secureGOV

Securing Australia's future

The state of Australia's cyber security landscape
BY PHIL WINZENBERG

Forrester's 2024 cyber security predictions
BY JINAN BUDGE

The intersection of data privacy and cyber security
BY ANDREW LAWRENCE

2024

AISA

SANS | GIAC CERTIFICATIONS

25 Years IN AUSTRALIA EST. 1999

SANS Australia: Supporting and Strengthening the Australian Cyber Security Community for 25 Years

Since 1999, SANS Institute has trained over 15,000 students across Government Organisations, Enterprise and SMBs.

While a lot has changed in 25 years, one thing stays the same: the SANS Institute mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.

From cyber foundations to leadership strategies, SANS offers more than 85 hands-on courses to help cyber professionals at every level of experience gain immediately applicable skills.

Why SANS Training Courses?

World's Best Instructors

SANS instructors includes the industry's most accomplished professionals, having battled in the cyber security trenches firsthand, to enable the immediate and effective application of your coursework.

Hands-on Training

Our curriculum, with practical hands-on exercises, includes the most comprehensive array of courses and post-training a rich ecosystem of resources and access to a community of the world's most experienced cyber-professionals.

Most Valued Certifications

GIAC Certifications provide the highest and most rigorous assurance of cyber security knowledge and skill available to industry, government, and military clients across the world.

Multiple Training Options

The learning experience at SANS starts with letting cyber students train when, where and how they need to - live or on-demand, in-person or virtual.

The SANS Experience Scores

4.78 Stars

Average SANS cyber training Content Scores

4.85 Stars

Average SANS cyber training Teaching Scores

4.78 Stars

Average SANS cyber training Overall Scores

Discover how SANS can help with developing your team's cyber security skills, Contact anz@sans.org for more information

+61 2 6174 4581
www.sans.org

Foreword

BY **CRAIG FORD, BOARD DIRECTOR, AISA**

Regardless of where you look, there is constant overlap between the digital and physical worlds.

We depend on technology and connectivity for almost every aspect in our life. Just look at the effect that the Optus outage caused towards the end of 2023 – even hospitals and transportation systems were affected. I was personally affected, as I was trying to catch a flight from Brisbane to Sydney and couldn't access the airport parking. I also couldn't use the Qantas app to retrieve my boarding pass, so I had to revert back to old-fashioned printed assets. It was very obvious what sort of a spanner in the works this kind of incident could bring, so it shouldn't surprise us that it is a big focus for the general public and the government.

In the case of the Optus outage, it was routine maintenance that caused the fault at around 3 am that morning, which caused services to be out until midday for most locations – with many taking a lot longer to restore. This incident – combined with several large cyber breaches, including the ones prior for Optus, Medibank, DP World and more – makes it completely understandable that cyber security has become a very hot topic of late.

The Australian Cyber Security Strategy, released late last year, shows the priority that the government is putting on uplifting the Australian maturity level for security across the board.

The government is assembling a team of cyber experts, and has been seeking advice from industry for some time. The Australian Information Security Association's (AISA's) formal submission response was considered as part of its plan. There is strong focus on small and medium-sized enterprise (SME) cyber uplift, which is something that we all need to embrace, given that SMEs make up 98 per cent of businesses in Australia.

This focus is long overdue – industry and government have been failing in this area for a long time. Only time will tell if this path will shift the dial for success – and I have my doubts if it is the right approach – but it is great to see a plan being created to at least try to improve the space.

There is a greater focus on what is classed as critical infrastructure and responsibility in organisations when it comes to ensuring that cyber security is taken seriously. For the first time, this has been pushed into the public agenda, with the mandate that all agencies and organisations in the public sector must have a director for cyber security – such as a head of security, CISO or similar – with the capability to ensure that each agency is given the cyber security focus it needs.

Overall, industry and government will need to come together to ensure this plan succeeds. AISA, as the peak body for cyber security in Australia, will continue to do everything it can to support initiatives that help our members and the wider community. We are in this together – industry and government – and we must work together collaboratively and effectively in order to achieve successful outcomes.

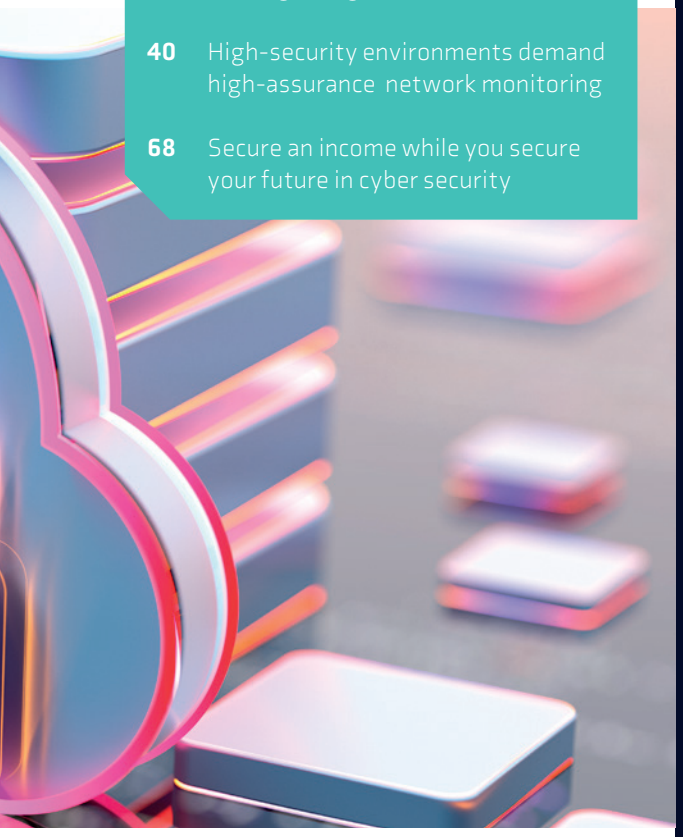
secureGOV is just one of the many ways that AISA can continue to bring awareness to issues and projects that affect government at all levels, and how this flows over into the private sector. It is a magazine that helps to facilitate conversations and resources, raising issues that need debating, and providing an opportunity for them to be understood and acknowledged.

With the inaugural edition of *secureGOV* being such a success, we are really lifting the bar for both this edition and future editions to ensure that it is as valuable to readers as possible. We welcome any feedback or suggestions you might have to help drive *secureGOV*'s relevance further.

Please send your thoughts to editorial@aisa.org.au, and we will do our best to incorporate your feedback as we continue to develop this annual journal of record for government.

Craig Ford

Contents



PUBLISHED BY :

EXECUTIVE MEDIA

ABN 30 007 224 204
PO Box 256, North Melbourne, VIC 3051
Tel: 03 9274 4200
Email: media@executivemedia.com.au
Web: www.executivemedia.com.au

PUBLISHER
David Haratsis
david.haratsis@executivemedia.com.au

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

CO-EDITOR
Craig Ford

EDITORIAL ASSISTANTS
Eden Cox and Ruby O'Brien

DESIGN
Sam Garland

PARTNER ORGANISATIONS
Aris Zinc Group | BT Software Australia Pty Ltd | Edith Cowan University | Filigran | OPSWAT Inc | Prophecy International | SANS Training Australia | Senetas | Syber Services
Trend Micro Australia Pty Ltd | Zoho Corporation Pty Ltd

COVER
iStock.com

All stock images sourced from iStock.com and Adobe Stock.
Vegetable-based inks and recyclable materials are used where possible.
We acknowledge the Wurundjeri people of the Kulin nation who are the traditional custodians of the land on which this magazine is published.

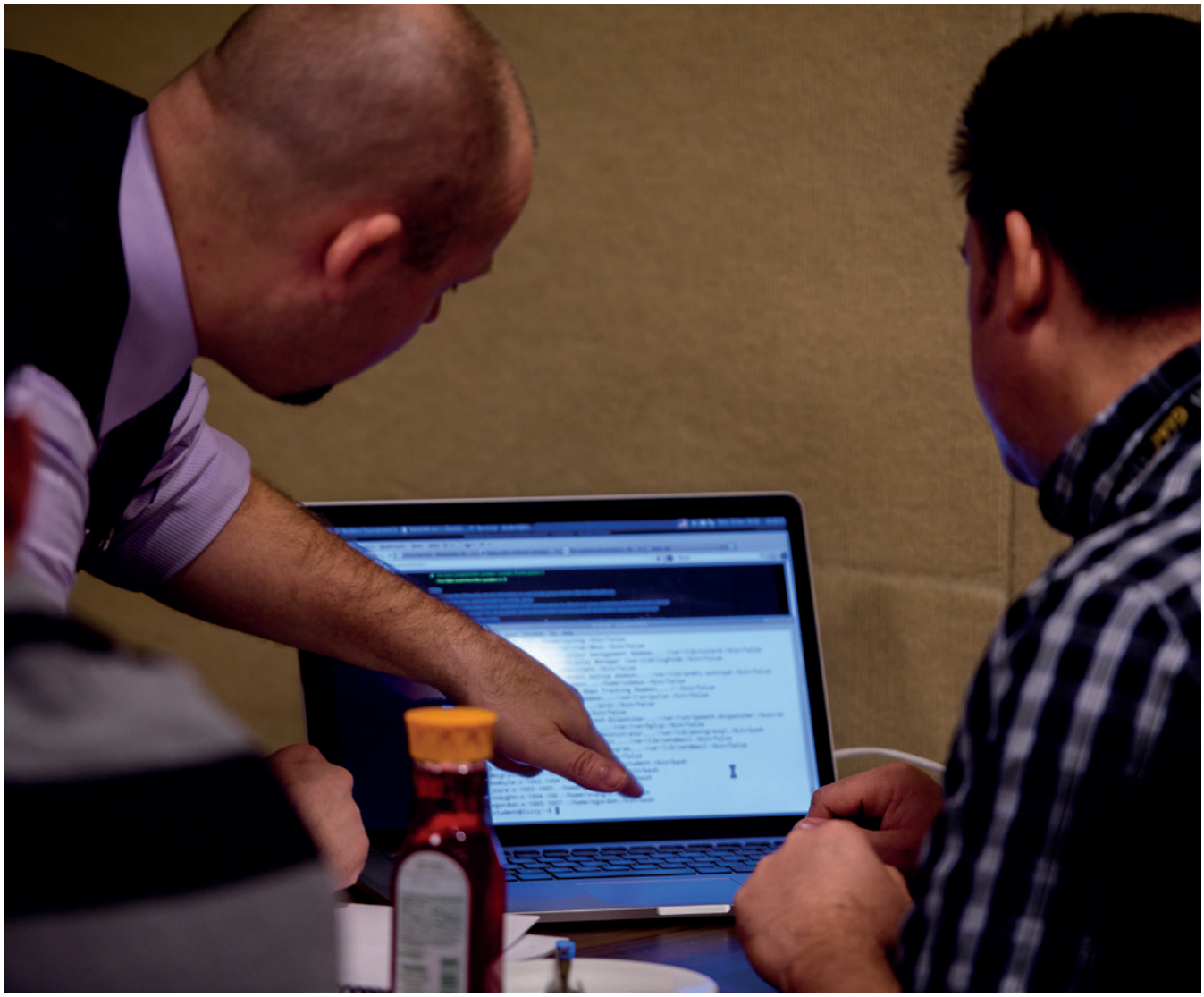
Proudly Printed In Australia

SANS Institute's quarter-century journey in Australia

Twenty-five years of community, partnerships and training excellence in Australian cyber security.

In an era defined by rapid technological advancement, the realm of cyber security has evolved, through necessity, at an incredible pace. As SANS Institute Australia celebrates 25 years of providing cyber security training and certification to Australian information security professionals, it proudly reflects on a quarter of a century of community building, innovation and partnerships. For a remarkable 25 years, SANS Institute Australia has stood by the side of cyber security professionals, government organisations, Australia's largest enterprises, and small and medium-sized businesses.

SANS Institute Australia's journey began with a vision to bridge the gap between the growing digital landscape and the increase in cyberthreats. Today, it is evident that



cyber security training and certification is becoming more important than ever. The Australian Signals Directorate Cyber Threat Report highlights a significant 23 per cent uptick in cybercrime reports throughout 2022/23, emphasising the importance of enhancing cyber security measures. SANS Institute Australia's mission is to provide cutting-edge cyber security training solutions and certifications to empower cyber security professionals with the practical skills and knowledge they need to make our community – and our world – a safer place.

During its 25 years, SANS Institute Australia has delivered more than 15,000 training courses to cyber security professionals from the most important organisations across Australia, contributing to the development of a skilled and resilient cyber security workforce. Alumnis are spread across many industries, holding key positions in cyber security, and playing pivotal roles in protecting Australia's digital infrastructure. More than 11,500 of them have been Global Information Assurance Certification–certified, and provide the highest and most rigorous assurance of cyber security knowledge and skill available.

One thing has been constant over the SANS Institute's 25 years of delivering training in Australia: the SANS Institute Promise: everyone who completes SANS training can apply the skills and knowledge they've learned, from the first day they return to work as the training is delivered by some of the world's most respected global practitioners and cyber security leaders.

SANS Institute is also regarded for the wealth of exclusive online cyber security resources, news and tools it provides, completely free of charge, to support cyber professionals in the practice and development of their skills. Whether it's newcomers to the industry or seasoned practitioners and leaders, there is valuable content available for everyone.

As SANS Institute Australia continues on its mission with the Australian community, the organisation remains committed to serving Australia's cyber security needs. SANS's focus is to provide high-quality training, certifications, cyber ranges and resources to meet the needs of every cyber professional. S

For more information on how SANS Institute Australia can support your organisation in strengthening cyber resilience with training and certifications, email ANZ@sans.org, call +61 2 6174 4581, or visit www.sans.org/au_en

The state of Australia's cyber security landscape

BY **PHIL WINZENBERG, ACTING HEAD OF THE AUSTRALIAN CYBER SECURITY CENTRE**

Australia is lucky to be a prosperous and digitally connected nation. Unfortunately, as Australians have regrettably discovered, our success as a nation has been accompanied by an increase in our attractiveness to malicious cyber actors.

The harm that malicious cyber activity causes Australia is real, and mitigating cyberthreats to protect Australia deserves our full attention and action.

My organisation, the Australian Signals Directorate (ASD), produced its latest Annual Cyber Threat Report in November 2023. The report shows that more than 94,000 cybercrime reports were received during the 12 months to June 2023. This is about one report every six minutes, an increase of 23 per cent from the past financial year. It confirms that cybercrime is a multi-billion-dollar industry stretching across international borders, resulting in real harm and significant cost to Australia.

CYBERTHREAT OUTLOOK

The risks are no longer an inconvenience, but have, in fact, become grave in consequence.

The Cyber Threat Report – ASD's fourth such snapshot – also highlights the persistent threat posed by nation-state cyber operators as part of ongoing cyber espionage and information-gathering campaigns. Such activity against Australia will only increase as our strategic circumstances continue to deteriorate.

Globally, a broad range of malicious cyber actors – including state actors, cybercriminals and issue-motivated groups – have demonstrated the intent and the capability to target a nation's critical infrastructure. We have seen examples of this in the context of the conflict in Eastern Europe, and my organisation is aware of instances in Australia and other allied nations.

In an increasingly hostile environment, Australia's most critical industries and infrastructure have become prime targets for cyber attack. Malicious cyber actors are increasingly going after our hospitals, schools, government services, transport and energy grids, stealing data, ransoming critical networks, and potentially putting lives at risk.

Phil Winzenberg

Malicious cyber actors may target our infrastructure for a range of reasons, such as to:

- attempt to degrade or disrupt services through denial-of-service (DoS) attacks and distributed denial-of-service (DDoS), causing significant impact on service providers and their customers
- steal and encrypt data, or gain inside knowledge for profit or competitive advantage
- preposition themselves on systems by installing malware in anticipation of future disruptive or destructive cyber operations, potentially years in advance
- covertly seek sensitive information through cyber espionage to advance strategic aims.

In May 2023, ASD joined international partners in calling out a cluster of activity associated with a People's Republic of China state-sponsored cyber actor, also known as Volt Typhoon. The campaign involved 'living off the land' techniques – using built-in operating tools to help blend in with normal system and network activities. Industry partners identified that this activity affected networks across US critical infrastructure sectors. These same techniques could be applied against Australian critical infrastructure sectors.

During financial year 2022/23, ASD responded to 143 incidents reported by critical infrastructure entities, an increase from the 95 incidents reported in the prior year.

The main cyber security incidents affecting Australian critical infrastructure were:

- compromised account or credentials
- compromised asset, network or infrastructure
- DoS/DDoS.

These incident types accounted for approximately 57 per cent of incidents affecting critical infrastructure for 2022/23. Cyber security and reinforcing our online resilience is a critical government priority. The work performed by ASD is more important than ever, given the cyber incidents seen in Australia over the past year.

But regardless of ASD's capabilities, or how advanced the private sector's cyber defences are, we cannot protect Australia, its systems and interests in isolation. ASD's Cyber Threat Report highlights how, with a team approach, we can mitigate against cyberthreats while taking advantage of the digital opportunities so vital to our nation.

This means that every organisation, government entity and household must sharpen their online defences, improving cyber security to protect our essential services and the data of millions of Australians. Reporting anomalous activity early and not waiting until activity reaches the threshold for mandatory reporting helps piece together a picture of the cyberthreat landscape. It also informs ASD's cyber security alerts and advisories that forewarn other potential victims and minimise harm for the benefit of all Australians.

ESSENTIAL EIGHT

Malicious cyber activity targeting Australian government entities and critical infrastructure is likely to increase as networks grow in size and complexity. Close collaboration and a unified approach across industry, government, and business is key to national resilience. This includes getting the basics right, such as implementing ASD's Essential Eight, and using products that are both secure by design and secure by default.

ASD's Essential Eight is the best practice to mitigate cyber security threats. It has been designed to protect organisation's internet-connected IT, and represents the best-value investments that an organisation can make to minimise risk of cyber harm. Measures outlined include patching applications and operating systems, mandatory multi-factor authentication, restricting administrative privileges, implementing hardened application controls across networks, adequately configuring Microsoft Office macros, and implementing and testing regular data backups.

ASD's latest Cyber Threat Report confirmed that one in five critical vulnerabilities identified within IT products were exploited by malicious actors within 48 hours. Such speed demands that all entities patch, update or otherwise mitigate critical vulnerabilities in online services, internet-facing servers and internet-facing network devices within 48 hours of an alert or when a working exploit exists. Otherwise, vulnerabilities should be patched, updated or otherwise mitigated within two weeks.

If due to high-availability business requirements or system limitations an entity is not able to apply these mitigations, they should consider compensating controls. These could be disabling unnecessary internet-facing services, strengthening access controls, enforcing network separation and closely monitoring systems for anomalous activity. Boards and leaders need to understand the level of risk they hold and the potential consequences should their systems or data be compromised due to unpatched vulnerabilities.

Entities with limited cyber security expertise who are unable to rapidly patch should consider using a reputable cloud service provider or managed service provider that can ensure timely patching.

