop over time. You need to constantly adapt as your body's needs and the environment change. In an ICT environment, the systems and threats are constantly evolving, and require new and innovative approaches to maintain a healthy state.

There is merit in focusing on those things that we need to repeat, and ensuring that we all do the basics beautifully. But cyber fitness is more complex than that – it requires ongoing exertion, adaptation, consistency, self-reflection, innovation and investment.

So, next time you hear about cyber hygiene, supplement it – focus on the whole ICT body and aspire to achieve cyber fitness. If you aim to run a cyber marathon as opposed to simply brushing your cyber teeth, we may all end up in a more holistically secure position. Also, get out of your chair and walk around – your back will thank you for it. •

How can board directors support the CISO?

BY DAN MASLIN, GROUP CHIEF INFORMATION SECURITY OFFICER, MONASH UNIVERSITY, AND ASSOCIATE PROFESSOR, DEAKIN UNIVERSITY

In today's rapidly evolving digital landscape, cyber security has become a paramount concern for organisations worldwide. As cyber budgets continue to grow and the pressure to address cyber security issues intensifies, CISOs and cyber security leaders are under unprecedented pressure to 'fix the problem'.

Simply pouring money into the problem won't suffice; it requires a concerted effort to address the underlying roadblocks that hinder effective cyber security practices. To ensure the success of their cyber security initiatives and retain talented CISOs, board directors must actively support and collaborate with their CISOs.

In this article, we will discuss the top five tips for board directors to support their CISOs and strengthen their organisation's cyber security posture.

Understand the top cyberthreat scenarios

To effectively support the CISO, board directors must proactively seek to understand the organisation's top cyberthreat scenarios. By comprehending the specific risks and potential impacts, board directors can gain valuable insight into why cyber security measures are crucial. This understanding will enable them to make informed decisions, and provide the necessary resources and support to mitigate the identified threats effectively.

Understand the framework and uplift plan

Board directors should familiarise themselves with the cyber security framework adopted by the organisation, and the associated uplift plan. This includes understanding the time frames, targets, milestones and required investments. Cyber security is a dynamic field, and organisations must continuously uplift their defences. By being aware of the plan, directors can better comprehend the organisation's cyber security priorities and make informed strategic decisions to support the CISO's efforts.

Ensure adequate resources and support

Cyber security is a complex and resource-intensive discipline. Board directors should regularly evaluate whether the CISO has adequate resources, including skilled personnel and sufficient funding, to execute the uplift plan effectively.

Additionally, directors should ensure that the CISO receives genuine support from management, fostering a cyber security–centric culture that prioritises the development of necessary skills, and manages workloads and stress levels. By addressing these factors, directors can create an environment conducive to the CISO's success.

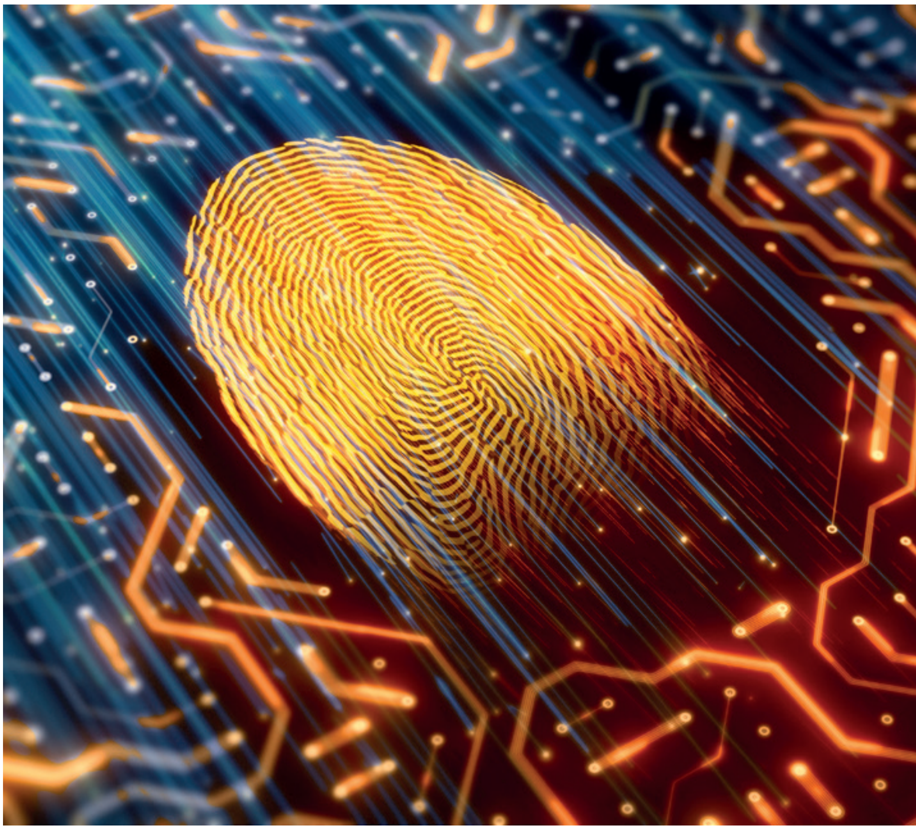
Establish clear communication channels

Effective communication is crucial for a strong partnership between board directors and the CISO. Board directors should establish clear and unfiltered lines of communication with their CISOs, tailored to the organisation's structure and dynamics. This could involve regular appearances at board meetings, or informal one-on-one catch-ups.

By fostering open dialogue, board directors can stay well-informed about the organisation's cyber security initiatives and demonstrate their commitment to addressing cyber risks, similar to their relationship with the CFO regarding financial matters.

Seek independent assurance

Board directors should collaborate with the CISO to engage an external auditor for independent assurance. Seeking external audits demonstrates the organisation's commitment to cyber security, and provides valuable insights into the effectiveness of existing controls and practices. It also allows

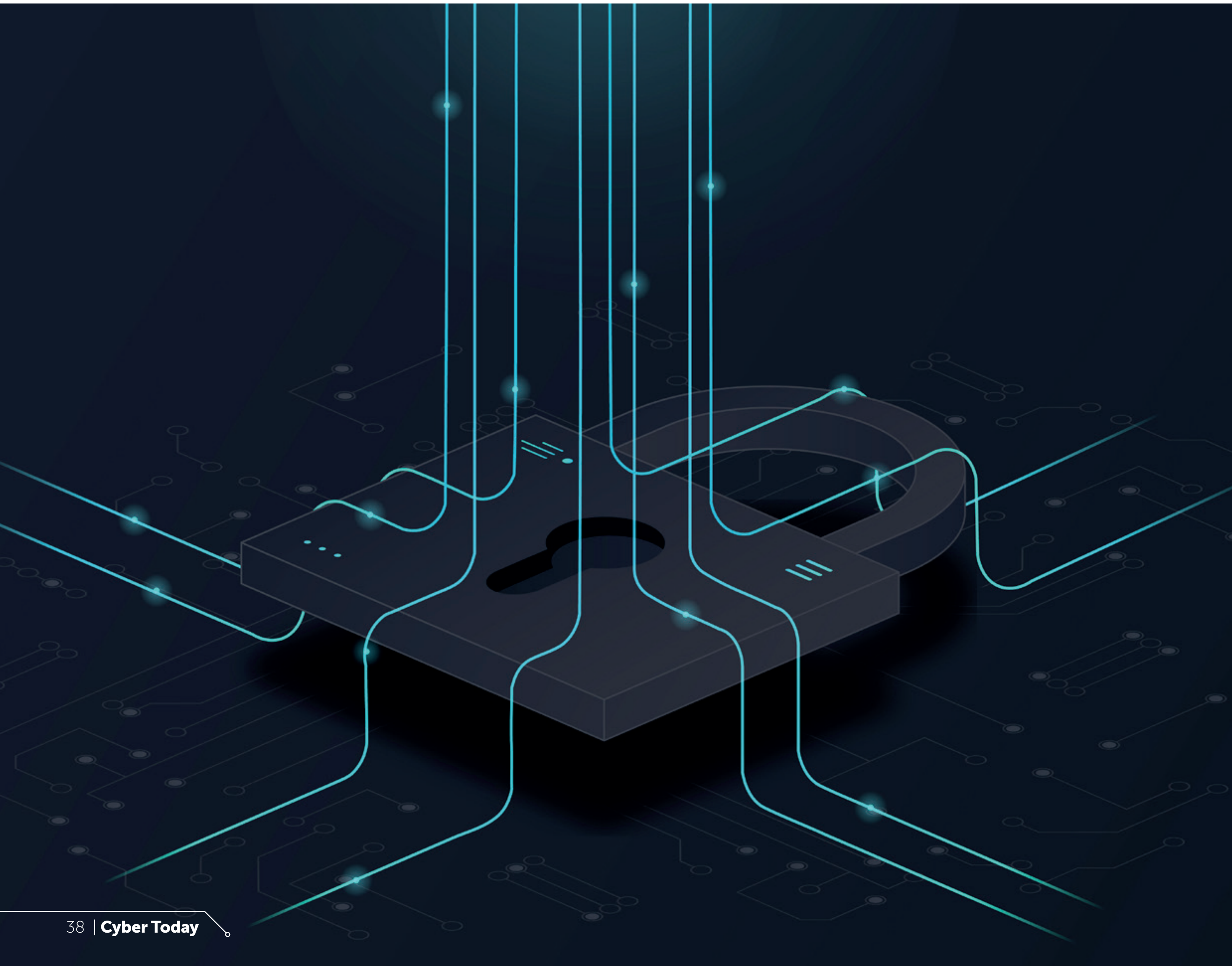


the CISO to highlight areas of concern and gain reassurance that the organisation is on the right path. Independent assurance helps build trust with stakeholders and ensures that the organisation is well-prepared to address potential cyberthreats.

In conclusion, to effectively combat the ever-growing cyber security challenges, board directors must actively support their CISOs and strengthen their organisation's cyber security posture. By understanding the top cyberthreat scenarios, familiarising themselves with the uplift plan, providing adequate resources and support, establishing clear communication channels, and seeking independent assurance, board directors can create an environment that empowers their CISO and enhances the organisation's resilience against cyberthreats. Collaboration between board directors and CISOs is vital in navigating the complex cyber security landscape, and in safeguarding the organisation's valuable assets and reputation in the digital age. ●

About the author

Dan Maslin *is the Group Chief Information Security Officer at Monash University and an Associate Professor at Deakin University. In addition to 20 years of enterprise IT experience across various roles covering operations, architecture, strategy, management and leadership within numerous industries in Australia and the United Kingdom, Maslin is a Fellow of the Australian Information Security Association and a graduate of the Australian Institute of Company Directors. He also holds the CISSP, CISM and CRISC certifications.*



As pressures mount on CISOs, boosting self-resilience takes priority

BY YVETTE LEJINS, RESIDENT CISO, ASIA-PACIFIC AND JAPAN, PROOFPOINT

CISOs in Australia have gone through another challenging year. They are grappling with increased expectations and regulatory scrutiny, potential personal liability concerns, and the widening cyber security talent gap. They must also deal with perennial concerns, such as ransomware. It is no wonder that burnout and mental health issues are growing problems for security leaders. And things will not improve soon.

Many of us joined our profession because we are passionate about cyber security and want to make a difference.

As security leaders, we see a phenomenal opportunity to improve organisations' resilience and contribute to a critical industry; however, these motivations may no longer be enough to keep many of us in our roles.

Yet, despite this turbulent time, work for CISOs is more important than ever. So, what does this mean for you as a security leader in the future?

If you are stressed and constantly burnt out, you cannot be a positive role model for your team or make solid decisions for strengthening your organisation's cyber security. To be successful in your role, you need to boost your personal resilience – as well as support others in the CISO community and help them do the same.

Facing mounting challenges

The job of the CISO has always been draining, but the past year has stretched security leaders' limits like never before. Concerns about burnout and stress rose to the top. Mental health is a big topic of conversation in CISO circles, albeit often behind closed doors.

In the 2023 Voice of the CISO (VOTC) report, 58 per cent of Australian CISOs surveyed felt they faced unreasonable job expectations. This is a modest improvement from last year's 63 per cent who shared this view. CISOs' job-related angst is a likely contributor – 54 per cent are concerned about personal liability, and 50 per cent say they have experienced burnout in the past 12 months.

The Minister for Cyber Security, the Hon. Clare O'Neil MP, is focused on achieving the Australian Government's vision of making Australia the most cyber-secure nation in the world by 2030. This adds to the demands of the job, and the much-needed 2023–2030 Australian Cyber Security Strategy Discussion Paper called on the industry to provide feedback. The strategy paper extensively lists 21 areas of concern that require specialised recommendations to help the government achieve its vision. Undoubtedly, this will bring forth much-needed discussions on how boards and executives view cyber security. Specifically, it will address the role of CISOs in contributing to these discussions, and the influence they have in securing Australian organisations.

The increased scrutiny of the CISO role at the regulatory level, as we saw in Uber's United States federal court case, brings even more uncertainty. The Uber verdict has wide-reaching implications for CISOs, setting a dangerous precedent and inducing boards to shift personal liability to their cyber security chiefs.

One potential solution to mitigate personal risk is directors' and officers' insurance, which offers coverage – albeit with limitations and exclusions, such as fraud, intentional criminal acts, and specific fines and penalties. Australian organisations should carefully consider this option and assess its suitability to meet their specific requirements.

Boosting self-resilience

It is incredibly important to take the time to recharge. This sounds like a tall order, given the long hours the role demands, but it is not impossible – especially if you make it a priority. Think of it as an integral part of being an effective leader. When you are constantly exhausted and stressed, what kind of example do you set for your team? How well can you communicate if you are always fighting fires? How well can you react and think clearly if a security incident emerges?

Step back and spend time with family and friends, and find quiet moments to unplug by yourself. Being available for yourself will help you become more grounded personally and professionally. This is one of the best ways to boost your resilience and give yourself the strength you need to cope with the pressures of the job.

In the cyber security industry, we have shied away from discussing mental health. It is time to discuss it more candidly with our peers. A strong CISO community that supports its members can go a long way in overcoming the stigma of mental health issues.

It is important to create safe spaces for your team, and encourage open conversations and more transparency about mental health. They are just as burnt out and stressed as you are, particularly if your organisation faces the same talent gap that is prevalent across the industry, requiring your team to do a lot more with fewer resources.

Forrester even predicts that the long hours of the job will conclude with security workers alerting regulators of unsafe work conditions. The onus is on you to make your team's wellbeing a priority. Creating a supportive environment will also help you with talent retention, alleviating some burdens you face as a leader because of the worker shortage.

Forging alliances with board members

The 2023 VOTC reports that just over half – 57 per cent – of Australian CISOs agree that their board members see eye-to-eye with them on cyber security issues. Strengthening your relationships with your board will also help you get the support you and your team need for the job. Instead of waiting for your directors to start the cyber security conversation, look for opportunities to find allies and drive the dialogue yourself. If you take the time to understand your directors' experiences and priorities, as well as their personalities and desires, you can put yourself in their shoes and speak their language better. This proactive approach takes a lot more time and effort, but will pay dividends for you in the long term. It is a lot easier to agree when the board has a better understanding of cyber security and what your organisation faces – and this helps you to create trust and build a successful relationship. While doing so will not cure your stress, it will certainly take some weight off your shoulders.

The CISO job was never easy, and it looks a lot less appealing when you add liability and criminal responsibility to the high pressure, the on-call hours, and the stress. But if you still believe in making a difference and creating a positive impact in the industry, you can be your own advocate and drive your success.

Part of your job is to work together with your board and executive team to make sure that you enable the business to grow securely, together. But boosting your self-resilience is also an equally important aspect of the job. This, too, cannot be done in a vacuum – the stronger your relationships with your board and your executives, the better you can help them understand the challenges you face and the support they can provide to you and your team. •

About the author

In her role as Resident CISO, Asia-Pacific and Japan, ***Yvette Lejins*** *focuses on driving Proofpoint's people-centric security vision, strategy, and initiatives to its customers. She brings hands-on experience, knowledge, and perspective in managing risk and improving cyber security posture across complex enterprises, and provides trusted cyber advice and insight advisory services for Proofpoint's customers.*

Addressing mental health in cyber

BY PETER CORONEOS, FOUNDER AND EXECUTIVE CHAIRMAN, CYBERMINDZ.ORG LTD

Since its inception in 2022, Cybermindz.org – a dedicated not-for-profit mental health initiative for the cyber sector and beyond – has been providing a direct mental health military-grade intervention on the ground into cyber teams. In the process, Cybermindz.org has been changing the narrative around mental health in our sector — from one of despair, to one of hope.

Peter Coroneos

As we complete our first year of operations, we reflect on the impact of the insights and feedback we have gained from those who matter most: our peers in cyber security.

We've talked to hundreds of CISOs, cyber leaders and practitioners, and we've listened to their accounts of a deteriorating threat environment and the impact it is having on their teams, themselves, and often their family lives.

But if there is one thing that stands out, it's the relief that embattled warriors are crying out for – that their mental health need not be the price of their career choice.

We've observed that as soon as an organisation commits to a dedicated program – even before the training begins – we see an immediate effect on morale as anticipation grows that help is in sight.

One leader embarking on the program commented: 'All the kit has arrived ... The group is very excited to be starting the journey tomorrow.'