If patches are not implemented, the outcomes can be devastating for organisations. In early 2023, a business in regional Australia experienced a malicious network compromise. The business had missed a patch for a remote server, and a malicious actor took advantage of the exploit, compromising a privileged account. They elevated their credentials and moved laterally across the network. Fortunately, the compromise was discovered; but, the consequences would have been disastrous if the malicious actor had installed ransomware, exfiltrated critical data and deleted backups.

ZERO TRUST CONSIDERATIONS

The Essential Eight is the start of an organisation's cyber security journey, not the end. An organisation may derive greater return on its security investment by implementing further mitigation strategies depending on its unique circumstances; the threat environment it operates in; and what threats it is most concerned about, such as malicious insiders deliberately working to compromise a network, or trusted staff clicking on a link within a compromised business email.

Traditional networks are designed on the principle of perimeter security, a boundary between a network and the internet (like a moat around a castle), built with defences like gateways and firewalls; however, once behind these initial security measures, movement in the network can sometimes be largely unrestricted. Instead, an organisation

MALICIOUS CYBER ACTIVITY TARGETING AUSTRALIAN GOVERNMENT ENTITIES AND CRITICAL INFRASTRUCTURE IS LIKELY TO INCREASE AS NETWORKS GROW IN SIZE AND COMPLEXITY

may take a Zero Trust approach to network design – trust no-one, verify everything. This approach acknowledges that cyberthreats exist both inside and outside a network (assuming the network has already been compromised by a malicious actor). Zero Trust principles add emphasis on protecting each individual piece of data, resource and service within the network in case of malicious access. The Essential Eight contains elements aligned to some Zero Trust principles, especially those concepts discussed earlier: patching applications and operating systems, multi-factor authentication, and restricting administrative privileges.

CYBER SUPPLY CHAIN

Increasingly complex supply chains have made it imperative for organisations to scrutinise their cyber supply chain vulnerabilities and risks. While an entity can outsource its ICT functions to access specialist skills, increase efficiency and potentially lower costs, it must still manage and be accountable for cyber security risk. ICT supply chains can increase the attack surface, particularly as there may be varying levels of cyber security maturity among both suppliers and their subcontractors and their own suppliers.

Consider prioritising suppliers that have made a commitment to transparency, as well as a demonstrated commitment to the security of their own systems, products and services. Build cyber security costs into budgets for the entire life cycle of the product, including the product's replacement.

ASD provides security guidance for organisations on a range of additional mitigation strategies for specific

environments, such as cloud services. In addition, the principles and intent behind the Essential Eight may be applied to cloud services, such as ensuring that administrative accounts are separate, minimised, strictly monitored and configured to access only the cloud resource. Implementing mitigation strategies proactively can be more time and cost effective than having to respond to a large-scale cyber security incident. This is greatly aided by embedding good cyber security practices in your organisation.

This includes (but is not limited to) knowing the business criticality of your data and critical business functions, and ensuring that senior leadership from all parts of your organisation is engaged in the management of cyber security – from IT to legal, communications and human resources functions. Importantly, you should be continually reviewing, testing and exercising your cyber security posture.

And, as always, report all cybercrime and cyber security incidents to the ASD. This reporting is vital, as it helps the ASD to build the national threat picture and alert more Australians to evolving threats, making all of us more cyber secure. Help us help you, and others.

About the author

Phil Winzenberg *leads the Australian Cyber Security Centre's Cyber Engagement and Strategy Division, which coordinates the Australian Signals Directorate's (ASD's) strategy and relations with industry, government, and the media.*

ManageEngine

Dare to defend.

Safeguard your digital enterprise with
ManageEngine's cybersecurity solutions.

Our solutions

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

www.manageengine.com/cybersecurity

ManageEngine is a division of ZOHO Corp.

Is today's security surveillance culture a necessary invasion of privacy?

In an age where security and privacy are delicately balanced, the emergence of advanced surveillance technologies using AI sparks a contentious debate: is security surveillance an inevitable accepted intrusion into our private lives?

As society grapples with evolving threats and vulnerabilities, Strategic Executive Solutions, a division of the Aris Zinc Group, introduces ThynkMobix, an innovative asset intelligence platform powered by Mapcite Location Intelligence. While hailed as a groundbreaking tool in bolstering asset identity and performance with security measures, its implementation prompts us to ponder the boundaries of privacy.

The argument for security surveillance often circles back to the paramount importance of safety. Proponents emphasise its role in safeguarding against threats, both internal and external. ThynkMobix, for instance, offers predictive insights into human, AI, and machine behaviours, allowing for proactive measures against potential risks. But does this warrant the potential infringement on privacy? Can the AI element be responsible and ethical where humans might not?

Critics argue that the rapid advancement of AI surveillance technologies is treading a fine line. The pervasive reach of surveillance into our daily lives, from workplace monitoring, home asset tracking, to public spaces, poses questions about the extent of acceptable scrutiny. How far can surveillance encroach before it undermines individual freedoms?

Thynk Mobix's comprehensive suite of services, encompassing data preparation, applications, intelligence solutions, and insider peril monitoring, amplifies the discourse around privacy invasion. While it promises unparalleled insights into location data, including internal communications monitoring, it also raises concerns about the overreach of surveillance capabilities again.

Yet, amid this debate, the necessity of security surveillance persists. The proactive identification of potential risks within an organisation, the analysis of location data for security purposes, and the ability to anticipate and prevent security breaches all underscore the criticality of surveillance in modern risk management.

Ultimately, the conversation around security surveillance requires a delicate balance - a balance between safeguarding against threats and respecting individual liberties.

ThynkMobix stands at the forefront of this discourse, offering innovative solutions that necessitate a thoughtful examination of where the line should be drawn.

For a deeper understanding of Thynk Mobix's capabilities and how we navigate the realms of security and privacy using AI and non AI data capture and analysis, visit ThynkMobix at **www.strategicexecutive.com/thynkmobix-location-and-asset-intelligence/** and explore the services that redefine the landscape of asset intelligence and security surveillance.

Lizzie Christiansen Young
Global Partner/CTO

THYNK MOBIX

POWERED BY MAPCITE MOVEMENT INTELLIGENCE

- Personalised advertising
- Risk management
- Crime prevention
- Asset performance
- Asset tracking
- Security surveillance
- Land integrity
- Crowd monitoring
- Insurance asset and land intelligence
- Urban planning
- Environmental tracking and ESG reporting

info@strategicexecutive.com
1300 274 794

We will, we will prosecute you: ICC web catches cybercriminals

BY **JADE PEACE, LEGAL COMPLIANCE MANAGER, LEXTECH; ASSISTED BY PRIYESHA NAIDU, SENIOR COMPLIANCE OFFICER, LEXTECH**

It is certainly not 1977 anymore, and cybercriminals are being warned. To quote the band Queen, 'Somebody better put you back into your place', for there is much at stake for nations across the globe due to a significant surge in cybercrimes, and the strategic deployment of cyber capabilities in warfare.

Prosecution of persons by the International Criminal Court (ICC) for involvement in cybercrime is being considered by the ICC under the Rome Statute 1998 (the Statute).

In late 2023, the ICC's lead Prosecutor, Karim A. A. Khan, reiterated the importance of the ICC, recognising the impact of cyber warfare, whereby it is the court of 'last resort' to prosecute persons for serious international crimes.

In Australia, the businesses that originate and operate within our golden soil and internationally must consider their systemic risk and third-party integrations, to ensure any such changes are considerate of potential liability under the Statute.

Any and all businesses may be caught under the Statute, whereby sufficient evidence is provided to satisfy the prosecutor of such crimes committed, and an investigation is accepted by the assembly.

WHAT IS THE ROME STATUTE?

After a conference on 17 July 1998, 160 states created the first treaty establishing the ICC as the permanent international court.

The purpose of the Rome Statute is to establish the four most serious international crimes being:

- genocide (Article 6)
- crimes against humanity (Article 7)
- war crimes (Article 8)
- crimes of aggression (Article 8 bis(1)).

Since then, over 120 countries have ratified the Rome Statute.

WHAT IS THE ICC?

The ICC is the permanent independent international court established to investigate, prosecute and try persons accused of committing the most serious crimes of concern to the international community.

It is important to note that the ICC does not replace national criminal justice systems; rather, it complements them whereby they are genuinely unable or unwilling to carry out such proceedings.

DOES THIS AFFECT YOU?

Yes – any and all businesses that operate via the use of technology, cloud infrastructure and the internet can be affected.

As our world becomes increasingly interconnected, the vulnerability within digital infrastructures has become a prime target for malicious actors seeking to exploit, manipulate, or disrupt communities. This escalating trend raises critical concerns about the intersection of technology, security, geopolitics and the law.

Although many nations are adapting their defence strategies in the face of evolving cyberthreats, how the law will be applied to prosecute cyberwar criminals who attempt to bypass or successfully bypass these safeguards remains unclear.

WHAT IS THE ICC'S PLAN?

The ICC recognises that the methods used to commit serious international crimes are constantly evolving – from traditional tools such as bullets and bombs, to emerging technology like the internet and artificial intelligence.

While cyberspace activities are not specifically written into the Statute, it should not be assumed that violation within this realm remains free from regulation, accountability and prosecution.

Recently, cyber security commentators have been advocating for some cyber operations to be assessed in the same vein as other acts of war.

The ICC has also agreed that there is a need for these considerations, as attempts to impact critical infrastructure (such as medical facilities, transport or control systems) may result in immediate consequences for many civilians, particularly those in vulnerable communities.

Previously, institutes like the Human Rights Center at the University of California and Berkeley School of Law have urged the ICC to investigate various Russian cyber attacks in Ukraine as possible war crimes.

In the absence of an independent legal framework that directly addresses cyber attacks, the ICC aims to ensure legal accountability through existing statutes (such as the Rome Statute), which may deter

Jade Peace

offenders who seek to engage in cyber attacks and will provide a precedent to navigate legal ambiguity as it currently stands.

WHILE CYBERSPACE ACTIVITIES ARE NOT SPECIFICALLY WRITTEN INTO THE STATUTE, IT SHOULD NOT BE ASSUMED THAT VIOLATION WITHIN THIS REALM REMAINS FREE FROM REGULATION, ACCOUNTABILITY AND PROSECUTION

WHAT CONSTITUTES A CYBER 'ATTACK'?

One clear challenge is undoubtably fitting cybercrimes into the current international legal framework, specifically in relation to defining key terms and activities.

Most of the international legal framework, including the Statute, is heavily geared towards the occurence of the crime first followed by reprimand; however, a more proactive approach is being considered by the ICC.

Unfortunately, the varying applications of international law make it difficult to foresee how the ICC will position itself when responding to cyber attacks. The term 'attack' is not defined in the Statute; however, Article 8 of the Statute can be used to identify if an attack has actually occurred. For example, hacking for surveillance purposes and espionage would not qualify as an attack.

It is also important to note that cyber attacks can quickly become widespread. Just as a conventional physical bombardment of a military base can temporarily suspend their action, a cyber attack to the same military base may, in fact, also result in the same suspension of action.

The difficulty then becomes not the actual attack happening and proving its consequences, but the persons responsible as the specific perpetrators of the cyber attack.

WHAT ARE THE CHALLENGES FACED WITH SUCH APPLICATION?

The challenge will ultimately be defining the below for each crime from a 'cyber lens'.

- **Ratione temporis (Jurisdiction):** Where a claim by a state to be unable to, or to be unwilling to, handle must be a state recognised as a party to the Statute prior to the claim (Article 11 of the Statute).
- **Mental element of intent:** Where the cybercriminals are a group of actors 'unknowingly participating' in warfare, or have no mental intention to 'engage in the conduct' and 'cause the consequence or is aware that it will occur in the ordinary course of events' (Article 30 of the Statute).
- **Nullum crimen sine lege:** A crime definition shall not be extended by an analogy. If any ambiguity occurs, the definition is interpreted in favour of the person being investigated, prosecuted or convicted (Article 22(2) of the Statute).
- **Jurisdiction of cybercrime:** Where did the cybercrime in its first instance originate, and what if the cybercrime is felt across more than one jurisdiction with conflicting national legal framework?

THE FUTURE STATE FOR CYBERCRIME PROSECUTION

Under current international legal framework and, arguably, national, there are no immediate changes. The consideration by the ICC of such events of cybercrime being perpetrated during warfare is a step in the right direction.

Application of the Statute is a mitigation step under the current ICC action to consider the Statute's suitability to handle such technological advancements in warfare to include cyber attacks.

The use of the same statute criteria on prosecuting cybercriminals in warfare to 'put you back into your place' is not perfect; however, it is the first step that the ICC is taking to claim 'we will, we will' prosecute you.

About the author

Jade Peace *is an Australian legal practitioner working in the fintech industry as Legal & Compliance Manager at LEXTECH. With expertise in how business meets regulatory technology concerns, alongside managing people against business risk appetite, Peace is never without words of wisdom.*

SENETAS
SECURITY WITHOUT COMPROMISE

SOVEREIGN
CYBER SECURITY
FOR GOVERNMENT

The Strongest
Data Privacy Protection
Against Network Attacks

Trusted Globally.
Chosen To Protect The Most Sensitive Australian, US, EU & UK Government Networks.
Certified for Governments By FIPS, Common Criteria, NATO & ANSSI.

Senetas solutions provide maximum data protection
without compromising performance or user experience.

Senetas Global
T: +61 (0)3 9868 4555
E: info@senetas.com

PROUDLY MADE IN AUSTRALIA

senetas.com
info@senetas.com

Filigran: the emerging favourite startup for government institutions

Filigran, a dynamic cyber technology startup established in 2022, is rapidly gaining recognition in the public sector. Esteemed entities, including the European Commission, the European Union Agency for Cybersecurity, the French National Agency for the Security of Information Systems, NYC Cyber Command, Dutch Police, the FBI, various Australian federal agencies, and several European ministries, are among its customers. Specialising in cyberthreat intelligence–driven open-source solutions, Filigran serves a global array of cyber security teams. With its recent Series A funding, led by the prominent Silicon Valley venture capital firm Accel, Filigran is poised to redefine threat intelligence for government institutions.

The cyberthreat matrix facing these federal and local institutions is complex and multifaceted. From data breaches and espionage, to the insidious rise of ransomware targeting essential services, the challenges are profound. These threats are further amplified by the advent of Internet of Things and 5G technologies, which expand the attack surface exponentially. The situation is compounded by sophisticated adversaries, who employ advanced tactics and procedures to infiltrate and dwell within critical systems undetected for extended periods. This evolving threat landscape necessitates a comprehensive and advanced cyber security strategy to safeguard national interests, and ensures the security of sensitive information.

The government sector grapples with unique challenges in threat intelligence. The swift pace of cyberthreat evolution often outstrips existing defensive measures. The complexity and volume of data requires

effective filtration and prioritisation to identify genuine threats and false alarms. Real-time threat intelligence is crucial for pre-emptive action, yet integrating this intelligence seamlessly into operational systems remains a daunting task. Bureaucratic inertia and limited resources further constrain the government sector's ability to adapt quickly to new threats.

Addressing these challenges requires a nuanced understanding of the threat intelligence landscape, emphasising the critical nature of collaboration among various stakeholders. The success of threat actors is often attributed to their ability to collaborate, sharing tools and techniques that enhance agility and precision in evading defenses.

In contrast, many organisations remain hesitant to share sensitive threat information that could prevent the re-use of these tactics by adversaries. Effective collaboration involves sharing detailed observations of attacks, including tactical information like file hashes, domains, internet protocols, and strategic insights into actor motivations and behaviours. This type of threat intelligence sharing, especially within formal communities – such as information sharing and analysis centres – can significantly enhance an organisation's defensive posture by providing a more comprehensive understanding of relevant threats. Such collaboration allows for a diversity of perspectives and expertise, leading to stronger overall threat analysis and a more informed defensive strategy against known and suspected threats.

Filigran's flagship product, OpenCTI, and its adversary simulation tool, OpenBAS, represent a leap forward in meeting these needs. OpenCTI is not just a platform for aggregating and organising cyberthreat intelligence; it's a catalyst for transforming raw data into actionable insights. By correlating information from OpenBAS with OpenCTI, Filigran offers a comprehensive solution that not only identifies threats, but also simulates potential adversary actions, providing a holistic view of the cyber security landscape.

The value of OpenCTI is profoundly seen in its capacity to foster a secure ecosystem for threat intelligence sharing across agencies, ensuring data integrity and confidentiality are never compromised. The data can be securely disseminated through expediting response times and bolstering the collective cyber security defences. Moreover, the sophisticated access management ensures that intelligence is shared according to the specific clearance or role of a person or an entity, permitting segmentation and the safeguarding of sensitive information. This precision in access control is crucial for operational security and integrity within the collaborative framework of multiple agencies sharing important data.

Moreover, the open-source approach allows the government sector to thoroughly inspect and assess the software, ensuring it meets the specific security standards and requirements for transparency. This model not only builds a foundation of trust, but also enables agencies to adapt the software to their regulatory and security needs, showcasing the adaptability and reliability of open-source solutions in meeting the stringent demands of government cyber security protocols.

Additionally, the technology's support for air-gapped operations is crucial for intelligence services and critical infrastructure sectors, where offline platform operation is mandated by stringent security protocols. This feature is particularly beneficial for defence groups, intelligence agencies and critical service industries, demonstrating the ability to cater to highly specific and secure government operations. This adaptability underscores the technology's alignment with the unique and rigorous cyber security requirements of these sensitive government sectors.

Advanced cyberthreats have significantly challenged governments worldwide, exploiting slow-moving policies and departmental silos. The strategic integration of threat intelligence, as facilitated by solutions like those offered by Filigran, empowers government agencies to not only anticipate and mitigate cyberthreats more effectively, but also to fortify their overall security posture. This integration is not merely beneficial – it's a critical step for maintaining an edge in the digital threat landscape, highlighting the necessity for governments to adopt a more responsive and cohesive approach to cyber security.

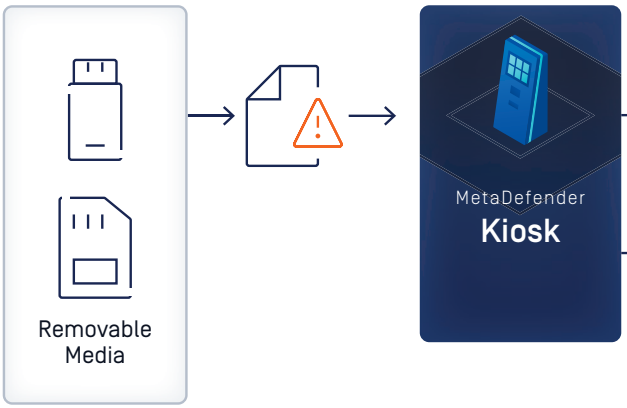
OPSWAT.

The Public Sector and Removable Media Cybersecurity

3 Reasons to Focus in 2024

The forms of removable media government and public sector entities rely on to update critical, air-gapped assets continue to be a substantial threat vector for bad actors to exploit. As technology advances and techniques grow in sophistication, removable media security cannot be ignored. Let's explore three compelling reasons government entities and public sector organizations need to focus on removable media cybersecurity in 2024 - and see how OPSWAT can help.