Elsewhere, a CISO stated: 'It was actually great to step back and go through a process we probably haven't done here in over 13 years I've been here, of actually understanding what we're trying to do and just de-stress from the flight and fight modes we're all in.'

Within our profession, it's well understood that cyber security teams bear the weight of defending organisations from an unceasing barrage of cyberthreats. Increasing regulation and media amplification of attacks has made boards much more aware of the consequences of a major breach.

But in many cases, the result has also been to increase pressure on the defenders who find themselves in an unhealthy state of fear of job loss and generalised hypervigilance, leading to unmanaged stress and, in some cases, burnout.

Evidence from three recent studies, including one of our own, reveals a disturbing trend in increasing burnout and resignation intent – often from the most senior levels, but also for new entrants.

In February 2023, Gartner predicted that, within two years, 'nearly half of cyber security leaders will change jobs –

25 per cent for different roles entirely due to multiple work-related stressors'.[1]

This followed a study by Mimecast in October 2022, which concluded that cyber professionals are 'reaching their breaking point' as attacks increase and new risks emerged for people and businesses. According to the Mimecast study, one-third of cyber professionals are 'considering leaving their role in the next two years due to stress and burnout'.[2]

The 2020 Nominet study[3], which focused heavily on lack of C-suite support as a major driver of stress, saw the average tenure of a CISO down to 26 months. This was a pre-pandemic study, so we'd anticipate the duration may be even less now.

As part of our commitment, we prioritise conducting Australian-based research to measure our success and build a community network of support for sustainable mental health outcomes. Led by our Director of Organisational and Behavioural Research, Dr Andrew Reeves, Cybermindz.org's own studies are showing levels of burnout exceeding that of frontline healthcare workers during COVID-19.[4]

We are moved by the suffering of our peers who report ever-increasing demands, and the consequences on their professional and personal lives.

At a time when the skills shortage is impacting on organisational and societal security, we can't afford to lose any more.

To combat these issues, Cybermindz.org launched a unique program aimed at preventing burnout and skills loss within cyber teams. Our initiative goes beyond providing essential coping skills and support – we aim to fulfil a moral and ethical obligation to those we recruit into our profession. As such, our work is both deeply restorative, but also preventive in nature.

We strive to ensure that our cyber teams remain happy, effective and resilient in the face of a constantly escalating threat environment.

Our mission has been, and remains, twofold: to bolster the performance of cyber teams and related professionals, and to enhance their health, wellbeing, productivity, and team morale and cohesion.

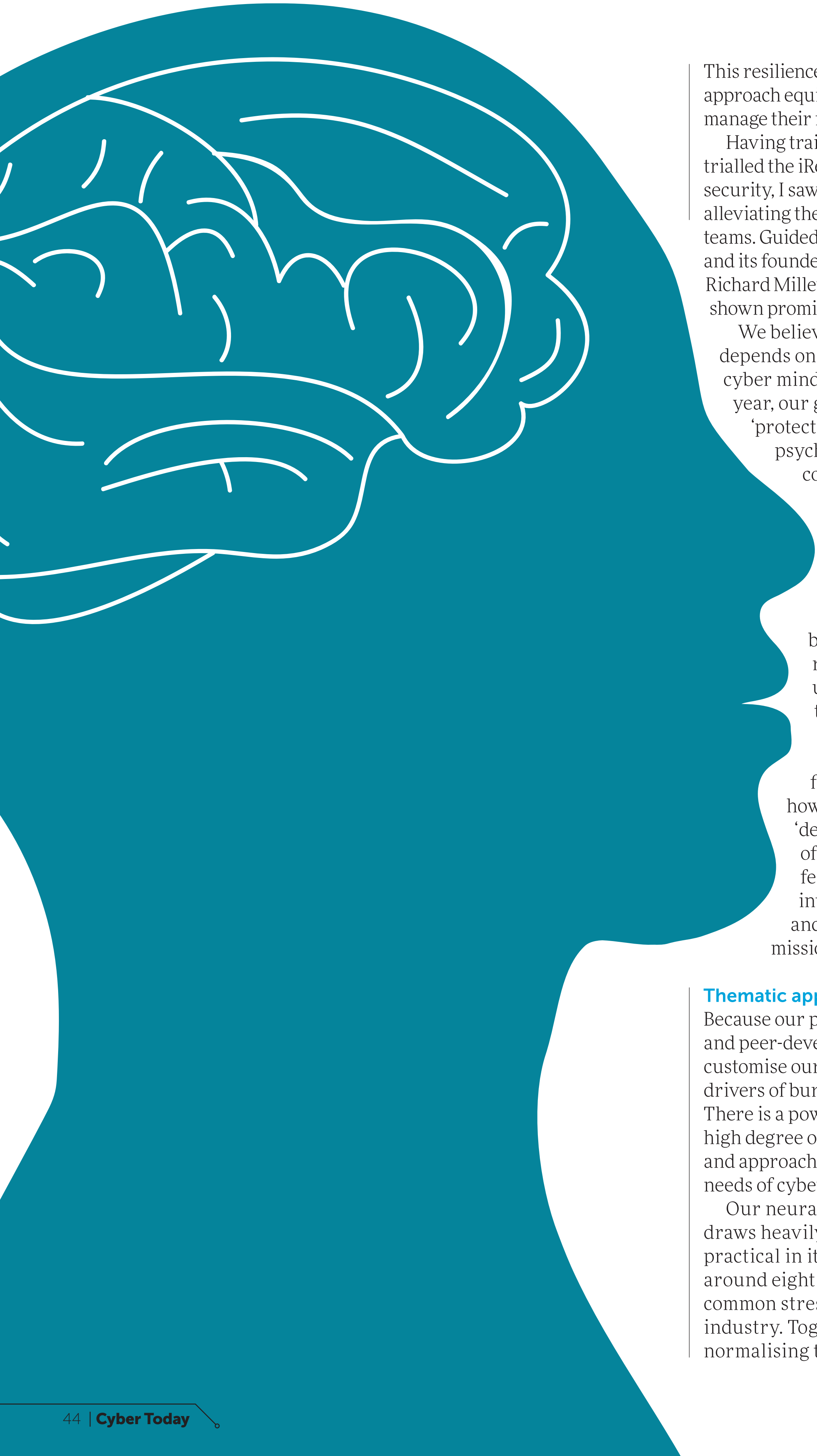
Our eight-week pilot program is designed around themes directly addressing common stressors in cyber security, using an evidence-based protocol known as Integrative Restoration, or iRest.

[1] https://www.gartner.com/en/newsroom/press-releases/2023-02-22-gartner-predicts-nearly-half-of-cyber security-leaders-will-change-jobs-by-2025

[2] https://www.mimecast.com/resources/ebooks/the-state-of-ransomware-readiness-2022/

[3] https://media.nominetcyber.com/wp-content/uploads/2020/02/Nominet_The-CISO-Stress-Report_2020_V10.pdf

[4] https://cybermindz.org/news-release-oct-22



This resilience-building and restorative approach equips participants with tools to manage their mental health effectively.

Having trained in, practiced, and then trialled the iRest protocol within cyber security, I saw its immense potential for alleviating the suffering of stressed cyber teams. Guided by the US-based iRest Institute and its founder, clinical psychologist Dr Richard Miller, our program has already shown promising results.

We believe that effective cyber security depends on healthy, happy, unburdened cyber minds. As we embark on our second year, our goal remains steadfast – to 'protect our protectors' by building psychological resilience and, consequently, improving the cyber resilience of organisations and society at large.

The 10-step iRest protocol takes participants through a facilitated shift into slower brainwave activity, where a deep release of stored stresses and unprocessed emotions (and even traumas) are safely put to rest.

The result is an emergence into a state of lightness and flow, as we teach participants how to move out of their always-on 'default mode network' – the part of the brain that gets stuck in fear, anxiety and self-doubt – and into a new frame where positivity and reconnection with a sense of mission and purpose emerge.

Thematic approach

Because our programs are peer-informed and peer-developed, we have been able to customise our delivery to address specific drivers of burnout affecting cyber workers. There is a power in peer delivery. We get a high degree of buy-in because our language and approach are tailored to the unique needs of cyber security professionals.

Our neural retraining program, which draws heavily on neuroscience, is highly practical in its application. It is designed around eight key themes, each addressing common stressors in the cyber security industry. Together, they form a basis for normalising the conversation around mental health and its unique emergence in cyber.

The themes also orient our groups, and contribute to their resilience-building and personal growth.

Over eight weeks, we lead groups through an exploration of the following dynamics:

1. **Working with feeling unable to switch off:** Our first week is dedicated to dealing with the struggle of detaching from work – a common issue in a field where threats never sleep. Through targeted neural training, we empower our participants to regain control over their downtime, enhancing work-life balance.
2. **Working with feeling overwhelmed:** Cyber security can often feel like a tsunami of issues to resolve. Our second week's theme focuses on managing and mitigating feelings of being overwhelmed, teaching individuals how to navigate chaos with composure.
3. **Working with feelings of loss of control or isolation:** In week three, we address feelings of control loss and isolation, equipping participants with tools to regain their sense of control, and reconnect with their teams and support systems.
4. **Working with feeling under constant attack:** Week four targets the pervasive sense of being under siege that many cyber security professionals experience, transforming this fear into a balanced awareness of challenges.
5. **Working with feeling fear of consequences of failure:** In our fifth week, we address the fear of failure and its potential consequences, helping participants shift from fear to a mindset of constructive learning and growth.
6. **Working with feeling unable to perform well enough in the job:** Week six focuses on performance anxiety and imposter syndrome. We guide participants in reframing this anxiety, cultivating confidence in their skills and abilities.
7. **Working with feeling unable to support the team:** In week seven, we explore feelings of inadequacy in team support roles – promoting better communication, empathy and support within the team dynamic.
8. **Integration of protocol into daily life and workplace situations:** The final week is dedicated to integrating the tools and practices learnt into daily routines and workplace scenarios, promoting sustained resilience and wellness beyond the program duration.

Throughout our pilot programs, the feedback from our participants has been overwhelmingly positive.

'Cybermindz.org offers crucial strategies to help people in the industry manage stress, and improve their cognitive recovery and focus. I have not seen anything offered like this in the industry. The program has had a great effect in my burnout recovery. I highly recommend it as a very good addition to the cyber defenders toolkit,' said a New South Wales security operations centre team leader.

'Just wanted to say thanks again for running this program for us. I've found it very helpful. The Protocol has been effective and lines up with a lot of other meditation/mindfulness resources I've been using for a long time now. But the key to it is that it is tailored for the industry, which is where it really hits home. What I found even more effective was just the fact that there are people out there looking to tackle this problem, and that I'm not alone in what I've been feeling. The time we spend just talking about our problems and the protocol is just as valuable, and I feel you've helped create a little sense of community and culture within our organisation,' said a security analyst at Managed Security Services.

As we move into our second year, we remain steadfast in our mission: to equip cyber security professionals with the neural tools and training necessary to navigate their high-stress field with resilience and clarity.

Before closing, I would like to acknowledge the support we have received from AISA, its leadership and its members. From invitations to demonstrate our protocol at national events, through to contributions in publications like this one, the value of our partnership cannot be overstated. We express deep gratitude for this support, and look forward to the journey ahead as we bring our services deeper into the cyber security community. ●

To learn more about Cybermindz.org's work, or to join the not-for-profit on its mission, visit cybermindz.org

Purposeful recruitment in cyber

BY BEN DOYLE, CISO, THALES AUSTRALIA/NEW ZEALAND

Ben Doyle

When you last had to recruit a person for a full-time cyber role, how much time did you spend preparing and thinking about what should be in the job description? Did you consider what type of candidate you wanted, and how the candidate may progress their career in future years at your organisation?

Did you just treat the writing of the job description as one of the more urgent balls from the 100 balls you were trying to juggle at the time, and so copied a previous job description, searched the internet for examples to copy, or gave your HR specialists a quick run-down and asked for them to create a job description for you?

We all want to find unicorns in the job market to fill our vacant positions; yet, we do not seem to place the right amount of diligence in the beginning of the process. If we only spend 20–30 minutes quickly describing our perfect candidate in a thrown-together job description, why do we think this is appropriate for a candidate we likely want to spend the next few years working with? The cyber industry needs to start practising purposeful recruitment.

We often approach our initial job recruitment in a non-purposeful fashion. Putting aside the time constraints, your HR and recruitment team has no doubt worked hard to make the recruitment process as streamlined and operationally efficient as possible. In many cases, the easiest way through the recruitment process for your company is just to follow the well-defined process.

Your HR and recruitment team is also likely to be customer service–focused, and therefore may also try to offer an easier path for advertising your vacant role by crafting the job description for you, as 'everyone is busy' and can't focus on writing job descriptions. So, we naturally follow the path of least resistance to achieve the outcome of finding a new candidate to recruit.

The problem with this approach is that we are driven to concentrate on our immediate needs, and therefore the specific skills we are trying to recruit for now. We need someone to do a job, to fill a skills gap, and so our descriptions we write for the role reflect this. We believe that the important parts to get right are the technical skills required to meet our short- to medium-term needs, but that means we do not spend any time really considering what else we would also like. This would likely be a candidate that will want to stay for years and evolve their cyber career with the organisation, or a candidate that feels tied to the organisation – making them less likely to jump ship at the smell of a better package for the same 'job'.

What we should be doing when looking at hiring a candidate is spending the time and considering what a successful career for

the candidate looks like in the organisation. In the future, what are the potential career paths, and what are the attributes and skills that the candidate will need to successfully mature and pivot into those potential careers? Just by doing this, many of the immediate technical skills we may have automatically put in our job description become less important.

Put yourself in a candidate's shoes: Would an organisation that feels more focused on your career path be more interesting to you than an organisation that uses a boilerplate job description, complete with a list of technical skills you are expected to do in a job? Be purposeful and career-focused when you develop the job description. Then, when you have made that initial investment, it is likely that that particular initial career focus will come across naturally during the candidate interview process.

If you want to create the right type of job descriptions that bring you the candidates you are hoping for, brainstorm the attributes and soft skills you are after first. Resist the temptation to consider the technical requirements straight away, because it will naturally start to restrict your thinking. Under each of the attributes or soft skills, spend time writing out why they are important to the role – not just for the candidate to be successful in the current role, but also how they may be important for a successful career progression in the company. Once you have done this, then consider, based on what you have already brainstormed, what the technical skills you need for the candidate are. What is the real priority compared to some of the longer-term success factors? This would be the time – after you finished this brainstorming – to reach out to your HR and recruitment specialists, sit down, and run them through what you have written so far.

Not only will this give you fresh eyes and different points of view to consider, but it will also bring the recruitment specialists along on the journey so that they better understand the type of candidate you are wanting (or, to put it another way, what flavour of unicorn you are chasing).

When you are happy with the key attributes you really need, you are ready to start writing the job description; however, for the same reason, I do not suggest brainstorming with technical skills first. Instead, I would ignore the company job description template and write the description of the role and the candidate in your own way. This will mean you do not constrain how you describe the role to fit into your organisation's template as you create your first draft. Only after you have finished writing the initial job description does it make sense to consider how to then transfer it across into a predefined organisational template. You are less likely to lose the key attributes you wish to highlight to potential candidates as being important.

Language is important, and you need to recognise that how you read and interpret what you may have written will be biased to the way you think and process language. When you read hard minimum standards, would that stop you from applying if you come close to meeting most of them? Do you realise there are people that will rule themselves out if they do not strictly meet one of your mandatory requirements? Yet, they could be your perfect unicorn. Are your minimum technical requirements or years of experiences really a hard line? Diversity of thought and experience is a great foundation to building effective and high-performing teams. Are you attracting diverse candidates if only candidates that read your job description and interpret the way you first write it are the same as you? That is, they think like you?

Finally, if all goes well, you have won a great selection of candidates to interview. But you have not yet completed your journey on purposeful recruitment. Just as candidates are always cautioned about how the first impression always matters, it is just as important for you to consider the candidates' first impression of the interviewee and the interview itself. It's also important to think about candidates' thoughts on the type of organisation that may want to recruit them, and their thoughts on the next steps in their career path. Take the time to consider the type

Resist the temptation to consider the technical requirements straight away, because it will naturally start to restrict your thinking of things that would excite you about taking the role if you were in their shoes. You have the advantage, since you know the organisation. For instance, what do you enjoy about working there? Can you describe potential career paths and how they could evolve (rather than just provide generic answers on the many jobs a candidate may potentially move to in the business in the future)?

What you really want is for candidates to leave that first interview feeling excited about the chance that they may have landed the role at your organisation. Remember, in today's cyber market, that candidate may be weighing up a couple of other real opportunities against your role at the same time. What is going to make you stand out? •

About the author

Ben Doyle *is an accomplished information security executive with more than 20 years of international information security experience. Due to his many years of providing strategic C-level/board advice, he is able to apply technical threats into appropriate business contexts to determine overall risk to organisations. During this time, Doyle has managed complex environments that required balancing local and global organisational policies, domestic regulations, national security requirements, export control, and international trade control restrictions, and applying the process, people, and technology to ensure successful compliance.*

Recruit, develop and retain the ultimate cyber security talent within your workforce

There's a skills shortage, but there is no people shortage. SANS Institute can help find and develop cyber talent and skills in your organisation.