OPSWAT MetaDefender Threat Prevention



The best course of action for a comprehensive removable media security strategy is one that features defense-in-depth. Rather than relying on a single solution to cover one aspect of the complex challenges presented by the removable media threat landscape, the MetaDefender Platform offers multiple layers of defense, and is trusted globally by governments, institutions, and organizations to defend what's critical.

MetaDefender Kiosk

Trust at the point of entry, our industry leading Kiosk series scans removable media before it enters a secure network. With trusted technologies such as Deep CDR, Multiscanning (with 30+ AV engines), Proactive Data Loss Prevention, and more, known and unknown threats are neutralized, ensuring the files stored on the media are safe to use.

1 Data Breach Prevention

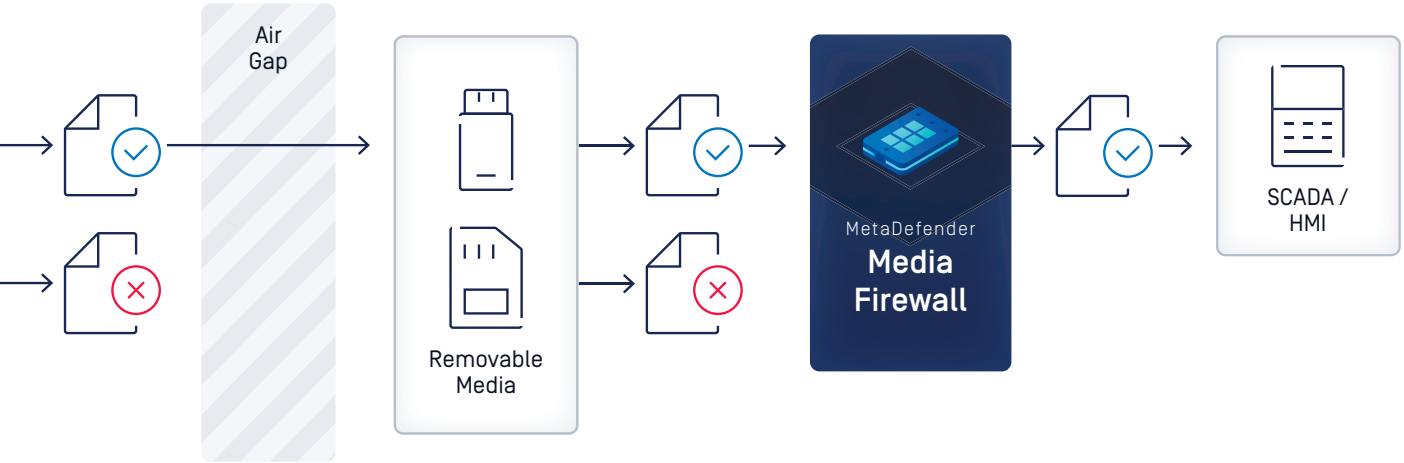
Government and public sector entities handle vast amounts of sensitive information, ranging from citizens' personal details to classified national security data. The utilization of removable media poses a substantial risk in terms of data breaches. Infiltration through infected USB drives or other external devices can lead to unauthorized access and potential leakage of sensitive data.

2 Mitigating Malware Threats

Malware attacks remain a persistent and evolving threat in the cybersecurity landscape. Removable media serves as a common vector for malware transmission. In a government or public sector setting, a single infected USB drive introduced into the system can compromise the entire network's integrity. Malware can not only disrupt operations but can also be designed to exfiltrate critical data or disrupt essential services.

3 Implementing Simple and Scalable Solutions

Governments and organizations in the public sector deal with high volumes of data moving through complex networks every day. That's why the removable media security strategy needs to be purpose-built for these environments: reliable, scalable, and simple to implement and maintain.



MetaDefender Media Firewall

Removable media security may start with Kiosk, but it ends with Media Firewall. This plug-and-play device enforces Kiosk's security by only allowing pre-scanned media to interact with essential endpoints, providing a critical layer of protection for assets on a secure network.

This only scratches the surface; discover why OPSWAT is the critical advantage in cybersecurity - scan the QR code for a free demo and see how we can start strengthening your perimeter of defense today.

https://opswat.com/get-started

CORPORATE PARTNER PROGRAM

As the largest dedicated cyber security association and peak industry body in Australia for information security, cyber security and privacy professionals, partnering with AISA is a great way for your organisation and staff to get involved and stay up to date with industry events, network with peers and learn more about an ever-changing field that is becoming more relevant by the day.

Partnering with AISA through our Partnership Program demonstrates your organisation's commitment to the cyber safety of Australians and highlights your organisation's efforts as a responsible corporate citizen.

COMPLIMENTARY AISA MEMBERSHIP

As an AISA Partner, your organisation can register any staff from the cyber security, IT, governance, risk and law functions as AISA members.

THOUGHT LEADERSHIP

As a Corporate Partner, you will have the opportunity to provide thought-leadership articles, case studies and white papers to the AISA community via the fortnightly member newsletter and print publications.

COMPLIMENTARY ACCESS TO BRANCH MEETINGS AND EVENTS

Your team will be able to engage and access the monthly branch meetings, webinars, presentations, recordings and resources.

AUSTRALIAN CYBER CONFERENCE COMPLIMENTARY PASSES

As a partner, AISA will provide your organisation with complimentary passes to attend our Australian Cyber Conference. These passes can be used by your organisation's staff or can be used to invite your customers or partners.

- Includes guaranteed early bird discounts to all AISA conferences
- Discounts on conference booth sponsorship

DISCOUNTED TRAINING & CERTIFICATION COURSES

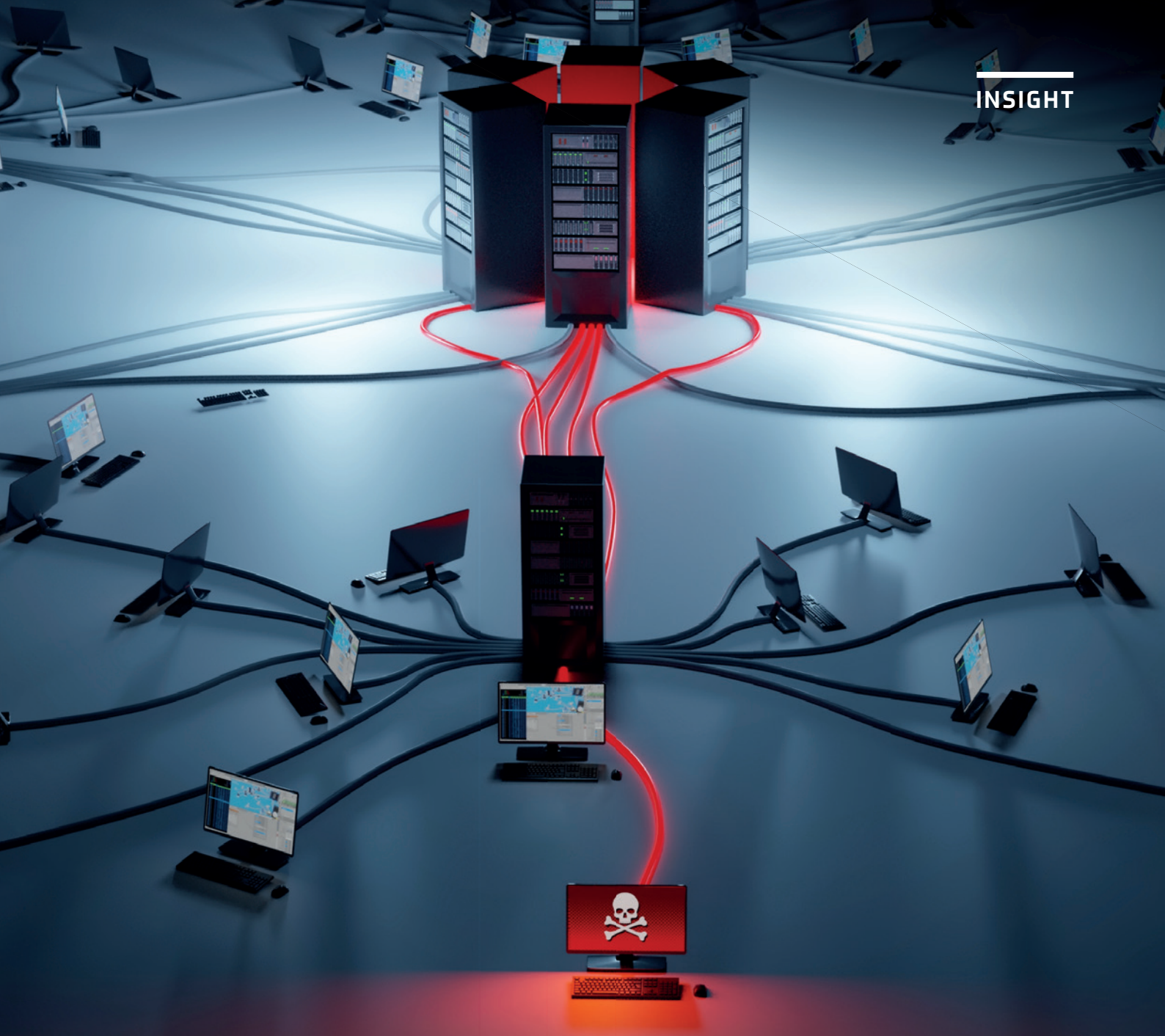
Obtain discounts on professional education training, skills development and certification courses via AISA's extensive network of partners including SANS, BSI, ALC, (ISC)², CompTIA and RMIA.

WE HAVE PACKAGES TO SUIT ALL ORGANISATION TYPES. SPEAK WITH US ABOUT TAILORING A PACKAGE FOR YOU.

FOR MORE INFORMATION:

cpp@aisa.org.au
www.aisa.org.au/CorporatePartners

AISA Australian Information Security Association



Acknowledging our faults

BY **TOBY AMODIO, FORMER CISO FOR AUSTRALIAN PARLIAMENT HOUSE**

One of my colleagues started a meeting recently by asking the group to be vulnerable – open to talking freely in the session. Being in cyber security, this provoked laughter about the need to be vulnerable about our vulnerabilities.

Toby Amodio

What I mean by this is the necessity to acknowledge the weakness of a system in order to facilitate remediation. While the session went on a separate tangent, this concept stuck with me. The challenge of being vulnerable about being vulnerable is at the core of many of the issues across government cyber security.

For better or worse, government cyber security team performance is often measured in reputation rather than risk. Being divorced from many of the financial realities that face businesses (the tax office isn't going to go out of business) means that reputation often plays a greater role in measuring success for senior executives and the agencies. Many public service careers are built or destroyed on the back of bad press. This means that perceived success or failure is often linked to events that shape your reputation.

Your cyber reputation in government is most often affected in one of three 'cyber' events: a breach of your systems/data, an externally visible audit, or as part of your mandatory reporting. They each have their own challenges, but managing your reputation throughout can be a double-edged sword.

Breaches are a fact of life and a reflection of the defender's dilemma – the defender must get it right 100 per cent of the time, and the attacker only needs to get it right once. Despite this, the narrative is often centred on blaming the victim following breaches. The story will focus on the missing controls, not the challenges that exist in implementing those controls across a complex ecosystem with 100 per cent efficacy. You would never blame a person in a pub for being sucker punched, so we should not blame the compromised entity.

This victim shaming of organisations that share that they have been impacted depresses incentive for people to voluntarily come forward, which, in turn, restricts the sharing of valuable lessons learnt. In the inverse, people are rewarded reputationally by not coming forward. It also reduces the greater community understanding of cyber attacks, which can provide a false narrative that everyone is doing fine.

Continuing the theme of visibility, externally reported audits provide public transparency of government entities. The flip side is that, often due to constrained budgets, these audits must be prioritised, which leads to agencies focusing on beating the audit, not managing risk. It's like studying for the test but not the life that comes after the test. Being publicly named and shamed in an audit result often leads to pressure on the cyber team, rather than the entities within the organisation who failed to maintain the controls. This is also not met with mandatory, ear-marked investment from the government, which can fund remediation or uplift. It's one thing to point out an issue, but those areas need support to remediate the issue.

Lastly, reporting in government is critical, and the annual compliance report can make or break cyber careers. Unfortunately, due to cross-agency visibility and ministerial or executive reporting, there is often a strong desire in executive groups to shape reporting. This is often achieved through selective scoping, creative interpretation and misrepresenting posture. Complement this with a constantly shifting compliance bar, and it proves to be a rod for the back of the cyber security leader, whose role is often to tell their boss how ugly their baby is.

This desire to minimise reputational hit has serious consequences for us as a profession. Without fear and frank transparency about the scale of the challenges facing government cyber, we cannot mobilise the resources to reduce risk. In turn, we fight our battles in isolation.

Without transparency, we cannot learn from each other's incidents to achieve the economies of scale in defence; we cannot use our audit processes to drive investment in the areas of most need; and we cannot empower the coordination agencies with the data to support whole-of-government uplift.

Only together can we build resilient systems, and this includes being vulnerable about our vulnerabilities so that we can work together to address them.

About the author

Toby Amodio *is a trusted cyber leader with a proven history of building strong capabilities. He has led large, diverse and geographically dispersed teams to protect, detect, and respond to the cyber challenges facing government. Amodio has previously held CISO roles at the Department of Parliamentary Services and the Australian Taxation Office. He is currently consulting for the federal government.*

State-of-the-art cyberthreats demand state-of-the-art cyber security

BY **SIMON GALBALLY**

Commercial and government cyber defences are successfully attacked daily; but what is unacceptable is that, too often, these attacks involve successful breaches of unencrypted, sensitive data. Thousands, if not millions, of records are routinely compromised, with damage extending throughout the digital supply chain.

As the sophistication of cyber attacks grows, so should the sophistication of cyber defences. Unfortunately, the reality is different. Many of today's breach nightmares result from cybercriminals exploiting vulnerabilities of outdated 'legacy' defences simply not fit for purpose. The Microsoft, Dropbox and MOVEit disasters highlight the problem. In the case of MOVEit, the scale is yet to be quantified, but at the time of writing, over 2000 companies and 60 million data records have been compromised.

The biggest issue is that, too often, sensitive data remains unencrypted, especially in the face of today's cyberthreats. Only when encrypted is the data secure and useless in the hands of cybercriminals – whether in use, stored at rest or in motion across public and private networks.

PROTECTION VERSUS PREVENTION

Like all criminals, hackers are always one step ahead – identifying and exploiting vulnerabilities faster than cyber defences can plug the gaps. Plan A should be optimising 'prevention' defences. Plan B acknowledges that breaches are inevitable and focuses on encrypting data should the worst happen. To succeed, both plans must not rely upon legacy solutions that constantly play catch-up.

One such example is Senetas CypherNET, which protects data in motion across network infrastructures where it is vulnerable to hackers. Used by the world's most secure commercial, government and defence organisations, it provides maximum encryption and data authentication across all network types. Data networks are not inherently secure – among business locations, data centres, to/within/from the cloud and to the last mile of business, defence and critical infrastructure operations. State-of-the-art CypherNET also provides quantum resistance to protect today's data from future quantum threats.

Another example is Votiro Zero Trust, a service providing real-time, Zero Trust content security, which leverages its patented consumer data right technology to protect against all file-born attacks, both known and unknown. Key to Votiro's success is the fact that it doesn't need to rely upon the existence of a known malware signature to identify a threat – protecting against signatureless and zero-day exploits.

Then there is SureDrop, the only secure encrypted file sharing, storage and collaboration platform that enables 100 per cent location control and data sovereignty. Built on cyber security principles, it provides the maximum security necessary in our remote working and digital communications world. Sharing confidential documents by email or using public file sharing and storage services are unsecure practices.

The evolving cyberthreat landscape requires cyber security solutions to offer more than the ability to shut the stable door after the horse has bolted. State-of-the-art cyberthreats demand state-of-the-art cyber security.

Revised Essential Eight guidelines reflect the evolving cyber security threat landscape

BY **SCOTT HESFORD, SENIOR DIRECTOR, SOLUTIONS ENGINEERING, APJ, BEYONDTRUST**

Developed by the Australian Cyber Security Centre (ACSC), the Essential Eight has provided guidance for public-sector agencies for well over a decade.

By implementing the security recommendations contained within the guidelines, organisations can significantly improve their cyber posture – specific to the most common attacks identified by the ACSC – and make it much more difficult for adversaries to compromise key IT resources.

The Essential Eight Maturity Model defines four maturity levels, ranked on a scale from zero to three, based on an organisation's ability to identify its risk exposure and take the necessary steps.

To ensure the Essential Eight continues to deliver the best possible protection, it is regularly updated, with the most recent changes being published in November last year. Three of the most important updates were:

1. RESTRICT ADMIN PRIVILEGES

The Essential Eight Maturity Model introduced a number of changes related to the restriction of admin privileges within IT infrastructures. Users with this level of access are regularly targeted by cybercriminals keen to steal their credentials and use them to mount attacks.

The changes are focused on consistently granting, controlling, and rescinding privileged access to systems and applications. These management guidelines have also been amended to reflect the growing usage of cloud services.

2. INTRODUCE A NEW MINIMUM STANDARD FOR MULTI-FACTOR AUTHENTICATION

For organisations at lower maturity levels, the Essential Eight now encourages the adoption of phishing-resistant forms of multi-factor authentication (MFA). It also provides enforcement for organisations aligning to higher maturity levels. Organisations are recommended to deploy tools that allow granular control over where MFA is enforced for privileged access. Some tools also leverage security keys as part of application control and are able to apply MFA, even where applications are not MFA aware. These capabilities provide users with a level of authentication that otherwise would not have been achievable.

3. DEPLOY NEW APPLICATION CONTROL REQUIREMENTS AT LEVEL TWO

The changes in requirements for application control reflect the increased use by cybercriminals of 'living off the land' techniques in their attacks. The Essential Eight now requires the implementation of Microsoft's recommended application blocklist at level two instead of the previous level three, with organisations performing annual reviews of application control rule sets.

Now that the ACSC has updated both application control and restricting admin privileges, it highlights the value of a holistic solution that performs both functions. At the same time, it removes the need to circumvent the controls on restricting admin rights by granting local admin rights for exceptions.

By undertaking these recommended steps, organisations can further strengthen their protection against constantly evolving cyber security threats. Just as the Essential Eight continues to evolve, so too must chosen protective measures. This will ensure that critical applications and data remain secure, and day-to-day operations can continue without disruption.

BeyondTrust

Achieving Essential Eight Compliance with BeyondTrust

For government departments and agencies, aligning to the requirements of the Australian Cyber Security Centre's (ACSC's) Essential Eight can be a challenge.

Application control, together with properly secured privileged accounts and access, plays a significant role in mitigating the risks associated with many of today's most common threats. BeyondTrust's market-leading Privileged Access Management (PAM) solutions enable these capabilities and more, aligning your organisation's security posture closely to the demands of the Essential Eight Maturity Model.

Scan the QR code to learn more!

beyondtrust.com/essential8

Government cyber guidance is only the beginning

Boosting security requires a multifaceted approach.