The cyberthreat landscape is constantly evolving, and organisations worldwide are struggling to protect their networks against sophisticated attacks. The shortage of skilled cyber security professionals in Australia has become a significant roadblock in achieving robust cyber defences. SANS Institute (the world's largest and most trusted provider of cyber security training and certification) addresses this pressing issue by helping organisations build and maintain high-performing cyber security teams.

Assessments: Identifying hidden potential

To build an exceptional cyber security team, it is crucial to identify individuals with the aptitude and potential for success in the cyber security field. SANS CyberTalent offers aptitude assessments that have proven successful in identifying thousands of individuals with high potential for cyber security training programs and future job roles. These assessments help organisations uncover hidden talent and make informed decisions in their recruitment processes.

SANS Private Training: Tailored learning experiences

SANS Institute understands that each organisation has unique training requirements. With SANS Private Training information security training options, organisations can create custom training programs for groups of 25 or more, anywhere in the world. These tailored programs leverage SANS's topnotch technology and instruction to provide a comprehensive and impactful learning experience for participants. Private training ensures that your team receives the specific knowledge and skills they need to excel in their roles.

Cyber ranges: Hands-on skill enhancement

To truly excel in the field of cyber security, practical hands-on experience is invaluable. SANS offers a comprehensive suite of hands-on cyber ranges and advanced simulations, with industry-leading interactive learning scenarios. These ranges provide a platform for your team to sharpen their skills, practice real-world scenarios, and collaborate in engaging team-building experiences. By immersing themselves in these virtual environments, cyber security professionals can enhance their abilities to effectively defend against sophisticated threats.

Voucher Program: Simplifying training budgets

Managing training budgets can be a complex task for many organisations. The SANS Voucher Program simplifies this process by allowing organisations to consolidate their training funds into a single SANS Voucher Account. With this account, organisations can efficiently allocate funds for SANS training and certifications for their employees using the online SANS Admin Tool. This streamlined approach provides flexibility and convenience in managing and utilising training budgets.

```
2017-11-11 17:53:40+00 MacBook-Pro InstallAssistant[
2017-11-11 17:56:32+00 MacBook-Pro InstallAssistant[609]: Running OS Build: Mac OS X 10.13 (17A365)
Nov 11 18:01:31 MacBook-Pro OSInstaller[550]: Running OS Build: Mac OS X 10.13 (17A365)
Nov 11 18:05:45 MacBook-Pro OSInstaller[550]: Running OS Build: Mac OS X 10.13 (17A365)
2017-11-11 14:47:49-05 MacBook-Pro Installer[2933]: Running OS Build: Mac OS X 10.13 (17A365)
Nov 11 20:53:47 MacBook-Pro OSInstaller[558]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-11-11 16:56:00-05 MacBook-Pro Installer[1505]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-11-12 22:59:21-05 Sarahs-MBP InstallAssistant[2486]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-11-16 14:11:37-08 Sarahs-MacBook-Pro Installer[19193]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-11-16 14:13:23-08 Sarahs-MacBook-Pro Installer[19234]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-11-16 14:20:39-08 Sarahs-MacBook-Pro Installer[37128]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-11-25 22:30:07-05 Sarahs-MBP Installer[3793]: Running OS Build: Mac OS X 10.13.1 (17B48)
2017-12-17 22:06:15-05 Sarahs-MacBook-Pro Installer[23976]: Running OS Build: Mac OS X 10.13.1 (17B1003)
2018-01-19 13:51:41-05 sarahs-mbp Installer[48509]: Running OS Build: Mac OS X 10.13.1 (17B1003)
2018-01-23 20:15:26-05 Sarahs-MBP Installer[659]: Running OS Build: Mac OS X 10.13.1 (17B1003)
2018-02-10 11:29:46+00 Sarahs-MacBook-Pro Installer[2280]: Running OS Build: Mac OS X 10.13.1 (17B1003)
Feb 17 13:46:08 MacBook-Pro OSInstaller[550]: Running OS Build: Mac OS X 10.13.3 (17D47)
2018-03-03 20:24:16-05 Sarahs-MBP Installer[74593]: Running OS Build: Mac OS X 10.13.3 (17D47)
Mar  7 02:04:19 MacBook-Pro OSInstaller[561]: Running OS Build: Mac OS X 10.13.3 (17D47)
```

SANS DFIR
FOR518.3 | Mac and iOS Forensic Analysis and Incident Response

Strategic talent development: Targeted skill building

Every organisation faces unique skills gaps in their current workforce, and building a program that can effectively address these organisational capability needs is essential. SANS provides tailored training and development programs to enhance the specific skills needed by your team. Whether it's network defence, incident response or cloud security, SANS offers a wide range of courses and resources to address the diverse needs of organisations.

Cyber security leadership training: Guiding from the top

Effective cyber security leadership is critical for organisations to navigate the complexities of the digital landscape and steer their security strategies in the right direction. SANS offers leadership training programs that empower security professionals to take on leadership roles and guide their organisations towards long-term security objectives. By investing in leadership development, organisations can ensure that their cyber security teams are equipped with the necessary skills and knowledge to make informed decisions, and drive effective security practices.

In the face of a growing skills shortage in the cyber security industry, organisations need to take proactive steps to build and maintain high-performing cyber security teams. SANS Institute offers a comprehensive range of solutions – from talent assessment and recruiting, to career planning and team building – to help organisations develop their cyber security talent. ●

To find out more about how SANS can assist with building the ultimate cyber security team, email ANZ@sans.org or call +61 2 6174 4581.

AusCERT's new course

This won't be another article pointing out the increasing frequency of data breaches, as there's no need: data breaches are now a topic of conversation among people of all ages and walks of life. Gone are the days when cyber security was contained to an inner circle of skilled professionals; however, the industry can be difficult for newcomers to enter, with specific role descriptions requiring many years of experience and industry certifications.

For anyone who has been part of the industry for well over 20 years, it's heartening to at last see recognition of the importance of all kinds of diversity in cyber security roles. Great strides have been made by pioneers, such as the Australian Women in Security Network, and by individuals who lead by example – encouraging, mentoring and hiring individuals from all diversity groups.

This has enabled the cyber security industry in new ways. For example, corporate structures usually now include communications, training and awareness right under the CISO. These teams work alongside highly technical cyber security operations centres, and governance, risk, and compliance experts. The significance of this is summed up best by the mantra: 'Security is everyone's business.'

What does this mean? Who is 'everyone', and what are they responsible for? Quite simply, it is literally everyone. No matter who you are, it's likely you'll handle data in some form at some time during your working day, and that data may be covered by regulatory controls or, at the very least, a duty of care will apply to prevent undesirable outcomes due to mishandling.

But how will the shopkeeper, the schoolteacher, or the medical centre receptionist know how to correctly handle data? The relatively new discipline of data governance strives to do exactly that, applying risk-appropriate controls that also take into account the relevant legislation and obligations of the organisation. This fits hand in hand with the organisation's cyber security management program, with the aim of detecting and preventing data breaches.

AusCERT is proudly part of The University of Queensland (UQ) and, over the past few years, UQ has undertaken a bold data governance transformation. The sheer scale (measured in petabytes) of research data housed at UQ necessitated this, even if the regulatory reasons for doing so didn't mandate it. Forgetting the physical limitations of the internet for a moment, imagine the challenges of classifying this data and controlling its distribution among not only in-house researchers, but also other collaboration teams worldwide!

AusCert is pleased to announce that it has joined forces with UQ's data governance team to bring invaluable expertise to AusCERT's members. Through this partnership, the company will provide comprehensive training on data governance principles and important insights into the implementation of data governance strategies via a new AusCERT education course. Stay tuned for further updates and announcements from AusCERT, as it prepares to launch the new course soon! ●

AUSCERT

TRAINING COURSES

AusCERT provides a range of cyber security training courses, suitable for cyber security, IT or risk management professionals, as well as cyber security awareness training that delivers important foundational knowledge in an engaging way that online, self-service training does not.

Our training courses are designed and delivered by highly experienced AusCERT staff or industry trainers. We only use practitioners with relevant industry experience to ensure an authentic, real-world experience for training participants, delivered in an engaging and interactive way.

Our one day training courses are split into two half day sessions delivered online. Available exclusively to AusCERT Member organisations.

For more information please visit auscert.org.au

UPCOMING TRAINING COURSES

- ✓ CYBER SECURITY FUNDAMENTALS
- ✓ INTRODUCTION TO CYBER SECURITY FOR IT PROFESSIONALS
- ✓ INTERMEDIATE CYBER SECURITY - INTERNET TECHNOLOGIES
- ✓ CYBER SECURITY FOR RISK PRACTITIONERS
- ✓ INCIDENT RESPONSE PLANNING
- ✓ CYBER SECURITY RISK MANAGEMENT

FOR MORE INFORMATION VISIT AUSCERT.ORG.AU

From the battlefield to the boardroom

BY PROFESSOR NEIL CURTIS, SENIOR EXECUTIVE – CYBERSECURITY AND BUSINESS DEVELOPMENT, DXC TECHNOLOGY AUSTRALIA

The value of the veterans' internship programs in the cyber security sector.