Current cyber security best practice standards have been 'politicised', and fail to address the 'big disconnect' between stated ideals and real-world operating conditions, a senior cyber security expert has warned.

That disconnect has worsened, as efforts to simplify security guidelines – the hundreds of controls of the Information Security Manual, which gave way to the Australian Signals Directorate's Top 35 Mitigation Strategies, which was then distilled into the Essential Eight – reduced security compliance to a 'tick-box perspective'. According to Trend Micro Managing Director of ANZ Commercial Business Srujan Talakokkula, that is no longer suitable for today's complex hybrid cloud and on-premises environments.

'Tick-box compliance doesn't really keep up with the landscape that we're seeing, as people have moved from traditional environments,' Talakokkula explains.

'It's predominantly built around Microsoft endpoints and a few basic features around that – but as we move into more complex ecosystems built around cloud and serverless architectures, and everything else, those controls haven't really kept up.'

The newly released 2023–2030 Australian Cyber Security Strategy has introduced yet another paradigm – the 'six shields' approach to mapping and addressing security risk points.

But given the heavily politicised approach that shaped the plan and the fact that it represents, according to Talakokkula, probably a five- to 10-year cultural change, 'there's still a big disconnect between what those six shields look like, what agencies and organisations need, and who they need to partner with.'

Close scrutiny of several recent major cyber attacks shows that neither the six shields nor the Essential Eight would likely have prevented the compromises, says Talakokkula, arguing that governments need specialists to adapt such guidelines to departments' specific needs.

HELP WHERE IT'S NEEDED

Limited resources mean that organisations, such as the Australian Cyber Security Centre, 'can't get involved in all the other breaches that are disrupting the bottom end of the market'. This includes small businesses, small government agencies and more, and Talakokkula believes that the Cyber Security Strategy will create 'a bit of a vacuum' as centralised security operations absorb skilled cyber security specialists.

This will create opportunities for managed service provider partners to help businesses and government bodies balance security, artificial intelligence analytics, and automation capabilities, while addressing challenges educating and retaining key staff.

'The strategy isn't going to suddenly give agencies something that's going to help them achieve cyber resilience,' Talakokkula explains. '[The] government has to start balancing cost versus benefit, and not seeing cyber as a cost or a necessary evil, or something where they implement antivirus software and feel they're good to go.'

A truly secure government will also require mature privacy practices, with General Data Protection Regulation–level privacy protections 'encouraging us to be really careful about why we're collecting data, and what we're collecting it for.' S

TREND MICRO™

Cybersecurity Platform for Federal Government Agencies and Departments

Helping you meet compliance requirements

Leveraging our 30+ years of cybersecurity expertise, we bring the highest level of protection, detection, and response to federal and compliance-driven organisations

TrendMicro.com

Fighting Cybercrime Globally, Trusted By

INTERPOL

Forrester's 2024 cyber security predictions

BY **JINAN BUDGE, VICE PRESIDENT AND PRINCIPAL ANALYST, FORRESTER**

Balance speed of innovation with accountability and governance. Talent crunches, evolving threats, emerging technologies, and regulatory sprawl are the conventional problems that have plagued security leaders for decades; but in 2023 in Australia, these problems have collided.

Jinan Budge

Until recently, Australia has largely avoided global breach headlines and regulator attention. That is until 2021 and 2022, when 31 per cent of the 55 most notable breaches in our research were from the Asia-Pacific region, with some well-documented breaches from within Australia. Regional regulators, including in Australia, could no longer ignore these breaches, with India, Singapore and Japan also strengthening their regulations. As well as releasing its 2023–2030 Australian Cyber Security Strategy, Australia has refreshed its Essential Eight threat-mitigation strategies; implemented industry-focused regulations, such as the *Security of Critical Infrastructure Act* and Prudential Standard CPS 234 Information Security; and will soon overhaul its *Privacy Act*.

To make matters more interesting, emerging tech in the form of generative artificial intelligence (genAI) has surfaced, bringing renewed optimism and excitement, new threats, and new ways to deal with those threats. It's inevitable that, as governments, businesses, and citizens embrace rapid experimentation of genAI in 2024, they also must make sure they balance this speed of innovation with greater accountability and governance.

CISOs are already stretched and fatigued dealing with these dynamics on the smell of an oily rag – constrained budgets, a resource gap and, often, a lack of buy-in. With this environment as a backdrop, in 2024, Forrester predicts the following.

NINETY PER CENT OF DATA BREACHES WILL INCLUDE A HUMAN ELEMENT

Breach publications and industry sources estimate that up to 74 per cent of breaches include a human element, where people are involved in the error, misuse, stolen credentials, or social engineering used in the breach. Even technically focused industry groups now acknowledge the role of humans in exploiting tech. The percentage of breaches that include a human element will increase even further in 2024, due to the impact of genAI and the prevalence of communication channels that make social engineering attacks simpler and

faster. This increase will expose one of the touted silver bullets for mitigating human breaches: security awareness and training. As a result, more CISOs will shift their focus to an adaptive human protection approach in 2024, as the National Institute of Standards and Technology (NIST) updates its guidance on awareness and training, and as more human quantification vendors emerge.

ROLES WITH ZERO TRUST TITLES WILL DOUBLE ACROSS PUBLIC AND PRIVATE SECTORS IN SOME COUNTRIES, AND EMERGE IN OTHERS (SUCH AS AUSTRALIA)

In November 2023, there were 83 Zero Trust positions advertised on LinkedIn in the United States, four in India, one in Singapore, and zero in Australia. We expect that to change in 2024. Why? The explosion of Zero Trust mandates and executive orders in the United States; the release of Australia's 2023–2030 Australian Cyber Security Strategy with its intent to draw on internationally recognised approaches, such as Zero Trust; the Zero Trust framework finally going mainstream in the Asia Pacific and Europe, the Middle East, and Africa; and a broad adoption of the NIST's Zero Trust Architecture framework will all spur a need for cyber security roles. These roles will be dedicated to Zero Trust architecture, engineering, governance, strategy and leadership. The roles won't just be in government; in fact, they can't be. The commercial Zero Trust adoption landscape will be changed. Providers to government will need to upskill their Zero Trust workforce, as will non-government enterprises. In Australia, the government has identified 11 key sectors and 22 sub-assets as part of the nation's critical infrastructure, including communications, water, health and medical. In the United States, these private sector enterprises are responsible for supporting 85 per cent of the United States' critical infrastructure.

AT LEAST THREE DATA BREACHES WILL BE PUBLICLY BLAMED ON AI-GENERATED CODE

As developers embrace AI development assistants known as TuringBots to generate code and boost productivity, the most conscientious organisations will scan that code for security flaws. Unfortunately, some

overconfident development teams will trust that AI-generated code is secure. At the same time, many technology leaders will wonder about the generated code's security – which is understandable, given significant application programming interface misuse rates in large language models' responses to Stack Overflow questions. Without proper guardrails around TuringBot-generated code, Forrester predicts that, in 2024, at least three data breaches will be publicly blamed on insecure AI-generated code – either due to security flaws in the generated code itself, or vulnerabilities in AI-suggested dependencies.

About the author

Jinan Budge *leads Forrester's security and risk research in the Asia Pacific. Budge's research focuses on enabling CISOs and technology executives to lead a high-performing security organisation and culture. She globally leads Forrester's awareness, behaviour and culture coverage, using strategic and innovating thinking to shape the market. She is also an advocate for diversity and inclusion in security. Budge focuses on ensuring that cyber security teams not only attract talent, but also retain the best talent, and she brings a local and global perspective and cultural lens to her research and practice.*

What can cyber security learn from safety and reliability engineering?

BY **DR IVANO BONGIOVANNI, SENIOR LECTURER, INFORMATION SECURITY, THE UNIVERSITY OF QUEENSLAND**


Dr Ivano Bongiovanni

When he gave his keynote presentation at CyberCon 2022, Captain Chesley 'Sully' Sullenberger, renowned for his heroic landing on the Hudson River, brought an intriguing perspective into a global cyber security conference. He proposed parallels between the principles of high-reliability organisations and their potential application in cyber security, revamping a dialogue on learning from other disciplines, which the cyber security world has been traditionally a bit deaf to.

This article delves into how the matured field of safety and reliability engineering can inspire cyber security practices.

HISTORICAL DISASTERS: LESSONS IN SAFETY AND RELIABILITY

This story begins between the end of the 1970s and the 1980s, when the world was shaken by a series of catastrophic industrial accidents resulting in thousands of casualties; dramatic, long-lasting effects on affected populations; and incalculable economic damage.

Seveso, Bhopal, Three Mile Island and Chernobyl were not merely catastrophic events; they were also instrumental in revolutionising our understanding of safety and reliability in complex systems.

First, in 1976, a chemical plant in Seveso, Italy, inadvertently released a toxic cloud of dioxin, leading to widespread environmental contamination and health hazards. This incident underscored the need for stringent safety measures in chemical manufacturing and environmental protection laws.

To date, the most serious commercial nuclear accident that occurred on American soil was the Three Mile Island accident in 1979 (an event also made famous by a recent Netflix series), which involved the partial meltdown of a reactor at a nuclear power plant in Pennsylvania. It exposed the vulnerabilities in nuclear power plant design and operational protocols, prompting a re-evaluation of nuclear safety and emergency procedures.

In 1984, what is considered by most as the largest industrial accident ever recorded, occurred in Bhopal, India. A gas leak at a pesticide plant released methyl isocyanate, resulting in thousands of deaths and long-term health issues. This tragedy highlighted the critical need for robust safety systems and emergency response strategies in the chemical industry.

Finally, probably the most notorious on this list, is the Chernobyl disaster in 1986. The explosion and subsequent meltdown at the Chernobyl nuclear plant in Ukraine represented the most severe nuclear disaster in history. It demonstrated the catastrophic potential of nuclear energy when safety systems fail, leading to significant reforms in global nuclear safety standards.

In dramatic circumstances, the four events built further momentum to work on expanding our understanding of how large-scale accidents unfold, what their root causes are, and what measures can be taken to mitigate their consequences.

In fact, significant progress in this area had been made well before the unfolding of those industrial disasters.

In 1978, a British author and journalist, Barry A. Turner, published, together with Nick Pidgeon, a book that would become a milestone in the study of industrial disasters and risk management in general. *Man-Made Disasters* (originally subtitled 'The Failure of Foresight') was one of the first publications to explicitly acknowledge the common, slow-burning build-up of unnoticed or unaddressed failures, leading to an industrial disaster. In his work, Turner emphasised the role of organisational and human factors, highlighting the importance of understanding organisational culture and communication in preventing disasters, or mitigating their consequences. *Man-Made Disasters* was also one of the first books to theorise the concept of 'safety culture' – an organisational culture in which a focus on safety permeates the shared beliefs, practices, and attitudes. It also lead to engagement with, and integration of, safety practices at all organisational levels – from operations to strategy.

Another milestone in the safety and reliability engineering literature, sociologist Charles Perrow's *Normal Accidents* unpacked how complexity of modern organisations has the potential to lead to accidents that, despite common belief, are not unusual, and are, in fact, 'normal' in the grander scheme of things. Perrow's work introduced the concepts of 'tight coupling' and 'interactive complexity' in complex systems. Tight coupling refers to

systems where processes are closely linked in a sequence, with each step dependent on the preceding one, leaving little room for error or delay without affecting the entire system. Interactive complexity pertains to systems with numerous components and interconnections, where interactions can be unpredictable and unintended consequences can arise, making it difficult to foresee all potential failure modes. Perrow argued that in systems characterised by both tight coupling and interactive complexity, accidents are not just possible, but are also inevitable. Following in the footsteps of Turner, Perrow acknowledged that organisational practices and process – such as inadequate internal communication, suboptimal supervision and counterproductive culture – can become co-determinants in major accidents.

Turner and Perrow's work led to a shift in focus from individual component failures to broader systemic issues, translating to the need for a holistic approach to safety that considers human, organisational, and technical factors in system design, operation, and maintenance.

GETTING OUR HOUSE IN ORDER: SOME MUCH-NEEDED DEFINITIONS

Nancy Leveson, a Massachusetts Institute of Technology Professor, is one of the most eminent living researchers in the field of safety and reliability engineering. In her seminal work *Engineering a Safer World: Systems Thinking Applied to Safety*, Leveson defines safety as a 'freedom from accidents (loss events)'. In Leveson's work, safety is therefore a systemic feature, one intrinsically determined by a system's design. Designing for safety is about ensuring that a system or process operates without causing unacceptable risk of harm to people or the environment.

According to Patrick O'Connor and Andre Kleyner in *Practical Reliability Engineering*, reliability is 'the probability that an item will perform a required function without failure under stated conditions for a stated period of time'. This definition underscores the importance of consistent performance and dependability in engineering systems.

While being distinct concepts, safety and reliability are deeply interconnected. A reliable system is often a prerequisite for a safe system, but a reliable system is not necessarily safe. For instance, a system can reliably perform a dangerous operation, which would not be considered safe. Conversely, a safe system's reliability may be hampered by fail-safes that shut down the system under certain conditions to prevent harm.

So, what does this all have to do with cyber security?

Well, it all boils down to the essence of security itself: safety accidents happen in the absence of human intent; security events happen only when human intent is present.

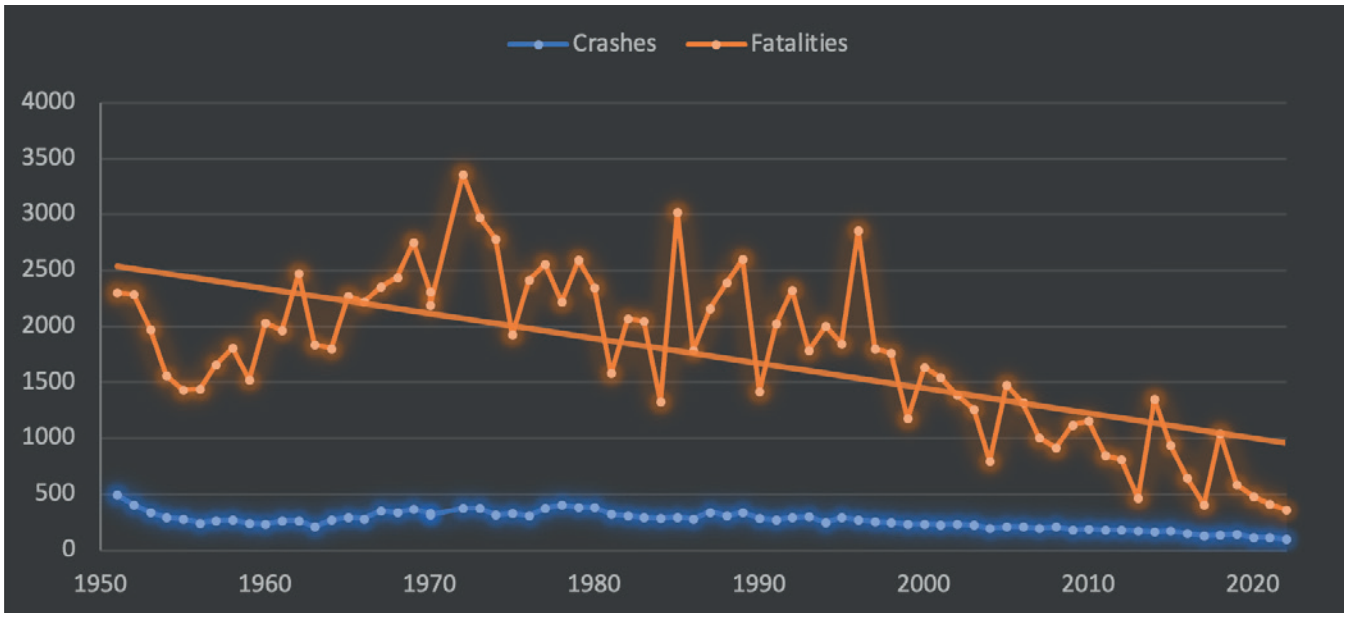


FIGURE 1. CRASHES AND FATALITIES IN AVIATION, GLOBAL (1950–2022). DATA FROM WWW.BAAA-ACRO.COM

To put it differently, from a safety engineering perspective, safety and security are simply two facets of the same token. Security merely adds the component of intentionality (cybercriminals' intent). Yet, safety engineering would nonetheless focus on designing-out, or mitigating, the impact of adverse events, regardless of perpetrators' intentions, capabilities, motives, etc.

CONTRASTING TRAJECTORIES: AVIATION SAFETY VERSUS CYBER SECURITY CHALLENGES

For simplicity, let's examine an industry that deals with safety, security (and reliability) on a daily basis: aviation. The contrasting paths of aviation safety and cyber security offer a stark illustration of how different sectors can evolve in response to safety and security challenges. As a domain, aviation has the potential to be a 'hotspot' for safety and reliability engineering issues: using Perrow's lessons, its operations tend to be interactively complex and systemic components (think of an airport) are tightly coupled. Nonetheless, aviation has achieved remarkable success in reducing accidents and enhancing safety.

Aviation's journey since the 1950s demonstrates a commitment to safety, marked by technological advancements, regulatory oversight, a strong safety culture, and an emphasis on human factors and training. Innovations in aircraft design and systems, stringent regulations by bodies like the Federal Aviation Administration and the International Civil Aviation Organization (ICAO), and a culture that encourages learning and information sharing have been instrumental to this. The industry's focus is on technical expertise, as well as on human factors – as exemplified by comprehensive crew training programs. As an example, ICAO's Annex 6 to the Convention on International Civil Aviation states that 'an operator shall establish and maintain a ground and flight training program, approved by the State of the Operator ... The training program shall ... include training in knowledge and skills related to human performance' (ICAO Annex 6, Part 1, Chapter 9, Para 9.3.1). This, together with the use of more advanced flight simulators, has significantly reduced aviation accidents and fatalities across the years (Figure 1).

On the other hand, the cyber security world struggles with an ever-escalating trend in data breaches. According to research by IBM and the Ponemon Institute, the global average cost of data breaches increased by

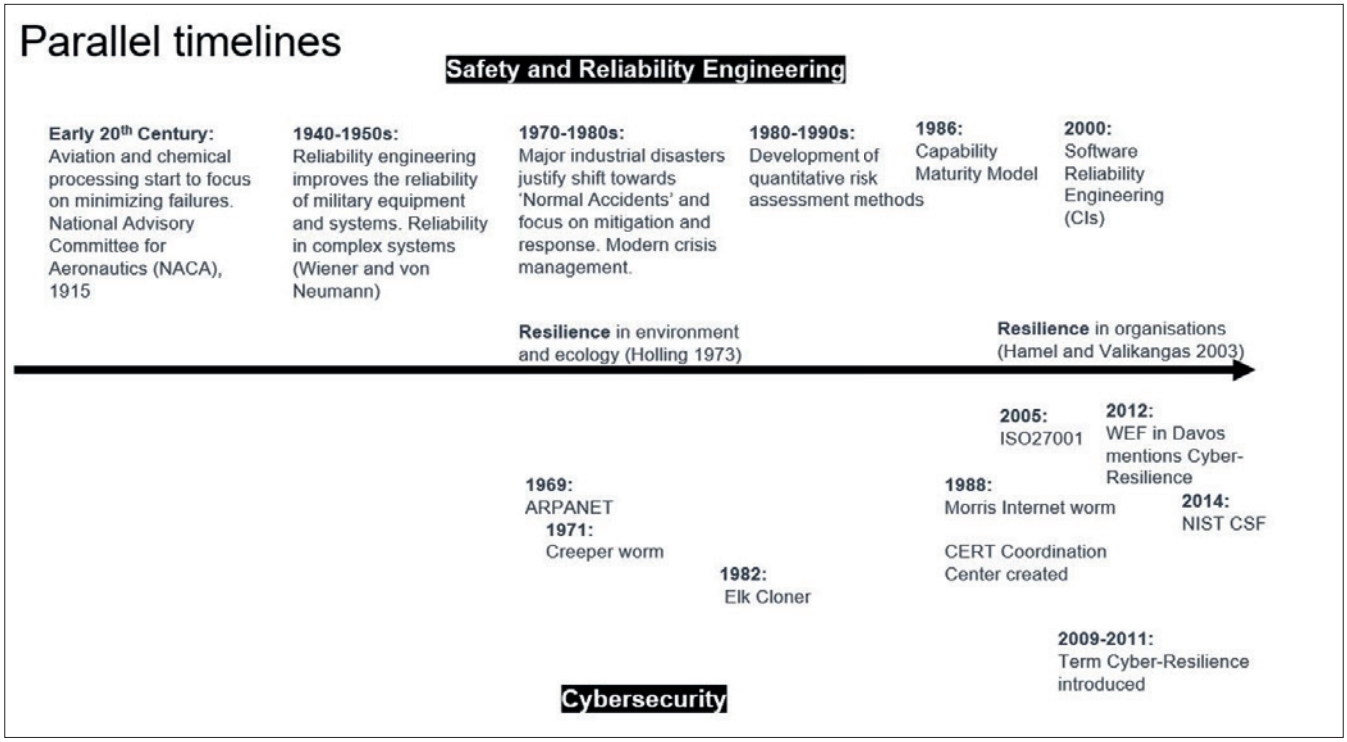


FIGURE 2. PARALLEL TIMELINES BETWEEN SAFETY AND RELIABILITY ENGINEERING, AND CYBER SECURITY

2.3 per cent in 2023 as compared to 2022, landing at US$4.45 million (https://www.ibm.com/reports/data-breach).

Cyber security is a rapidly evolving field. It is often outpaced by the technologies it seeks to protect and is complicated by a generic lack of unified regulatory frameworks, by the complexity and interconnectedness of digital systems, by a significant skills gap, and by an ever-evolving threat landscape that contributes to the increasing frequency and severity of cyber incidents. Unlike aviation, where changes are more gradual and regulations are hyper-responsive, cyber security must contend with fast-paced threats.

ARE THERE COMMONALITIES IN THE ADVANCEMENTS THAT SAFETY AND RELIABILITY ENGINEERING AND CYBER SECURITY EXPERIENCED?

There certainly are. Generally speaking, safety and reliability engineering have crossed similar milestones to the cyber security world, but some decades in advance. An example of this is the concept of resilience. As we know in cyber security, cyber-resilience stems from the consideration that 100 per cent security is virtually impossible and resources need to be invested not just in prevention and preparation, but also in response and recovery. Now, it is difficult to identify when the concept of cyber-resilience was first used, but probably around 2009–11 is when it first started to get traction.

In the physical world – in ecology, in particular – resilience was a concept introduced in the 1970s to identify the capacity of an ecosystem to respond to disturbance and maintain functionality under duress.

Figure 2 represents the two parallel time lines of safety and reliability engineering, and cyber security. The commonalities, with a time lag, are undeniable.

WHAT ARE THE LESSONS FOR CYBER SECURITY?

Advancements in safety and reliability have allowed the aviation industry to dramatically reduce the number of losses (human or otherwise) across the decades. So, what lessons and principles can cyber security extract from safety and reliability engineering?

SYSTEMS THINKING APPROACH

A fundamental principle in safety engineering is the adoption of systems thinking. This approach involves understanding and addressing the cyber security challenges not just at the component level, but also as part of the entire system, including its interactions, dependencies, and the broader context in which it operates. Interactive complexity means that simply breaking down complex systems (e.g., infrastructure, processes, humans, etc.) and addressing them one by one would lead us to overlook unexpected dependencies. Systems thinking enables cyber security professionals to identify potential vulnerabilities and interdependencies that might not be apparent when focusing on individual elements. It encourages a holistic view, considering how different parts of a system can affect each other and the system's overall behaviour, especially under attack.

CULTIVATING A SAFETY CULTURE

In safety engineering, a strong safety culture is paramount. This involves creating an environment where safety is prioritised, and every individual – from top management to operational staff – is encouraged to take responsibility for it. Translating this to cyber security means fostering a culture where security concerns – actual events as well as near misses – are openly discussed, and employees are encouraged to report potential vulnerabilities without fear of reprisal. It also involves regular training and awareness programs to keep all staff updated on the latest security practices and threats.

LEARNING FROM ACCIDENT MODELS

Safety engineering has developed various accident models, such as Leveson's Systems-Theoretic Accident Model and Processes (STAMP), which provide frameworks for analysing accidents and near misses, both ex post and ex ante. Applying these models to cyber security can help in understanding the complex interactions within digital systems and the human factors that contribute to security breaches. These models emphasise the importance of looking beyond immediate causes, and examining the underlying system structures and processes that

allow vulnerabilities to exist. In the United Kingdom, the National Cyber Security Centre has taken steps to implement STAMP-based frameworks to cyber security.

EMPHASIS ON SOFTWARE AND AUTOMATION SAFETY

In safety-critical applications, the reliability and safety of software and automated systems are paramount. Cyber security can learn from this by adopting rigorous software engineering practices, including formal methods for software verification and validation. This ensures that software used in critical infrastructures and services is robust against both unintentional faults and deliberate cyber attacks.

PROACTIVE REGULATION AND STANDARDS

Safety engineering recognises the role of proactive regulations and standards in preventing disasters. STAMP, for example, models how external factors (e.g., socio-economic circumstances and regulations) have the potential to impact the system's performance, including vulnerability to safety or security events. Cyber security can benefit from a similar approach, moving beyond compliance-based strategies to more proactive, system-oriented safety measures. This involves not only adhering to existing cyber security standards, but also actively participating in the development of new standards that address emerging threats and technologies.

CONTINUOUS LEARNING AND IMPROVEMENT

Preventing disasters in safety engineering is an ongoing process that involves continuous learning from past incidents or near misses. This principle can be effectively applied to cyber security, where it is crucial to conduct thorough investigations of security incidents, identify root causes, and implement corrective actions. Lessons learnt from past breaches should be used to inform future security strategies and improvements.

CONSIDERATION OF HUMAN FACTORS

Finally, the consideration of human factors is a critical aspect of safety engineering. This includes understanding how human operators interact with complex systems, and designing systems that support safe and effective human performance. In cyber security, this translates into designing user-friendly security systems and protocols that minimise the likelihood of human error, negligence or distraction, and training staff to minimise behaviours that could lead to organisational vulnerability to cyber attacks.

PRACTICAL STEPS FORWARD IN CYBER SECURITY

As we draw insights from the intersection of safety and reliability engineering with cyber security, it becomes clear that a proactive, systematic approach is essential for enhancing digital security. The lessons learnt from safety engineering can guide us in developing more robust and cyber-resilient organisations.

EMBRACING A HOLISTIC VIEW

Organisations should adopt a holistic view of cyber security, recognising that it is not just a technical issue, but is one that encompasses organisational culture, human factors, and operational practices. This means integrating cyber security considerations into all aspects of business operations and decision-making.

FOSTERING A CULTURE OF CONTINUOUS LEARNING

Just as safety engineering emphasises learning from past incidents, cyber

security must also be rooted in continuous learning and adaptation. Organisations should establish mechanisms for regular training, incident and near-miss reviews, and knowledge sharing to stay ahead of emerging cyberthreats.

INVESTING IN RESILIENCE

Preparation for potential cyber incidents is crucial. This involves not only implementing robust security measures, but also developing comprehensive incident response and recovery plans. Regular drills and tabletop simulations can help to ensure that these plans are effective, and that staff at all organisational levels are prepared to respond to breaches.

LEVERAGING EXPERTISE

Organisations should recognise the value of expertise in cyber security, ensuring that decision-making in crisis situations is informed by the most knowledgeable individuals. This may involve investing in specialised training for staff or partnering with external experts to enhance internal capabilities.

ADOPTING ADVANCED RISK ASSESSMENT TOOLS

Utilising advanced risk assessment tools and methodologies from safety engineering, such as STAMP, can provide deeper insights into potential vulnerabilities and help in developing more effective mitigation strategies.

COLLABORATION AND STANDARDISATION

Finally, collaboration across industries and adherence to standardised security protocols are key. Sharing knowledge and best practices can help organisations learn from each other, while standardisation ensures a consistent and effective approach to managing cyber risks.

About the author

Dr Ivano Bongiovanni *is a researcher, consultant, author and speaker whose work focuses on the managerial and business implications of cyber security. A senior lecturer in information security, governance and leadership with The University of Queensland (UQ) Business School and a member of UQ Cyber, Bongiovanni helps business leaders and executives make evidence-based decisions in cyber security. With a professional background in risk and security management, Bongiovanni's work bridges the gap between technical cyber security and its repercussions across organisations. He has advised ministers, policy-makers, board members, and senior executives on strategies, governance structures, policies, and training programs for effective cyber security management.*

High-security environments demand high-assurance network monitoring

Effective monitoring requires having the right data, not all of the data.

The time that cybercriminals spend on target networks may be dropping overall, but that's little consolation for government agencies. A lack of a well-integrated, robust data analytics architecture leaves government agencies struggling to meet statutory, compliance and operational security requirements.

'Data is becoming more prevalent and important in this day and age,' explains Rhys Thornton, Snare Product Lead with Prophecy International. Thornton notes that monitoring solutions can identify telltale behaviours that may indicate cyber security compromise.

'When you add real-time analytics and insight on top of that data, you can really start to build a picture – alerting mechanisms for threats that are unfolding within your environment.'

Developed in Australia 25 years ago, Snare grew out of close engagement with high-security government agencies. It has secured a range of high-security, high-assurance implementations based on its comprehensive network visibility, which is crucial, given the spread of government applications and data onto third-party cloud environments, and the surge in less formal 'shadow IT' systems.

'With the rise in cloud computing, there has been this real challenge where parts of the organisation could just go and use a service somewhere very quickly with an email address and a few details,' Thornton says.

Limited funding has compounded the problem.

'Do you collect everything, or just a filtered subset of the data to reduce costs? We see it all the time where budgetary pressures are winning this trade off, usually until it's too late,' he adds.

'Being able to monitor that filtered data is critical, which is why addressing customers' blind spots is a key focus – so we can help CISOs get complete network visibility and sleep better at night.'

Snare efficiently analyses, prioritises and summarises the most important environmental data, then feeds it into security information and event management (SIEM) systems.

As recent major breaches have shown, better data visibility helps to quickly identify network performance issues and breach indicators. With cybercriminals spending just 16 days on target networks in 2022 before being detected, down from 21 days in 2021, monitoring tools need to respond to network changes faster than ever.

Smarter collection, analysis and storage of operational data also helps manage data costs that 'are really starting to hurt', Thornton says.

'Everybody wants to ensure that there are no blind spots across the network,' he explains. 'But ultimately, for every piece of data you're collecting, there's a cost.

'We're trying to help customers keep long-term stores of their data at low cost, and also have the mechanisms to get that data into bigger SIEMs while ensuring we only send information that's forensically valuable into those solutions.' S

Sovereign vendor protecting critical infrastructure and organisations globally.

Enterprise logging without the pain

Enterprise log management from:

snare
A PROPHECY SOLUTION

Simplified collection | 90-97% storage savings
Zero ingestion pricing | Filter, transform, and enrich your data
Integration with major SIEMs | Compliance out-of-the-box

---

www.snaresolutions.com

Visit us at CyberCon

25-27 March 2024 Stand 51

National Convention Centre, Canberra

As Australia unveils its six cyber shields strategy, is data science poised as the pivotal seventh?

BY **DR JESSIE JAMIESON, STAFF RESEARCH ENGINEER – DECISION SCIENCE OPERATIONS, TENABLE**

As Australia fortifies its defences for upcoming cyberthreats, the government has launched the 'six cyber shields' initiative, central to its 2023–2030 Cyber Security Strategy.

Dr Jessie Jamieson

The 2023–2030 Australian Cyber Security Strategy outlines six crucial cyber defence tactics aimed at protecting citizens, businesses, and every level of government; however, the potential addition of a seventh shield, powered by data science, could be the pivotal move that elevates Australia to a top-tier cyber nation by 2030.

Leveraging data science not only enhances our defences, but it also transforms this information into a formidable countermeasure against our cyber enemies. The next frontier in cyber security isn't about standalone protective barriers; it's about cohesive, smart systems, with data science being the linchpin to this evolution.

UNRAVELLING COMPLEX THREAT PATTERNS

At the core of every cyberthreat lies a pattern – a sequence of events, behaviours or anomalies that hint at a potential security breach. Data science, with its analytical prowess, is uniquely equipped to detect and interpret these patterns. Advanced algorithms, especially when trained with

vast datasets, can predict threats even before they manifest, offering a proactive defence strategy. Instead of merely reacting to threats, organisations can now anticipate and neutralise them.

THE POWER OF PREDICTIVE ANALYSIS

Historical data is a treasure-trove of insights. By analysing past cyber attacks and their modalities, data science can identify vulnerabilities and predict possible future attack vectors. This predictive approach allows businesses to fortify potential breach points in advance, thereby drastically reducing the chances of successful attacks.

REAL-TIME THREAT DETECTION

One of the key strengths of data science in cyber security is real-time analysis. Machine learning models, trained on a range of data points, can continuously monitor network traffic, system behaviours, and user activities, instantly flagging anomalies. Such real-time alert mechanisms can be the difference between a minor security hiccup and a full-blown breach.

USER BEHAVIOUR ANALYTICS FOR ENHANCED SECURITY

Every user – be it an individual or a system process – exhibits a certain behaviour pattern when interacting with digital assets. By leveraging data science, organisations can develop a clear behavioural baseline for each user. Deviations from this baseline – such as unusual access times, data requests or abnormal transaction volumes – can be flagged for review. This not only aids in detecting external threats, but it's also especially potent against insider threats.

OPTIMISING INCIDENT RESPONSES

A common challenge in cyber security is the sheer volume of alerts and false positives. Data science assists teams in prioritising these alerts based on potential impact and severity. By categorising and ranking threats, security professionals can focus on the most critical issues first, ensuring efficient allocation of resources and minimising damage.

DECIPHERING THE DARK WEB

The vast, unindexed part of the internet, commonly referred to as the 'dark web', is a breeding ground for cyberthreats. Advanced data science tools, coupled with natural language processing, can scan and analyse data from these regions, identifying potential threats, leaked credentials or emerging attack methodologies.

ENHANCING ENCRYPTION TECHNIQUES

Encryption is the bedrock of digital security. With quantum computing on the horizon, current encryption techniques might become vulnerable. Data scientists are at the forefront of developing new algorithms and cryptographic methods to stay ahead of the potential decryption capabilities of quantum machines.

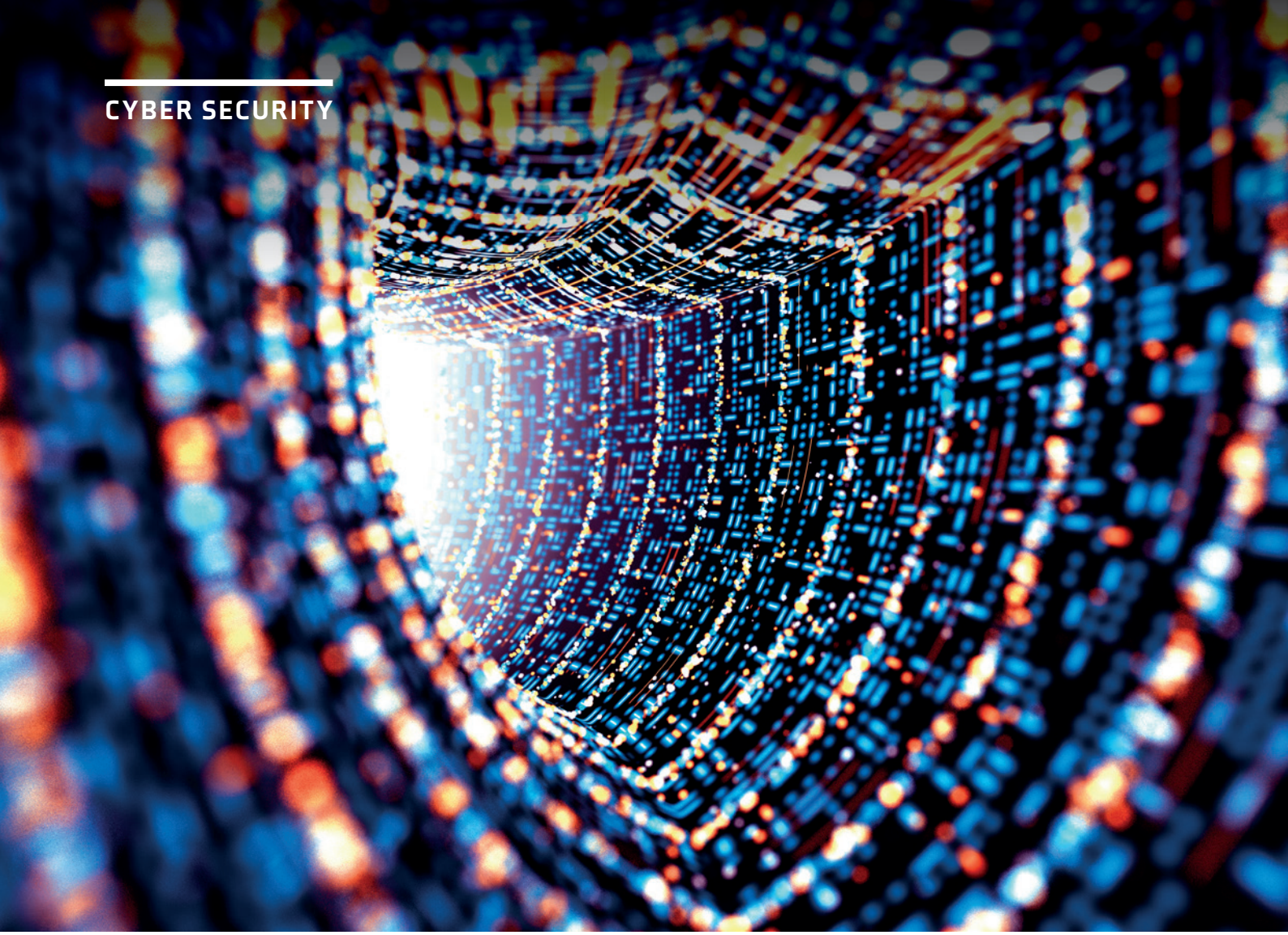
BUILDING A RESILIENT CYBER ECOSYSTEM

The synergy of data science and cyber security extends beyond just defence. It creates a resilient cyber ecosystem where threats are not just identified, but also learnt from. Each attack, attempted breach or vulnerability becomes a lesson, feeding into the models to refine and enhance them. Over time, this creates a self-evolving defence mechanism, adapting to the ever-changing cyber landscape.