The demand for skilled cyber security professionals is rapidly increasing in Australia, creating a pressing need to address the skills deficit in the cyber security sector. In response to this challenge, the Australian Government has recognised the importance of bridging this gap, and has invested $1.2 billion in Australia's digital future through the Digital Economy Strategy (DES). As part of this strategy, the University of Southern Queensland, in collaboration with DXC Technology Australia, has developed a groundbreaking program called the Bachelor of Cyber Security and Veterans Cybersecurity Interns Program. This program aims to transition military veterans from military service to industry employment, providing a unique and tailored pathway to meet the growing demands of the Australian cyber security industry.

Co-design of bespoke program with, and for, industry

The program stands out as an innovative initiative that focuses on supporting military veterans and military spouses during a critical transition point in their lives. Unlike traditional programs, this groundbreaking offering integrates a university degree program within the industry itself, ensuring that graduates of the program are well-equipped with the skills and knowledge demanded by the Australian cyber security industry. The program's design is the result of a collaborative effort between the University of Southern Queensland and DXC Technology Australia, ensuring that it aligns with the Australian Qualifications Framework and incorporates industry requirements. By co-designing the program with the industry, military veterans receive specialised training that directly addresses the skills gap.

The military veterans advantage – national target audience

The program acknowledges the valuable skills and experiences that military veterans bring from their military service. It is specifically designed to support military veterans at an important point in their lives as they transition from military to civilian careers. By providing tailored support and recognition of prior learning, this program ensures that military veterans have a smooth and successful transition into the cyber security industry.

The program is specifically aimed at military veterans and spouses who are separating from, or have separated from, Defence roles, and who have no prior experience in the cyber security field. Recognising the wealth of talent among military veterans, the program offers equitable access to opportunities by providing national internship placements in all capital cities of Australia, in addition to remote working within DXC Technology. This inclusive approach not only supports female employees within the cyber security industry, but it also fosters diversity in the field.

Neil Curtis

The demand for skilled cyber security professionals is rapidly increasing in Australia, creating a pressing need to address the skills deficit in the cyber security sector

Bespoke Bachelor of Cyber Security Internship Program

The program is designed to leverage the military roles and experiences of Australian military veterans, while building upon their defence experiences through industry-recognised credentials facilitated by IBM SkillsBuild. The program consists of three domains:

— Cyber Security Core
— Professional Practice Major
— Cyber Security Technical.

These domains cover a wide range of essential topics, such as risk management, digital forensics, security information and event management, penetration testing, network security, and ethical hacking. Through a combination of theoretical and practical learning, military veterans develop a strong foundation in cyber security principles, and gain expertise in specialised areas.

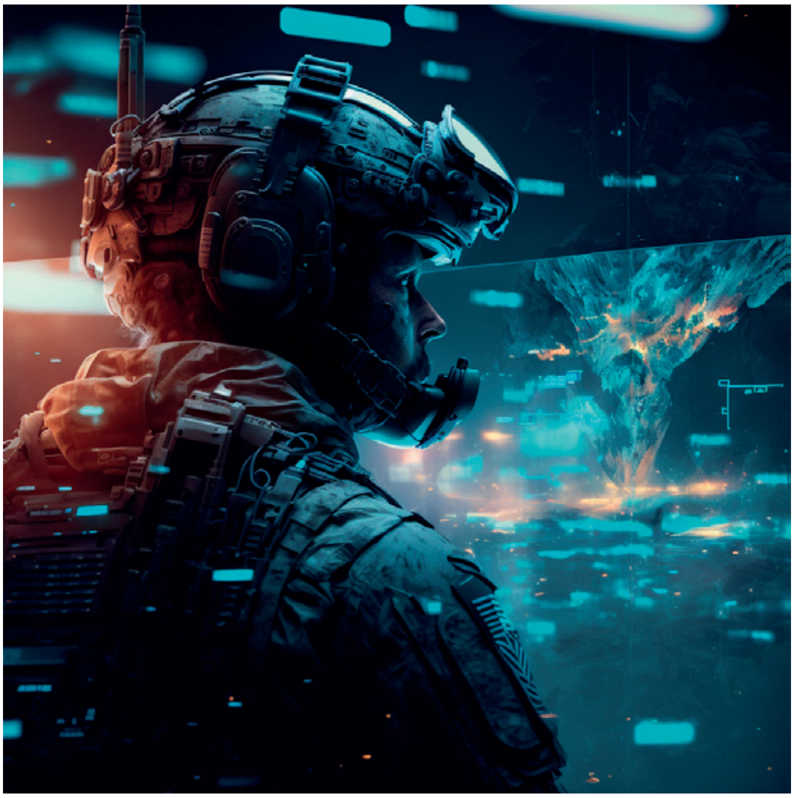
Cyber Security Core: eight credits in Cybersecurity Fundamentals (formal)

Student Negotiated Learning (a year-long, eight-credit capstone course) in Cyber Security Core is offered through a collaboration between a University of Southern Queensland academic lead, a DXC Technology supervisor, and a veteran internship. The internship program at DXC Technology lasts for 12 months. DXC Technology employs the students and, together with the University of Southern Queensland, evaluates their performance.

The assessment will be at Australian Qualifications Framework Levels 7 and 8, and will consist of 12,000 words (or the equivalent). The ePortfolio serves as a repository for the evidence gathered for the Professional Practice Major, and contains the results of the assessment.

Professional Practice Major: Concentration in Professional Practice (formal) – eight units

This award is intended for veterans who have served for at least five years, and who have recently separated from the Defence Force or are in the process of doing so. The Australian Qualifications Framework will only recognise military experience up to 10 years in length, even if the veteran has served for much longer. Each veteran's ePortfolio will be evaluated against the University of Southern Queensland's graduate qualities for degrees at the Australian Qualifications Framework Levels 6 and 7 (undergraduate level).



The Recognition of Prior Learning (RPL) Centre at the University of Southern Queensland was established in 2021 as part of a $340,000 strategic effort staffed by three faculty members. Students enrolled in the Bachelor of Cyber Security program can participate in a pilot program designed to offer RPL. Therefore, this strategic goal and the lessons learnt from this pilot will directly inform any future design of the Bachelor of Cyber Security program.

Cyber Security Technical: Technical Cyber Security (non-formal) – eight credits

Currently, all military veterans can apply for a scholarship through IBM SkillsBuild to retrain in professionally recognised training programs.

To help military veterans and their families find work in the growing field of cyber security, the Cyber Security Technical domain provides training in a variety of relevant technical areas. The University of Southern Queensland will formally accept eight industry credentials, all of which can be thought of as micro-credentials. An Articulation Agreement between the University of Southern Queensland and IBM SkillsBuild validates a set of trade-specific abilities on par with the diploma level of Australia's National Qualifications Framework. Military veterans can tailor their educational path to improve their employability in the cyber security field in one of three possible specialisations. These areas of expertise will become apparent while the program is being designed.

Internships with DXC Technology

What sets the program apart is its integration of a university degree program within the industry itself. This industry-embedded learning approach allows students to gain firsthand experience and exposure to real-world cyber security challenges. By working closely with industry professionals and organisations like DXC Technology, students have the opportunity to apply their knowledge and skills in a practical setting, preparing them for the demands of the industry.

One of the most distinctive features of the program is the inclusion of a one-year industry internship with DXC Technology.

This internship offers military veterans invaluable real-world experience, allowing them to apply their knowledge in a practical setting, and ensuring a seamless transition from military service to industry employment.

By combining academic learning with hands-on training, military veterans will graduate from the program with a Bachelor of Cyber Security from the University of Southern Queensland, and the practical skills needed to thrive in their careers.

Promoting diversity and equal opportunities

The program aims to promote diversity and equal opportunities within the cyber security industry. By targeting a gender balance that reflects the distribution within Defence, the program actively supports female military veterans and seeks to increase representation in the field. This commitment to diversity fosters a more inclusive and well-rounded workforce, bringing different perspectives and approaches to addressing cyberthreats.

Evaluating effectiveness and future development

To ensure the program's effectiveness in meeting industry standards and the requirements of the Australian Qualifications Framework, ongoing evaluation and feedback from participants and industry partners is crucial. The University of Southern Queensland and DXC Technology are committed to continuously improving the program, adapting it to evolving industry needs, and exploring additional avenues for collaboration and support.

Key findings to date

DXC Technology's cyber security practice currently has several military veterans working as interns. At the six-month mark, the most important results to date are:

- Interns have been trained in various new micro-certifications, such as Splunk, Splunk Admin, Sentinel, Trend Micro, and Palo Alto Network's security technologies, leading to increased in-house education and development.
- Leadership and mentoring programs, as well as other soft-skill instructions, have been provided in house.
- Interns have had more hands-on expertise with endpoint protection, email security, incident management, vulnerability management, and security operations.
- As a result of the positive impact the military veterans have had on the company, plans are in the works to expand the program and hire fewer graduates in favour of the more mission-focused, resilient veterans.

DXC's Military Veterans Program provides participants with further benefits, in addition to ensuring that DXC Technology has the appropriate support programs in place to assist military veterans in transitioning into programs and military veteran communities in the business. This is through the implementation of the Military Veterans Best Practice Framework, which was developed to get the best results from all military veterans in the business, and enhance resilience and support.

Conclusion

The Bachelor of Cyber Security and the Veterans Cybersecurity Interns Program represents an innovative and forward-thinking initiative to address the skills deficit in the Australian cyber security industry. By providing tailored support, industry-embedded learning and internship opportunities, the program offers a transformative pathway for military veterans to become skilled cyber security professionals. With the Australian Government's investment in the DES, and the commitment of educational institutions and industry partners, this program plays a vital role in cultivating a highly skilled and diverse cyber security workforce. Through ongoing evaluation and collaboration, the program will continue to adapt and evolve, ensuring its effectiveness in meeting the demands of the industry, and shaping the future of cyber security in Australia. ●

About the author

Professor Neil Curtis *is a distinguished Senior Cybersecurity & Business Development Executive with DXC Technology's Cybersecurity business. As the driving force behind the DXC Military Veterans Program, Curtis spearheads initiatives that bridge the gap between the military and the cyber security realm. Additionally, he holds the position of Business Executive Sponsor for Diversity, Equity, and Inclusion for the ANZ and Fiji region.*

AI and ontology synergy

BY REZA RYAN, NICKSON KARIE AND IAIN MURRAY, CURTIN UNIVERSITY

Enhancing knowledge representation and reasoning in cyber security.

Ontology provides a structured framework for representing knowledge by defining concepts, relationships and properties within a specific domain. The integration of artificial intelligence (AI) techniques with ontology helps systems to have better reasoning, better understanding of complex domains, and intelligent decision-making abilities. Incorporating AI techniques – such as natural language processing (NLP), machine learning and semantic reasoning – can empower an ontology to work with unstructured data, which allows for a more comprehensive and dynamic representation of knowledge. In cyber security, for example, AI can play a crucial role in contributing to the detection, prevention and response to various cyber security threats. Ontology, on the other hand, can help in threat intelligence sharing, contextual analysis, semantic reasoning and vulnerability management.

AI techniques, such as NLP, similarity-based matching and logic reasoning, can automate ontologies' generation and utilisation. This can be done by the extraction and integration of knowledge from heterogenous sources, understanding structured and unstructured information, and being able to exploit the semantic relationships and logical constraints to generate an ontology within a specific domain. AI-driven ontology can also play an important role in ontology alignment and interoperability with existing knowledge bases in specific domains. Ontology alignment involves the mapping of corresponding concepts and relationships across different knowledge base systems, enabling knowledge exchange and integration, while incorporating constraints.

NLP algorithms contribute significantly to the automatic development of ontologies. By applying NLP algorithms and ontological frameworks, important entities, events, properties, and relationships can be identified, extracted, and represented meaningfully. Several NLP techniques can also be employed to develop an ontology automatically. Moreover, NLP techniques can extract information, while ontologies provide a semantic representation of the information and its relationships to others. Named entity extraction can be used to identify or extract entities, like product name, event or location. Relationship extraction can be used to extract semantic relationships between entities – such as a person, task or device – and understand their semantic categories, such as when logged in, done by, and used. Information extraction can also be used to populate an ontology automatically by extracting structured information from unstructured text sources. Word-sense disambiguation can be employed to improve the accuracy of the ontology by providing additional contextual information and clarifying the meaning of concepts.

Despite this, challenges remain in fully harnessing the potential synergy between AI and ontology. Issues such as scalability, semantic ambiguity and disambiguation, AI training, information quality, explainability, ethics, and adaptability to evolving domains need to be addressed. Despite these challenges, the integration of AI techniques with ontology holds great promise in advancing knowledge representation and reasoning as technology continues to evolve so rapidly. In cyber security, combining the power of AI and ontologies can help to leverage advanced analytics, knowledge representation and reasoning capabilities to strengthen defence against evolving threats, reduce response times, and enhance the overall security posture of organisations. •

CRICOS Provider 00002J | FSE48129

MACQUARIE
University
SYDNEY · AUSTRALIA

Is a master's of cyber security worth it?

With so many ways to build cyber skills, Australia's universities are working to offer something different, reports ***David Braue.***

There are as many career paths into cyber security as there are cyber security practitioners – many of whom come to the industry with a slew of technical certifications, many with multiple degrees, and others with both or none of those.

Some have worked in the IT industry for years, bringing a world of experience but few formal certifications. Others come fresh out of university, with a bachelor's and/or master's degree tucked under their arms.

Still others have transitioned from other careers, capitalising upon the many parallels between cyber security and other industries to bring skills in areas such as people management, incident response, problem-solving, and technical analysis.

The importance of diverse perspectives – and resumés – has not escaped the notice of industry bodies such as CyberCX, whose recent collaborative research with Per Capita, entitled 'Upskilling and Expanding the Australian Cyber Security Workforce', anticipates a shortfall of 30,000 unfilled cyber security roles by 2026, and warns that no one training path will fill Australia's cyber skills gap alone.

Despite a 'dramatic shift' in strategy by universities that now offer 87 tertiary qualifications in cyber security (up from just eight in 2018) and 58 qualifications with a cyber security major, the report warns that traditional tertiary institutions will still only be producing several thousand cyber security trained graduates by 2026.

That's far too few to fill the gap alone, which has forced the industry to explore other options – including TAFE, private-sector, micro-credential and other alternatives that offer viable cyber security qualifications in a fraction of the time.

'The sector is highly skilled, with most professionals possessing an undergraduate degree,' the report notes, adding that 'many cyber security roles did not necessarily require a university level [graduate] qualification.'

'While this assertion was dependent upon category and focus, TAFE and other vocational qualifications are viewed as being of significant worth and immense practical value.'

The demand for such vocational qualifications has created opportunities for the likes of SANS, whose Master of Science in Information Security Engineering (MSISE) program runs for three to five years, can be completed online, and is designed to be undertaken alongside work in a cyber security field.

At a total cost of nearly $80,000 (US$54,000), a program like the MSISE isn't

to be undertaken lightly – and its sheer cost may make it more relevant to working professionals whose employers offer generous training subsidies – but its access to real-world, hands-on experience and incorporation of nine GIAC certifications makes it distinctly valuable.

'The SANS promise has always been that you'll be able to apply what you learn the day you return to the office,' SANS Technology Institute Assistant Director Kim Kafka explains, highlighting the benefits of having courses taught by working cyber security professionals.

'The secret sauce to SANS has always been, and remains, our faculty,' she says. 'They're not theoretically teaching you the coursework and giving you this old understanding from 10 years ago when they used to be in the field.

'They are in the field working full time – and they also happen to be phenomenal teachers, so you are learning from some of the best in the industry. The networking opportunities and the learning opportunities are limitless.'

What makes a university master's degree different?

With so many ways to get into the industry, making the decision to commit to a long-form master's degree isn't always an easy one.

There are, after all, many ways to build competency in the five key skills areas flagged by CyberCX – information security, network security, cloud security services, web security, and security architecture – as well as the seven high-level functions and 33 cyber security specialty areas identified in the National Initiative for Cybersecurity Education workforce framework.

Committing to a master's program is an excellent way to not only build skills across these domains, but also to differentiate one's self in the labour market – and pave the way towards more senior cyber security roles in the long term.

Many masters' programs at Australian universities are focused in this way, with core curriculums that address these areas complemented by interplay across faculties that enriches the degree with access to the universities' expertise in related areas – for example, business, statistics, international relations, law, public service policy, and more.

Whatever a student's specific background or interests, careful examination of university master's programs reveals that each is structured slightly differently, and has a different balance between technical skills, certifications, industry partnerships, hands-on experience, project management, collaboration, business skills, and the many other facets of cyber security careers.

RMIT University's Master of Cyber Security, for example, promises students that its two- or four-year program will equip students with 'the mathematical, technical and business tools to secure an organisation's information systems' – combining real-world scenarios and simulated exercises with industry engagement, internships, 'work-integrated learning experiences', and a '360-degree view of the field with a focus on ethics and people in addition to your developed technical skills'.