As cyberthreats grow in sophistication, the solutions to combat them must evolve, too. Designating data science as a seventh shield offers a fresh perspective on cyber security. The fusion of data science and cyber security isn't just a technological integration; it's a paradigm shift. It moves the narrative from vulnerability to resilience, and from reaction to anticipation. S

About the author

Dr Jessie Jamieson *is a mathematician and senior research engineer at Tenable, Inc., where she assists with research efforts and drives the innovation of decision support analytics for the organisation. She is the author of numerous scientific articles and, most recently, led Tenable's data analysis effort concerning continued prevalence of Log4j vulnerabilities. During her graduate studies, she held internships at the NASA Goddard Space Flight Center and Oak Ridge National Laboratory, the latter of which being where she first delved into cyber security by cooperating with the lab's security operations centre to develop machine-learning solutions for rapid case classification.*



Building resilience: a multi-tiered cyber security response approach

BY **NIGEL PHAIR, PROFESSOR, MONASH UNIVERSITY**

The recently released 2023–2030 Australian Cyber Security Strategy is a road map that aims to make Australia a world leader in cyber security by 2030.

The strategy is built around six cyber shields, each of which provides an additional layer of defence against cyberthreats, and places Australian citizens and businesses at its core. The strategy aims to develop national frameworks to respond to major cyber incidents, and bring about community awareness and victim support, investment in the cyber security ecosystem, and design and sustainment in new security technologies, while also implementing governance and ongoing evaluation.

As part of Shield 1 – Strong Businesses and Citizens – the government will work with industry to co-design a suite of legislative reforms, including options for new cyber obligations, streamlined reporting processes, improved incident response, and better sharing of lessons learnt after a cyber incident.

As part of the strategy consultation process, industry raised difficulties when engaging incident response firms. It was raised that there is a lack of clarity around professional standards for incident response providers, leading to inconsistent service quality. Without rapid and high-quality support, incidents can grow in scale and cause devastating consequences for Australian businesses and citizens. To address this, the government seeks to provide businesses with greater confidence when they engage with cyber security professionals, and will co-design an industry code of practice for incident response providers.

In the United Kingdom, which has historically been several years in front of Australia with regards to cyber public policy, the National Cyber Security Centre (NCSC) has created a Cyber Incident Response (CIR) scheme, which gives organisations confidence in companies that meet the NCSC's rigorous standards for high-quality cyber incident response. The CIR scheme was created back in 2013, and was recently expanded to make it available to a wider range of organisations with the creation of an additional level. The scheme is run on behalf of the NCSC by two industry delivery partners, including CREST.

The NCSC recommends that all UK organisations should use an NCSC-assured CIR provider when dealing with cyber incidents. This includes, but is not limited to, businesses – from small, local companies, to large, multinational organisations – central and local government, and charities.

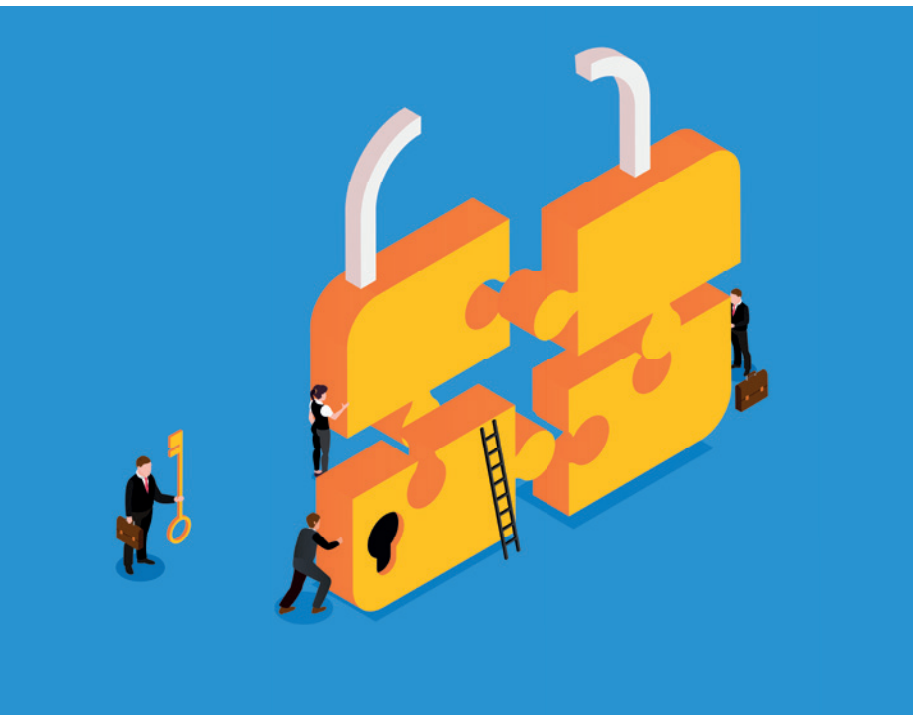
The NCSC assured CIR levels are:

- CIR Level 1 scheme, which assures companies that deal with sophisticated, targeted attacks against networks of national significance, including incidents caused by nation-state-backed actors. It is expected to have the capability to support cyber incident response for organisations that are part of the United Kingdom's central government, the Critical National Infrastructure, or which operate in a regulated sector or more than one country.
- CIR Level 2 scheme, which assures companies that have capability to support cyber incident response for most private sector organisations, charities, local authorities, smaller public sector organisations and organisations that predominantly operate in the United Kingdom. Service providers are expected to have the experience and capability to deal with incidents caused by financially motivated criminals (such as business email compromise, ransomware, etc.)

The benefits of the CIR scheme include:

- direct support from CIR companies when an organisation becomes a victim of a cyber attack

Nigel Phair



- assurance that the CIR company meets the NCSC's rigorous standards for high-quality cyber incident response
- expertise from the CIR company to help organisations investigate and recover from a cyber attack
- advice on how organisations can prevent future attacks.

Of all these benefits, I think it is the assurance given to victim organisations that is the most powerful. Like many other aspects of cyber security, organisations of all shapes and sizes purchase services with the hope that it will make a demonstrable difference in their risk management posture. When buying a cyber security professional service, organisations need assurances that the supplier it engages is reputable, trustworthy, competent and – while the organisation would hope not to need the service – has a clear complaints and resolution process in place.

The Australian Government should implement a similar scheme, with a focus on assurance, but should also implement a rigorous application process that examines a prospective CIR provider's quality processes and procedures, compliance with standards (e.g., ISO27001, ISO9001), professional indemnity insurance, contract management, informational security processes, complaint handing, and conflict of interest policies. Aspiring incident response organisations should use suitably competent and qualified individuals who are registered via a professional scheme, and whose bona fides can be identifiable to the client organisation.

In tandem to the creation of an approved incident response scheme should be the conduct of cyber security exercising. Again, this is a goal in the Australian Strategy. As part of Shield 4 – Protected Critical Infrastructure – the Cyber Coordinator will lead a National Cyber Exercise Program, exercising the full spectrum of incidence response plans, consequence management and communications channels.

Unsurprisingly, the NCSC has already created a Cyber Incident Exercising (CIE) scheme, which gives customers confidence that CIE Assured Service Providers meet NCSC standards for high-quality cyber incident exercising. CIE Assured Service Providers have been assured by the NCSC to develop and deliver controlled, scenario-based, tailored exercising that conforms to the NCSC CIE Technical Standard. These exercises are delivered for organisations that want to practice, evaluate and improve their cyber incident response plans in a safe environment. An important part of the CIE scheme is that Assured Service Providers are required to share limited, non-attributable information about the exercise being conducted with the NCSC. This is important for trend analysis and future guidance. Like the CIR scheme, this initiative is delivered on behalf of the NCSC by industry delivery partners.

These are just two aspects of a bold and ambitious cyber security strategy. I believe that the Australian Cyber Security Centre has an important role to play as the national technical authority for cyber security and in defining best-practice standards for industry. As a like-minded jurisdiction, we should closely follow the United Kingdom's lead in these two schemes and introduce similar initiatives, providing trust and assurance to Australian organisations. After all, the first time an organisation tries out its cyber incident response plan shouldn't be on the day it is attacked.

About the author

Nigel Phair *is a Professor within the Department of Software Systems and Cybersecurity at Monash University. He is also the Chair of the Australasian Chapter of CREST.*

Navigating the storm: unravelling the surge in cloud attacks in 2023

BY **CHATHURA ABEYDEERA, DIRECTOR, KPMG**

In the dynamic realm of cyber security, 2023 brought forth an unprecedented surge in cyber attacks targeting cloud infrastructure, revealing vulnerabilities amid organisations' digital transformation endeavours.

Chathura Abeydeera

The landscape unfolded with incidents of misconfigurations, unauthorised access and supply chain attacks, highlighting the challenges that businesses faced globally. Persistent issues like misconfigured storage buckets and data breaches exposed the scale of the problem, emphasising the potential national security implications. The alarming increase in data breaches attributed to cloud storage misconfigurations signalled a pressing need for organisations to fortify their security measures. A notable shift in credential advertisements suggested evolving tactics by threat actors, prompting organisations to adopt proactive defence strategies.

With cloud service-provider reliance reaching new heights, the landscape witnessed a rise in multi-cloud adoption, accompanied by complexities in identity and permissions management, as highlighted by Microsoft's report. The year also saw the emergence of malware delivery via cloud applications, emphasising the necessity for a holistic security approach beyond traditional measures. Organisations grappled not only with evolving ransomware and data exfiltration targeting cloud assets, but also with securing aging instances, exemplified by the concept of ghost sites. Reflecting on these events, it becomes evident that achieving a secure cloud environment requires continuous vigilance, adaptability, and a proactive stance against the ever-evolving threat landscape. The following outlines notable trends from publicly disclosed cloud-related security incidents throughout the year.

NOTABLE TRENDS

PERSISTENT CLOUD SECURITY CHALLENGES

Recurring incidents of misconfigured Amazon Web Services (AWS) S3 buckets, unauthorised access and general misconfigurations shows the persistent challenges that organisations face in securing their cloud environments. As organisations accelerate their digital transformation, ensuring the robust security of cloud infrastructure remains an ongoing struggle.

NATIONAL SECURITY IMPLICATIONS OF DATA LEAKS

The leakage of the US Transportation Security Administration's No Fly List through an unsecured AWS server highlights the serious implications of data breaches in the cloud, particularly when it involves sensitive information with potential national security consequences. Moreover, the disclosure of a Chinese cyber espionage operation targeting Microsoft cloud services revealed a sophisticated attack involving the forging of authentication tokens. This allowed the attackers to collect sensitive email data from targeted organisations, including the US State Department. These incidents serve as a stark reminder of the critical importance of safeguarding data with significant geopolitical ramifications.

DATA BREACHES FROM MISCONFIGURED CLOUD STORAGE

The rise in data breaches attributed to misconfigured or leaking cloud storage objects emphasises the urgent need for organisations to implement robust security measures, conduct regular audits, and promptly address configuration issues. The vulnerability of cloud storage necessitates a proactive approach to mitigate risks and protect sensitive data.

MULTI-CLOUD ADOPTION AND PROVIDER RELIANCE

Wiz's State of the Cloud 2023 report, highlights the increased reliance on major cloud service providers. Azure is commonly used as a secondary platform, and Google Cloud is a common tertiary platform in multi-cloud environments, reflecting the evolving landscape of cloud adoption. While multi-cloud strategies offer flexibility, they also introduce complexities in managing diverse environments.

IDENTIFICATION AND PERMISSION MANAGEMENT CHALLENGES

Microsoft's 2023 State of Cloud Permissions Risks report sheds light on significant challenges in identification and permission management. Issues, such as inactive workload identities, high ratios and 'super admin' permissions, stress the complexities that organisations face in maintaining secure cloud environments. Striking the right balance between accessibility and security becomes paramount.

CLOUD SERVICE PROVIDER OUTAGES

Service disruptions stemming from distributed denial-of-service attacks, accidental network changes, data centre fires and equipment failures, exposed the digital infrastructure's vulnerability. These incidents reveal the complex challenges faced by cloud service providers, highlighting the ongoing efforts required to enhance resilience and mitigate the impact on users dependent on these services for seamless operations. As for internet service providers, how many of you recall the outages we experienced in 2023 that prevented businesses from accessing their cloud applications for daily operations? Being an individual who's not using a physical wallet, I had to ask a colleague to cover my coffee expenses on one of those days when the coffee shop couldn't process digital payments. In retrospect, these widespread outages not only disrupted essential business operations, but also highlighted the increasing reliance on cloud services.

DIVERSE THREAT LANDSCAPE

Cybercriminals are increasingly adopting a business-focused approach, capitalising on opportunistic and random hacks to transform themselves into sophisticated business models. These threat actors strategically position themselves to maximise profits, constantly elevating their tactics. The evolving landscape indicates a shift towards organised, profit-driven cybercrime, requiring a response that matches the intricacy of their operations. The potential overlap in tactics used by nation-state threat actors and cybercriminals, as detailed in Google's Threat Horizons report, emphasises the need for organisations to be aware of diverse threats and employ comprehensive security measures. A nuanced understanding of the threat landscape is essential to tailor security strategies effectively.

THE INCIDENTS OF RANSOMWARE AND DATA EXTORTION TARGETING CLOUD ASSETS SHOWS THE DYNAMIC TACTICS EMPLOYED BY THREAT ACTORS

RANSOMWARE AND DATA EXFILTRATION TARGETING CLOUD ASSETS

The incidents of ransomware and data extortion targeting cloud assets shows the dynamic tactics employed by threat actors. These adversaries have enhanced their capabilities to intricately target cloud applications and cloud service providers. Given the adaptable nature of ransomware tactics, proactive defence measures become imperative to effectively counter evolving threats.

SECURITY RISKS OF GHOSTS

The concept of Salesforce 'ghost sites' reveals potential security risks associated with not properly decommissioning or securing old instances. Misconfigured Salesforce instances could lead to data exposure and compromise sensitive information. Organisations must ensure proper decommissioning procedures to mitigate such risks effectively.

DIVERSIFICATION OF CYBERCRIMINAL ACTIVITIES

The Freejacking campaigns, as identified by Unit42, characterises this particular cloud threat as 'play and run' activity, wherein threat actors deliberately avoid the payment for cloud resources. This strategy involves actors using freely available cloud resources or illicitly obtained or fabricated payment details to establish premium cloud accounts to their crypto mining operations. The advertisement of cloud exploitation services and crypto mining services indicates a diversification of cybercriminal activities. Organisations including cloud service providers must remain vigilant against various threats, including the unauthorised use of cloud resources for malicious purposes. A comprehensive security posture is crucial to thwart diverse cyberthreats.

RISE IN MALWARE DELIVERY VIA CLOUD APPLICATIONS

The observed increase in malware delivered via cloud applications, with Microsoft OneDrive being a significant contributor and using Google Calendar for malware command-and-control infrastructure, indicates a shift in the threat landscape. Organisations need to enhance their security measures within cloud environments, focusing on both detection and response to malware. The dynamic nature of malware and traffic delivery highlights the importance of continuous monitoring.

THE INFO STEALER ECOSYSTEM

Info stealer, or more commonly known as stealer malware, has emerged as a prominent threat, acting as a significant source of illicitly obtained identity data that is then traded on online criminal forums. The inherent danger lies in its capability to compromise the security of cloud systems and administrative portals directly, serving as an initial access mechanism for cybercriminals. A number of incidents emphasise the serious impact that a single stealer malware infection can have on any organisation. Regularly checking your organisation's exposure to stealer infections is crucial.

THIRD-PARTY AND SUPPLY CHAIN CLOUD ATTACKS

We witnessed a series of concerning incidents highlighting the risks associated

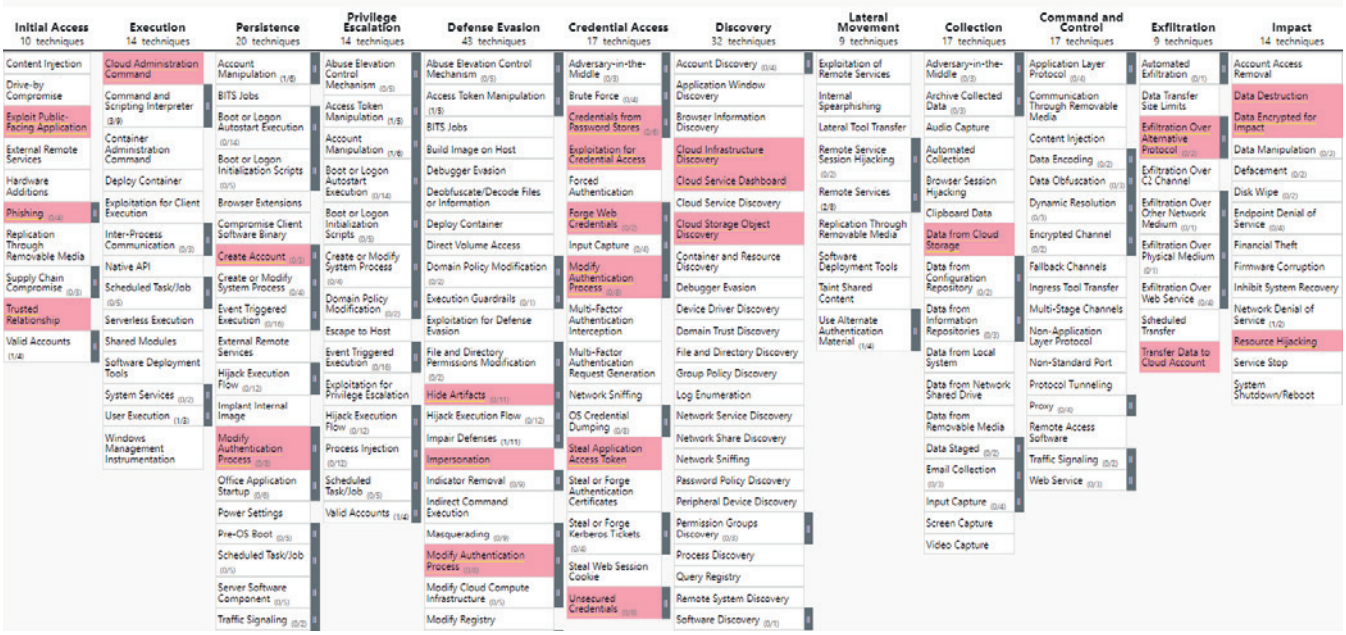


FIGURE 1. SUMMARY OF COMMON CLOUD INCIDENT TACTICS, TECHNIQUES AND PROCEDURES (TTPS) IN 2023

with third-party and supply chain cloud attacks, particularly impacting managed file transfer (MFT) applications. Kicking off the year, CL0P exploited a vulnerability in the GoAnywhere MFT application, evidencing the susceptibility of these widely used tools to malicious activities; however, the most significant blow came from CL0P's MOVEit campaign, which unfolded as one of the largest mass data breaches in history, compromising the security of more than 2000 organisations. This colossal incident not only exposed the vulnerabilities within a specific application, but also demonstrated the profound impact that such attacks can have on a broad spectrum of entities. Furthermore, the revelation of a supply chain attack targeting developers and repositories for various cloud services emphasised the far-reaching consequences of compromised supply chains, posing serious threats to the integrity and security of cloud-based systems.