Designed to be completed in just one year full time, Curtin University's Master of Cyber Security (MCybSec) program 'emphasises experiential project-based learning' with a focus on teamwork, real-world examples, technical and governance skills.

The curriculum has been designed to give students an understanding not only of technical concepts, but of the scientific and analytical methods that feed the development of collaborative problem-solving, ethical solutions creation, leadership and effective communication skills.

Deakin University's program combines foundation information technology studies with subjects in cyber security areas such as identity, access management, physical security, computer forensics, ethical hacking and application security, and then includes a 'capstone unit' focused on professional practice, as well as the project management and delivery of a team project.

Macquarie University has pursued the multidisciplinary approach with a range of graduate options. These include the one-year, skills-focused Master of Information Technology in Cyber Security (MITCS) – which focuses on technical topics like cryptography, data privacy, digital forensics, ethical hacking, and secure app development – and a Master of Cyber Security Analysis that has been paired with coursework to provide two-year joint degrees that also provide qualifications including the Master of Intelligence, Master of Security and Strategic Studies, MITCS, Master of Public and Social Policy, Master of IT in Networking, and Master of Laws.

But is it worth it?

With programs costing around $30,000 per year and accounting for two full-time years' worth of work, these and other programs offered at Australian universities aren't to be entered into lightly – but salary surveys suggest that they do pay off in the long term.

One recent analysis of US roles, for example, found that graduates from well-regarded cyber security graduate degrees can expect starting salaries of between $144,000 (US$100,000) and $288,000 (US$200,000) – with many proceeding to CISO, CIO and CTO roles that command executive-level salaries well into the six figures.

At those salaries, the up-front investment for a master's degree will be paid off within a few years – all the while offering a broader range of career prospects that, with the right combination of experience, may extend all the way to the boardroom.

'Prior to the course, I was in a position of having heaps of industry experience but few formal qualifications,' says Paul Nevin, a principal security architect in Canberra who completed the Master of Cloud Computing and Virtualisation at Charles Sturt University (CSU), and continued on to pursue a Doctor of Information Technology degree, exploring the evolution of internet-based attacks against government and commercial networks.

'I am now in a position [where] I have to hire staff,' he says, recalling how hard it was studying through the night with his baby daughter sitting on his knee. 'Graduating from the CSU course required a great deal of effort and, as a result, was hugely rewarding.' ●

SANS | GIAC CERTIFICATIONS

RECRUIT, DEVELOP AND ***RETAIN*** THE **ULTIMATE CYBER TEAM**

DEVELOP YOUR OWN CYBERSECURITY TALENT WITHIN YOUR WORKFORCE WITH SANS

The cyber security industry is facing an immense skills shortage in Australia and as a result, it's never been more important to recruit, develop and retain a cyber security workforce.

From talent assessment and recruiting to career planning and team building, SANS is your partner for developing a high-performing cybersecurity team.

Discover the SANS approach to cybersecurity workforce development and partner with us to build a high-performing team.

ASSESSMENTS

A proven method to identify hidden, high-potential cybersecurity talent is through assessment tools. SANS Aptitude assessments have successfully identified thousands of individuals with high potential for success in cybersecurity training programs and ultimately in securing cybersecurity jobs.

CYBER RANGES

SANS offers a comprehensive suite of hands-on ranges with industry-leading interactive learning scenarios. You can sharpen your team's cyber skills and maintain their focus with unique and engaging team-building experiences.

CYBER RANGES

PRIVATE TRAINING

SANS Institute's Private Information Security Training options allow you to create a custom training program for any group of 25 students or more, anywhere in the world. With options for commercial groups and government organisations, private information security training will be specifically designed to meet your needs using SANS' top technology and instruction.

VOUCHER

The SANS Voucher Program allows an organisation to manage their training budget from a single SANS Voucher Account. Once the Account is opened, the organisation can utilise funds from their Account for SANS training and certifications for their employees via their online SANS Admin Tool.

SANS VOUCHER

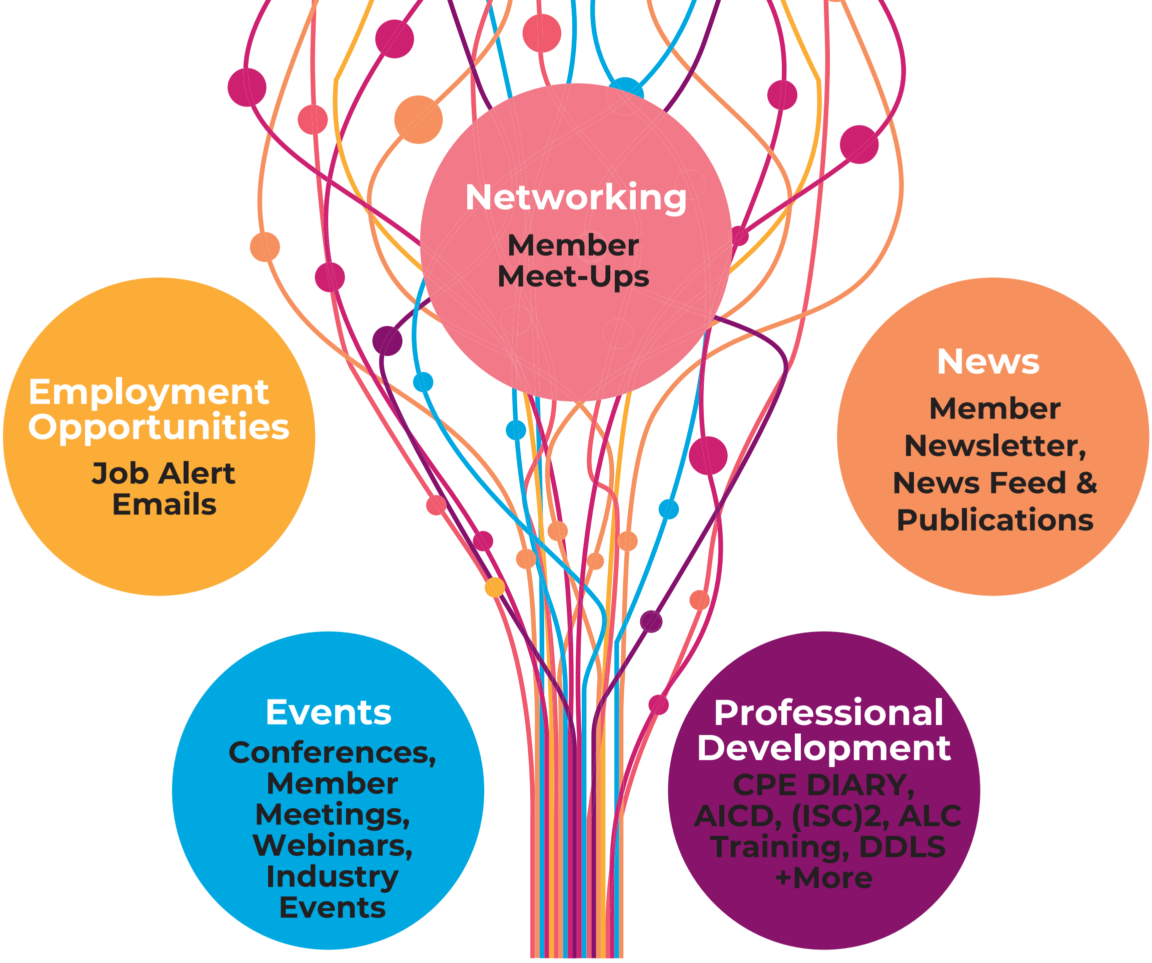
Strategic Talent Development

Develop specific skills needed on your team to combat specific threats your organisation faces every day.

Cybersecurity Leadership Training

Train and prepare your security leadership to guide your organisation toward long-term security

Discover how SANS can help with developing your team's cybersecurity skills,
Contact *anz@sans.org* for more information | *+61 2 6174 4581*



Networking
Member Meet-Ups

Employment Opportunities
Job Alert Emails

News
Member Newsletter, News Feed & Publications

Events
Conferences, Member Meetings, Webinars, Industry Events

Professional Development
CPE DIARY, AICD, (ISC)2, ALC Training, DDLS +More

make true

JOIN AUSTRALIA'S CYBER SECURITY COMMUNITY

connections

AISA invites individuals with an interest in cyber security and related industries to join our fast-growing membership of 10,000+.

Our broad membership base consists of information security professionals from industries such as IT, software development, financial services, education, energy, utilities, telecommunications, consultant/ advisory, healthcare, government, transportation, hospitality, tourism, retail, manufacturing and mining.

BECOME A MEMBER TODAY

AISA
Australian Information
Security Association

www.aisa.org.au