SUMMARY OF COMMON CLOUD INCIDENT TACTICS, TECHNIQUES AND PROCEDURES IN 2023

MISCONFIGURATIONS AND COMPROMISED CREDENTIALS

Persistent incidents involved misconfigured cloud services, often exposing data due to a lack of authentication protocols. Commonly, compromised credentials played a significant role in unauthorised access and data breaches.

EXPLOITATION OF PUBLIC-FACING APPLICATIONS

Threat actors consistently exploited vulnerabilities in public-facing applications to gain unauthorised access and compromise cloud environments. This tactic served as a primary entry point for various incidents.

DATA THEFT FROM CLOUD STORAGE

Theft of sensitive data from cloud storage remained a prevalent tactic, technique and procedure (TTP), emphasising the importance of securing storage configurations. Threat actors actively targeted misconfigured storage objects, leading to data exposure.

ABUSE OF CLOUD SERVICE DASHBOARDS/PORTALS

Incidents involved the abuse of cloud service dashboards, highlighting the need for organisations to secure administrative interfaces effectively. Attackers exploited vulnerabilities within dashboards to gain control over cloud resources.

MODIFICATION OF FIREWALL RULES

Threat actors frequently modified firewall rules to manipulate network access, enabling unauthorised activities within cloud environments. This tactic demonstrated a strategic effort to bypass security measures.

PHISHING ATTACKS

Phishing attacks were observed as a specific tactic, emphasising the need for organisations to educate employees about phishing risks. Attackers leveraged deceptive techniques to obtain credentials and gain unauthorised access.

ZERO-DAY VULNERABILITY EXPLOITATION

The exploitation of zero-day vulnerabilities and frameworks added complexity to incidents. Organisations need robust strategies for zero-day vulnerability management and timely patching.

These TTPs collectively highlight the diverse and evolving nature of threats in cloud environments. Organisations must adopt comprehensive security measures, focusing on configuration management, access controls and proactive threat detection to effectively mitigate these risks.

RECOMMENDATIONS TO SECURE CLOUD ENVIRONMENTS

CONTINUOUS MONITORING AND REMEDIATION

Regularly monitor cloud configurations and vulnerabilities, and use threat detection and leverage automated tools to promptly identify and remediate issues.

ROBUST IDENTITY AND ACCESS MANAGEMENT

Strengthen identity and access management practices by implementing least-privilege principles, regularly auditing access permissions, and ensuring strong authentication mechanisms.

MULTI-CLOUD SECURITY STRATEGIES

Embrace a multi-cloud approach, understanding the security features and challenges of each provider. Tailor security measures to the unique characteristics of each cloud environment.

COMPREHENSIVE INCIDENT RESPONSE PLANS

Develop and regularly update incident response plans specific to cloud environments, ensuring robust and effective responses to security incidents.

EDUCATION AND TRAINING PROGRAMS

Invest in comprehensive cyber security education and training for employees to foster a culture of security awareness, and reduce the risk of human error.

LEGACY INSTANCE DECOMMISSIONING

Implement secure decommissioning procedures for legacy cloud instances, mitigating the risk of data exposure and unauthorised access. This measure ensures the security of data even after instances are no longer in active use.

COLLABORATION AND THREAT INTELLIGENCE SHARING

Engage in collaborative efforts and share threat intelligence within the industry. This keeps the organisation well-informed about emerging threats, enabling the enhancement of collective defence mechanisms to stay ahead of potential risks.

REGULAR SECURITY TRAINING AND TABLETOP EXERCISES

Conduct regular security training sessions and simulated drills to test the effectiveness of security protocols and incident response plans. These exercises aim to strengthen preparedness and response capabilities in the face of evolving cyberthreats.

As organisations continue to harness the power of the cloud, these recommendations serve as essential building blocks for establishing and maintaining robust cloud security postures. In an era of escalating threats, the commitment to proactive security measures will be instrumental in safeguarding sensitive data, maintaining operational resilience, and ensuring the trust of stakeholders in the digital realm.

About the author

Chathura Abeydeera *is a director in the consulting practice of KPMG Australia, and leads the Cyber Attack and Response services. He possesses over 20 years of experience in offensive cyber security, establishing himself as a highly technical cyber security practitioner. He additionally holds a position as an advisory board member for CREST Australasia. He has delivered complex technical cyber security assessment programs and incident response engagements for numerous high-profile Australian and global organisations. He is a Fellow of the Australian Information Security Association and of CREST International. He is presently engaged in the pursuit of a doctoral degree in space intelligence.*

Are we counting the right costs?

BY **JOSEPH CHENG**

Looking at the impacts of cyber security incidents from a psychological perspective.

Joseph Cheng

In today's cyber era, cyber security has become a major concern for individuals, enterprises and governments. According to Cybersecurity Ventures, global cybercrime costs are expected to grow by 15 per cent per year over the next five years, reaching US$10.5 trillion annually by 2025 – up from US$3 trillion in 2015 (Calif, 2020). In 2022, the FBI's Internet Crime Complaint Center[1] reported that there were more than 800,944 complaints of suspected internet crime that year, and reported losses exceeding US$10.3 billion – a 50 per cent increase of monetary loss from 2021. The Global Risks Report 2022 from the World Economic Forum[2] suggested that cyber security measures in place by businesses, governments and individuals were increasingly being rendered obsolete by the growing sophistication of cybercriminals.

Cybercrime costs include damage and destruction of data, theft of personal and financial data, stolen money, lost productivity, theft of intellectual property, misappropriation, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational damage.

Because cyber attacks can result in the loss of personal and sensitive information, it can cause victims to feel violated, vulnerable, and helpless. They may experience a range of mental health problems as a result, including anxiety, depression and post-traumatic stress disorder (PTSD). The psychological impact of cyber attacks can be long-lasting, and may even result in individuals avoiding using technology. These impacts are far beyond the financial losses and reputational damage to the victims.

In addition to victims, cyber security professionals also face unique mental health challenges due to the nature of their work. They are responsible for protecting sensitive information and preventing cyber attacks, which can be a highly stressful and demanding job. The pressure to maintain high levels of cyber security, combined with long hours and a constant need to stay up to date with the latest technologies and threats, can result in burnout, anxiety, and depression. They may also experience feelings of guilt or responsibility when cyber attacks occur, which can further exacerbate their mental health challenges.

The long-term damaging effects of cyber incidents on the mental health of victims and cyber security professionals cannot be ignored (Agrafiotis, et al., 2018). Given the critical importance of cyber security and the growing occurrence of cyber attacks, it is essential to understand the impact of these issues on mental health, and develop strategies to support victims and cyber security professionals.

PSYCHOLOGICAL IMPACTS OF CYBER SECURITY INCIDENTS

Cybercrime can leave victims feeling vulnerable. Due to loss of personal and financial information, victims often feel anxious about safety, which could increase stress levels.

Anxiety is one of the most common psychological symptoms reported by victims of cybercrime.[3] Victims may experience depression and a sense of hopelessness, which could lead to a loss of trust in technology and online services. These feelings can be long-lasting and affect the victim's quality of life (Gross et al., 2016).

PTSD is another common psychological issue that victims of cyber attacks may experience. PTSD is a mental health disorder that occurs after a traumatic event. Cybercrime victims may experience PTSD-like symptoms, such as flashbacks, nightmares and avoidance behaviour.

The psychological aftermath faced by cyber security professionals is also enormous. Cyber security is a highly stressful and demanding field that requires constant vigilance, readiness and resilience. The practitioners are on the frontlines of defending against cyber attacks, and face the risk of cyber attacks, data breaches, ransomware, phishing, and other threats that can have serious consequences for their enterprises and clients (Singh et al., 2023).

WHAT IS MENTAL HEALTH?

Mental health refers to a person's overall psychological wellbeing, including emotional, cognitive and social aspects (Huppert, 2009). An individual with good mental health is able to handle everyday stressors, cope with challenges, maintain healthy relationships, and enjoy a fulfilling life.

Mental illness encompasses a diverse array of mental health disorders that impact an individual's cognition, emotions, actions and capacity to engage in everyday activities. It can be caused by genetics, life experiences, brain chemistry and environmental factors. These illnesses, which include bipolar disorder, depression, schizophrenia, anxiety and personality disorders, affect the way a person thinks, feels and acts.[4]

In 2019, the World Health Organization found that one in every eight people – or 970 million people around the world – were living with a mental disorder, with anxiety and depressive disorders being most common[5]. In Australia, of the 19.6 million Australians aged 16–85 years in 2020[6] that were suffering mental illnesses:

- over two in five (43.7 per cent or 8.6 million people) had experienced a mental disorder at some time in their life
- one in five people (21.4 per cent or 4.2 million people) had a mental disorder within the last 12 months
- 4.4 million people (22.3 per cent) experienced a short-term mental disorder (for less than 12 months) at some time in their life.

MENTAL HEALTH PROBLEMS OF CYBER SECURITY PROFESSIONALS

In 2020, Sekuro surveyed 101 cyber security professionals to find out how they've been coping over the past two years. The results were distressing, with the vast majority of cyber security professionals (91 per cent) reporting experiencing mental health challenges at work. Just as worryingly, only 11 per cent reported that they hadn't experienced burnout due to their job[7]. Another damning finding by security firm Nominet[8] in 2020 was that 88 per cent of CISOs reported feeling 'moderately or tremendously stressed', while 50.8 per cent of cyber security professionals had been prescribed medication for their mental health.

But does this figure really reflect the actual situation among cyber security professionals?

It's no secret that the global cyber security industry is still male dominated. Studies from recent years have highlighted the gender imbalance across the cyber security space. Although there was a significant increase in the per centage of women working in cyber security, growing from 11 per cent in 2017 to 24 per cent in 2019, there was still only 25 per cent women in 2021 (Cybersecurity Venture).

Research has shown that women are more likely to report mental health problems and seek help than males (e.g., National Centre for Social Research, 2004; Northern Ireland Statistics and Research Agency, 2002). Women are often taught to be more emotionally expressive and encouraged to seek help when they are struggling, while men are often taught to hide their emotions and be self-reliant. Many men feel pressure to conform to traditional ideas of masculinity that prioritise strength, stoicism and self-sufficiency. In addition, they may fear that admitting they have a problem will impact their job security or career prospects (Cavanaugh et al., 2000). Therefore, societal norms, expectations and job security create barriers for men to seek mental health support, which can result in a higher rate of undiagnosed or untreated mental illnesses.

THE IMPACTS OF BURNOUT AND STRESS ON MENTAL HEALTH

Burnout[9] and stress are two main factors that have significant impact on a cyber security professional's mental health (Nobles, 2022).

Burnout is more than just feeling tired at work – it's an emotional, mental and physical reaction to constant stress. When work demands constantly pile up, it takes a toll on people, and individuals may begin to feel unappreciated and overworked. This evolves into dread the next day, feeling as though they have nothing more to give, or they simply stop caring. There are many effects that work burnout can have on mental health, including individuals being at increased risk for:

- anxiety
- depression
- psychological distress
- poor decision-making
- shortened attention span
- lack of motivation
- negative or cynical outlook on life.

Stress also has a significant impact on mental health. When an individual experiences stress, their body releases stress-related hormones, such as cortisol and adrenaline, which can trigger a range of physical and psychological responses. If stress is chronic or prolonged, it can

increase the risk of developing mental health problems, such as anxiety disorders, depression, and PTSD. Stress could impair:

- **Cognitive functioning:** Prolonged stress can make it difficult to concentrate, remember things, and make decisions
- **Emotions:** Chronic stress can lead to feelings of anxiety, irritability, and low mood.
- **Physical health:** Stress increases the risk of conditions like cardiovascular disease, diabetes and obesity.
- **Behaviour:** Stress can lead to unhealthy coping mechanisms, such as substance abuse, overeating and social withdrawal, which can further exacerbate mental health problems.

CONSEQUENCES OF POOR MENTAL HEALTH

Studies have shown that poor mental health can have a significant impact on an individual's ability to perform their job effectively, particularly in the fast-paced and high-pressure environment of cyber security. The consequences of not recognising or promptly treating mental health problems are:

- **Decreased job performance:** Mental illnesses, such as anxiety, depression, and burnout, can decrease an individual's ability to concentrate, solve problems, and perform their job duties effectively. In a field as critical as cyber security, even small errors can have significant consequences, so reduced job performance can increase the risk of security breaches and data loss.
- **Security breaches:** If a cyber security professional is experiencing mental health problems, they may be more likely to make mistakes or overlook critical details, which can result in security breaches.
- **Workplace conflicts:** Mental illnesses can affect an individual's ability to communicate effectively, which can lead to conflicts with colleagues and managers. This can create a negative work environment, impacting overall team morale and productivity.
- **Personal consequences:** Mental illnesses can also have personal consequences, such as difficulty maintaining healthy relationships, increased substance use, and physical health problems. These personal issues can further exacerbate work-related stress and affect job performance.

HOW CAN WE MEASURE THE COSTS?

Mental health problems can be difficult to detect. Even worse, many people who are struggling with them may not even realise it, as the symptoms can be very subtle or gradual. Similarly, some mental health problems can manifest as physical symptoms, which can be confusing and difficult to diagnose; however, the toll exacted by these issues is overwhelming, spanning various dimensions.

Measuring the costs associated with the impact of mental health problems and cyber incidents caused by stress or burnout among cyber security professionals requires a systematic approach.

Financially, there are expenses tied to diminished productivity, such as heightened turnover rates and potential legal liabilities resulting from compromised security. Non-financially, qualitative measurements could include quality of life, work productivity, social functioning, physical health and mental wellbeing.

DIRECT COSTS

- **healthcare costs:** analyse health insurance claims and medical expenses related to mental health treatment sought by affected employees
- **counselling and support services:** calculate the expenses associated with providing counselling services, employee assistance programs, or other mental health support initiatives
- **incident response costs:** estimate the financial impact of cyber incidents, including costs for incident investigation, recovery and potential damages
- **legal and compliance costs:** consider any legal expenses or compliance fines resulting from cyber incidents related to stress-induced errors.

INDIRECT COSTS

These are the intangible costs that arise from the impact of mental health problems and cyber incidents, which can be more challenging to quantify but are equally crucial to consider.

These include:

- **productivity loss:** measure the decrease in productivity due to mental health struggles and its impact on the cyber security team's ability to detect and respond to threats
- **absenteeism and turnover:** calculate the financial impact of employee absences, sick leaves, and the costs associated with hiring and training new employees to replace those who leave due to mental health issues or burnout
- **reputation damage:** assess the potential harm to the organisation's reputation caused by cyber incidents resulting from stress-related errors
- **reduced innovation and creativity:** quantify the impact of burnout on employees' ability to innovate and contribute new ideas, potentially leading to missed opportunities
- **elevated stress for colleagues:** consider the costs of addressing elevated stress levels and potential impacts on other team members.

REMEDY ACTIONS FOR VICTIMS

For the victims, it is important for enterprises to take steps to help them deal with the psychological impacts. Here are a few ways enterprises can provide support:

- **Communicate promptly and transparently:** It's important for enterprises to communicate quickly and clearly about the incident, and take necessary steps to address the issue.
- **Provide resources for coping:** Enterprises can provide resources, such as tips for coping with stress and anxiety, contact information for counselling services, and other mental health resources.
- **Provide support for affected customers:** Enterprises can provide dedicated support for the victims affected by the cyber attack.
- **Take responsibility and apologise:** If the cyber attack was due to a security breach, it's important for the enterprise to take responsibility and apologise for any harm caused to customers.

Overall, by taking a proactive and compassionate approach, enterprises can help victims deal with the psychological impact of a cyber attack and minimise the long-term negative effects.

REMEDY ACTIONS FOR EMPLOYEES

An employer has a duty of care to ensure the health and safety of its employees, and this includes taking steps to prevent or address burnout and stress. For an enterprise's employees, a cyber attack can also have a significant impact on their mental and emotional wellbeing. It's important for enterprises to support employees in the aftermath. Here are a few ways that enterprises can provide psychological support to staff after a cyber attack:

- **Offer counselling and mental health resources:** Enterprises can provide employees with access to confidential counselling services and other mental health resources to help them cope with the emotional impact of the cyber attack.
- **Provide a safe and supportive environment:** After a cyber attack, employees may feel vulnerable and anxious. It's important for enterprises to create a safe and supportive environment where employees feel comfortable sharing their concerns and asking for help.
- **Communicate transparently and consistently:** Enterprises should provide regular updates on the incident and any steps being taken to address the issue. Employees may feel more secure and less anxious when they know what's happening and what to expect.
- **Encourage self-care:** Employees may need time to recover and manage their stress levels after a cyber attack. Enterprises should encourage employees to take time off, practice self-care activities, and prioritise their mental and emotional health.

By prioritising the mental and emotional wellbeing of employees, enterprises can help prevent long-term negative effects of a cyber attack and support a healthy work environment.

RECOGNISING THE WARNING SIGNS OF MENTAL HEALTH ISSUES

It is also crucial for an employee's family, colleagues and employers to identify if someone is experiencing mental illnesses. Most often, family, friends, colleagues or individuals themselves begin to recognise small changes or a feeling that 'something

is not quite right' about their thinking, feelings or behaviour before an illness appears in its full-blown form.

Some symptoms that may be early warning signs, especially if in combination, are sleep or appetite changes, mood changes, social withdrawal, a drop in functioning, problems thinking and concentrating, increased sensitivity, boredom, feeling disconnected, nervousness and changes in. Early intervention can help to reduce the severity of an illness and interruptions in quality of life and functions. It may even be possible to delay or prevent a major mental illness altogether.

MENTAL HEALTH FOR CYBER SECURITY PROFESSIONALS

For cyber security professionals, it is crucial to establish healthy boundaries and take breaks when needed to prevent burnout. There are several strategies that cyber security professionals can use to prevent mental health issues in busy and stressful workplaces:

- **Set boundaries:** Establish clear boundaries between work and personal life. This can help reduce stress and prevent feelings of being overwhelmed.
- **Practice time management:** Learn effective time-management techniques. This can help you stay organised and reduce stress by breaking down large tasks into manageable parts.
- **Seek support:** Don't be afraid to reach out to colleagues or a mental health professional if you are feeling overwhelmed or stressed.
- **Take breaks:** Taking regular breaks throughout the day can help reduce stress and improve productivity.
- **Prioritise self-care:** Engage in activities, that bring you joy and help you relax. This can help prevent burnout and improve your overall mental health.
- **Stay active:** Regular physical activity can help reduce stress and improve mental health.

Cyber security professionals can help each other in the workplace by creating a supportive and open environment where individuals feel comfortable discussing their mental health concerns. These strategies can be:

- **Creating a safe and non-judgmental space:** Encourage open communication and active listening. Ensure that everyone feels heard and respected.
- **Checking in regularly:** Consistently check in on each other to ensure that everyone is coping well. This can be as simple as asking how someone's day is going or sending a quick message to check in.
- **Offering support:** Be there for your colleagues when they need it. This could mean offering to listen, providing resources, or simply being a shoulder to lean on.
- **Respecting boundaries:** Everyone has different comfort levels when it comes to sharing personal information. Respect your colleagues' boundaries and do not pressure them to share more than they are comfortable with.

By taking care of themselves and using these strategies to manage stress, cyber security professionals can help prevent mental health problems from arising in the first place. They should also encourage their colleagues to do the same, and remind them that there is no shame in seeking help.

CONCLUSION

Cyber security incidents have a significant impact on the mental health of both victims and cyber security professionals; however, the psychological impact of cyber security incidents is often overlooked.

To address these issues, it is important for the enterprises and government to recognise that cyber security incidents can cause long-term damaging effects on the mental health of victims and cyber security professionals. To support the victims in overcoming these impacts, enterprises should provide essential support and resources. This includes mental health support services for employees, such as access to counselling, stress management training, and other resources that can help mitigate the negative effects of cyber incidents.

It is important to educate people to recognise the signs and symptoms of mental illness, and to encourage seeking help when needed. It is essential that we continue to raise awareness about the prevalence of mental health problems in the cyber security industry, and the importance of seeking help when needed.

Enterprises should also promote diversity and inclusion in the workplace, provide access to mental health resources and support services, and create a culture of open communication and support surrounding mental health problems. Additionally, employers must create an environment that encourages employees to prioritise their mental health without fearing reprisal or discrimination.

By taking these steps, we can reduce the negative consequences of cyber attacks and help those impacted to recover and move forward. Ultimately, it is up to all of us to prioritise mental health and support those affected by cyber security incidents, in order to build a more resilient and secure digital world.

About the author

Joseph Cheng *is an experienced auditor with a unique background that sets him apart from others in his field. He comes from an extensive IT background, having worked in various IT roles before transitioning to auditing. Cheng also completed a Bachelor of Psychology. He has always been fascinated by how people interact with technology. This led him to start examining cyber security issues from a psychological perspective. He believes that understanding the psychological and human aspects of cyber security is crucial for an enterprise to protect itself from cyberthreats.*

Endnotes

1 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
3 Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology,* 6(2), 205-228.
4 https://www1.health.gov.au/internet/publications/publishing.nsf/Content/pub-sqps-rights-toc~pub-sqps-rights-glo
5 https://www.who.int/news-room/fact-sheets/detail/mental-disorders
6 https://www.abs.gov.au/statistics/health/mental-health/national-study-mental-health-and-wellbeing/2020-21
7 Sekuro, 2022. Mental Health in the Australian Cyber Security Industry. https://sekuro.io/Sekuro_Mental_Health_Cyber_Security_Survey.pdf?utm_source=sekuro&utm_medium=webpage&utm_campaign=cyber_mental_health
8 https://www.nominet.uk/nominet-ciso-stress-report-one-year-on/
9 Nobles, Calvin. 'Stress, Burnout, and Security Fatigue in Cyber security: A Human Factors Problem' HOLISTICA – *Journal of Business and Public Administration,* vol.13, no.1, 2022, pp.49-72. https://doi.org/10.2478/hjbpa-2022-0003

References

Acquisti, A., Telang, R., Friedman, A. (2006). Is there a cost to privacy breaches? An event study. Proceedings of the 3rd International Conference on Intelligent Systems (ICIS), 2006.

Agrafiotis, J., Nurse, J., Goldsmith, M., Creese, S. & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, *Journal of Cyber Security,* Volume 4, Issue 1, 2018, https://doi.org/10.1093/cybsec/tyy006Budnick, C.J., Rogers, A.P. and Barber, L.K. (2020), 'The fear of missing out at work: examining costs and benefits to employee health and motivation', *Computers in Human Behavior,* Vol. 104, p. 106161.

Cavanaugh, M.A., Boswell, W.R., Roehling, M.V. and Boudreau, J.W. (2000), 'An empirical examination of self-reported work stress among US managers', *Journal of Applied Psychology,* Vol. 85, pp. 65-74.

Corrigan, P.W. & Rao, D. (2012). On the self-stigma of mental illness: stages, disclosure, and strategies for change. Can J Psychiatry. 2012 Aug;57(8):464-9. doi: 10.1177/070674371205700804. PMID: 22854028; PMCID: PMC3610943.

Gross, M.L., Canetti, D. & Vashdi, D.R. (2016) The psychological effects of cyber terrorism, *Bulletin of the Atomic Scientists,* 72:5, 284-291, DOI: 10.1080/00963402.2016.1216502

Huppert, F.A., (2009). Psychological wellbeing: Evidence regarding its causes and consequences. Applied psychology: health and wellbeing, 1(2), pp.137-164.

Jansen, J., & Leukfeldt, R. (2018). Coping with cybercrime victimization: An exploratory study into impact and change. *Journal of Qualitative Criminal Justice and Criminology,* 6(2), 205-228.

Kshetri, N. (2019). Cyber security and psychology: Bridging the gap. Cyberpsychology, Behavior, and Social Networking, 22(11), 711-715. doi: 10.1089/cyber.2019.0189

Maria Bada, Jason R.C. Nurse, Chapter 4 - The social and psychological impact of cyber attacks, Editor(s): Vladlena Benson, John Mcalaney, *Emerging Cyber Threats and Cognitive Vulnerabilities,* Academic Press, 2020, Pages 73-92, ISBN 9780128162033, https://doi.org/10.1016/B978-0-12-816203-3.00004-6.

Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. (2021). Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors, 21, 5119. https://doi.org/10.3390/s21155119.

Nobles C. (2022). Stress, Burnout, and Security Fatigue in Cyber security: A Human Factors Problem. HOLISTICA – *Journal of Business and Public Administration,* Vol.13 (Issue 1), pp. 49-72. https://doi.org/10.2478/hjbpa-2022-0003

Rainer, R. K., Jr., Ortbach, K. E., & Storey, V. C. (2020). When 'Sorry' is not enough: Legal liability, reputation, and the psychological impacts of cyber security incidents. *Information Systems Journal,* 30(3), 419-447. doi: 10.1111/isj.12252

Romanosky, S. (2016). Examining the costs and causes of cyber incidents, *Journal of Cyber Security,* Volume 2, Issue 2, December 2016, Pages 121-135.

https://doi.org/10.1093/cybsec/tyw001.

Singh, T., Johnston, A.C., D'Arcy, J. and Harms, P.D. (2023), 'Stress in the cyber security profession: a systematic review of related literature and opportunities for future research', *Organizational Cyber security Journal: Practice, Process and People,* Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/OCJ-06-2022-0012.

https://www.emerald.com/insight/content/doi/10.1108/OCJ-06-2022-0012/full/html#article-tab

The intersection of data privacy and cyber security

BY **ANDREW LAWRENCE, CEO, DE.ITERATE**

How data privacy might just be the solution to your cyber security problems.

In an age when data breaches are as common as they are catastrophic, the intersection of data privacy and cyber security has never been more critical. The unveiling of Australia's ambitious privacy reforms in 2023 could be the unexpected hero in the cyber security saga, offering businesses a blueprint for fortifying their defences by protecting personal data.

An exploration of the symbiotic relationship between the Australian Privacy Principles (APPs) and cyber security measures demonstrates how adhering to stricter privacy laws might just be the secret weapon that organisations need to combat the digital threats of the 21st century. Australia's privacy overhaul could be the key to locking down cyber security threats.

THE GLOBAL CONTEXT AND AUSTRALIAN LANDSCAPE

The concept of 'data privacy' really started gaining traction in 2018, when the General Data Protection Regulation (GDPR) became law in the European Union, and the *California Consumer Privacy Act* became law in the United States. New Zealand followed suit in 2020, with its *Privacy Act* coming into force.

In Australia, the federal government commenced a two-year review of Australia's privacy laws in 2020. In February 2023, the government released the highly anticipated Privacy Act Review Report. It contained some of the most sweeping reforms to the privacy landscape in Australia, including 116 proposals to amend the *Privacy Act*. The proposed changes were aimed at bringing our privacy regime in line with equivalent overseas laws, and strengthening protection and control of personal information in the digital age.

In September 2023, the government published its response to the Privacy Act Review Report, in which it agreed to 38 proposals, agreed in principle to 68 proposals, and noted 10 proposals.

One of the key changes is the removal of the small business exemption. Currently, the *Privacy Act* does not apply to businesses with a turnover of less than $3 million. Once this exemption is removed, all Australian businesses will be required to meet minimum data privacy standards, regardless of turnover. This is a significant widening of Australia's privacy laws – one that will bring us in line with international laws, such as the GDPR.

WHAT THIS MEANS FOR AUSTRALIAN BUSINESSES

The government has assured that small businesses will not be immediately subjected to the new compliance measures under the *Privacy Act*, promising adequate support and time for adaptation.

Removal of the small business exemption will occur only after extensive consultation. This consultation process will aim to identify and address compliance gaps, so that educational material and compliance tools can be developed and supplied by the government.

The government's response also stipulates that there will be a transition period to ensure that small businesses are equipped to meet the new *Privacy Act* requirements.

So then, the question becomes: What will businesses need to do to comply with the *Privacy Act*? In a nutshell, they'll need to adhere to the APPs.

THE AUSTRALIAN PRIVACY PRINCIPLES

The APPs are the bedrock of Australia's privacy protection framework, and are deeply rooted in the *Privacy Act*. Any organisation or agency covered by the *Privacy Act* needs to uphold the APPs when it comes to personal information.

There are 13 APPs in total. They govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- the integrity and correction of personal information
- the rights of individuals to access their personal information.

They dictate how Australian businesses and government organisations should go about the collection, use, and disclosure of personal information. Whether it's a simple email address or more sensitive identifiers like health records and banking details, the APPs ensure that personal information is collected, stored and utilised safely. The APPs also ensure that individuals

Andrew Lawrence

can access and review their personal information when they wish.

Now, here's the beauty of the APPs – they're principles-based. This isn't about strict rules that box you in. Instead, it provides flexibility, allowing you to mould these principles to your unique business model and cater to the diverse needs of your clientele. Plus, they're technology neutral. This means that they're crafted to evolve with the times, adapting seamlessly to new and changing tech landscapes.

THE INTERSECTIONS

The APPs are where data privacy and cyber security intersect.

Let's run through these examples.

CYBER SECURITY	DATA PRIVACY
Business Policies	APP 1: Open and transparent management of personal information
Vendor Management	APP 5: Collection Notices APP 6: Use or Disclosure of Personal Information APP 8: Cross Border Disclosure of personal information APP 11: Security of Personal Information
Data Classification	All APPs
Essential Eight Data Leakage Protection	APP 11: Security of Personal Information

BUSINESS POLICIES

'APP 1 Open and transparent management of personal information' is usually satisfied through business policies. To comply, businesses need to keep their privacy policy up to date and transparent, and must contain key details, such as data-retention periods and the company's nominated privacy officer.

VENDOR MANAGEMENT

Four of the APPs (5, 6, 8 and 11) apply to vendor management. All good cyber security programs have a vendor management element – if your program lacks this element, you have a major gap. Organisations need to document who their vendors are, where their vendors are storing data, what types of data are shared with them, and whether the privacy laws of the destination country are commensurate to those in Australia.

DATA CASSIFICATION

Seven of the APPs (1, 3, 5, 8, 10, 11 and 13) touch on data classification, including collecting, managing, disclosing, updating and deleting data. Data classification is not exciting – it's boring, monotonous and time consuming; however, it is a very effective way to achieve a positive data privacy and cyber security outcome. If your organisation can implement effective data classification, you have a superpower. If you know where your data is, and you have effective controls around it, then your ability to meet APP commitments is much simpler.

ESSENTIAL EIGHT DATA LEAKAGE PROTECTION

Under 'APP 11 Security of personal information', an APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

Entities need to establish their own maximum and minimum retention periods for personal information they hold, and specify these retention periods in privacy policies. Configuration standards like the Essential Eight and compliance standards like ISO27001 help businesses demonstrate that they have taken reasonable steps to protect the information they hold. S

About the author

With over 20 years' experience, ***Andrew Lawrence*** *is a passionate information and cyber security leader. Lawrence's expertise spans risk, governance, compliance, strategy, critical infrastructure security, and technology management and architecture. Lawrence has worked with Japanese telco giant KDDI, Honda F1 racing, Credit Suisse, Commonwealth Bank, and Deutsche Bank. Lawrence founded de.iterate in 2021 to make privacy and cyber security stress-free for Australian businesses. For further information, visit https://deiterate.com*

SYBER SERVICES

ENABLING ENTERPRISE SECURITY

BUILDING WITH SECURITY

FROM DESIGN TO DEPLOYMENT, EVERY STEP OF THE WAY!

SECURE BY DESIGN

CLOUD SECURITY & ASSURANCE

OFFENSIVE & DEFENSIVE SECURITY

REFERENCE ARCHITECTURE & PATTERNS

SECURITY DESIGN & CONSULTING SERVICES

INFORMATION SECURITY DELIVERY RISK

SUPPLY CHAIN SECURITY & RISK

WWW.SYBERSERVICES.COM.AU

CONTACT@SYBERSERVICES.COM.AU

Decrypting the digital enigma

BY **ANDREW JACKSON AND MONA SIDHU**

Students should be encouraged to unravel the intricacies of cyber sleuthing.

Andrew Jackson

Mona Sidhu

Digital literacy represents a whole world of understanding over and above traditional skills, and is essential for students to effectively and safely navigate the technology-driven world in which they live.

Digital literacy is also an essential component of cyber security – a concept with practices that have become mainstream over recent decades.

One of the many specialty fields that contribute to this vital work is digital forensics – the science of examining data breaches. It may seem like too heavy of a topic for high school students, but with suitable age-appropriate methods – such as the Cybermarvel initiatives – it can have many benefits now and into the future.

CYBER SECURITY AWARENESS

Digital forensics teaches the importance of protecting personal information, the consequences of cyberthreats, and ways to stay safe online.

ETHICAL USE OF TECHNOLOGY

It also teaches students about responsible digital citizenship, the consequences of cybercrime, and the legal and ethical considerations of using digital tools.

CRITICAL THINKING AND PROBLEM-SOLVING

Digital forensics teaches students to analyse and interpret digital evidence, which encourages a mindset of inquiry and investigation.

CAREER OPPORTUNITIES

Early exposure to digital forensics can spark an interest in related fields, such as computer science or law enforcement. It can help students to explore potential career paths and develop skills that are in high demand in the workforce.

PREVENTING CYBERBULLYING AND ONLINE HARASSMENT

Students who understand digital forensics will be able to recognise and combat cyberbullying and online harassment. They will learn how to report incidents, protect themselves and contribute to a positive online environment.

PREPARING FOR THE FUTURE

As technology continues to advance, digital forensics skills will become increasingly valuable. Teaching these skills at a young age ensures that students are prepared for the evolving digital landscape and are equipped to address emerging challenges.

PROBLEM AWARENESS

Digital awareness teaches students to be conscious of potential problems and risks associated with digital activities. This is crucial for making informed decisions and understanding the potential consequences of their actions online.

LEGAL AND ETHICAL UNDERSTANDING

Digital forensics education helps students understand the legal and ethical implications of digital activities. This knowledge is essential for navigating the complex legal landscape surrounding digital technology, and encourages responsible behaviour in the digital realm.

GLOBAL CONNECTIVITY

In an interconnected world, understanding digital forensics fosters global awareness. It teaches students about cyberthreats that may transcend national borders, and offers insights into the international dimensions of cyber security. S

CYBERMARVEL: PROMOTING RESPONSIBLE DIGITAL CITIZENSHIP

The NSW Department of Education takes a proactive approach to preparing students for the challenges and opportunities of the digital world. It delivers this through a wide range of programs, including Cybermarvel, an online safety awareness program for schools and their communities. Its evolving repertoire of resources aligns with NSW Education Standards outcomes and the Australian Curriculum. Pertinent to digital forensics education are the lessons provided by ed-tech charity Grok Academy. For more information, visit www.nsw.gov.au/education-and-training/cybermarvel

Secure an income while you secure your future in cyber security

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

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

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

'That was a great way for me to prepare for the workforce,' says Antoniewicz. 'During my internship with IBM, I got to develop an internal application for a client that I continued to work on during my graduate position, [which] is now used by over 300 unique users every week.

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

WORK-INTEGRATED LEARNING WORKS

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

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

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

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

AUSTRALIA'S BIGGEST CYBER SECURITY CENTRE AT YOUR FINGERTIPS

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

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

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

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

AUSTRALIA
ECU
EDITH COWAN UNIVERSITY

CRICOS Provider No. 00279B

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

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

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

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

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

For more information
ECU.EDU.AU/RESEARCH/SRI

Creative thinkers made here.

The mind behind the monitor

BY **VANNESSA VAN BEEK**

The digital landscape is filled with threats that require immediate and adaptive responses, similar to those expected of emergency service professionals. Cyber security professionals, however, face a silent battle: chronic stress. It's a battle that rages not on screens, but in minds.

Vannessa Van Beek

A 2022 survey by Sekuro shed light on a troubling fact: nine out of 10 cyber security professionals are grappling with mental health challenges.[1] Complementing this, IBM Incident Responder Study – a global from 2022, revealed that 67 per cent of respondents suffer from stress and anxiety because of their work.[2] Fast forward to July 2023, and another Australian study reveals a similar story: working on the digital frontline and constantly guarding against relentless cyberthreats is taking a significant mental toll on cyber security teams.[3]

As a leader in security with experience managing teams in security operations, platform engineering and architecture for the past few years, I witnessed this firsthand. This ever-present stress carries a heavy human cost. Imagine the story of a colleague who worked 700 hours over two months during a cyber incident. This workload is equivalent to six months of work compressed into two months. Picture the dedicated security professional grappling with recurrent migraines, the silent departure of an overwhelmed security analyst in desperate need of a career break, or the heartbreaking moment when a security engineer receives a late-stage cancer diagnosis. Think about the sleepless nights endured by a security specialist due to stress-related insomnia and the toll it takes on their health, or the visible impact of stress-induced skin issues. These are the unspoken, real-life narratives of people working in cyber security – a world where the human stories behind the scenes often remain hidden, but are important to acknowledge.

Chronic stress doesn't just impact the mind – it can also lead to physical health issues. This is due to the complex interactions between the brain, the nervous system and various organs. For example, the stomach, liver and spleen communicate with the brain, affecting both physical and mental health. Humans, unlike zebras in the wild, cannot simply turn off their stress response after escaping a predator.[4] Our prolonged stress response can weaken the immune system, leading to a cascade of health issues. It keeps trauma-related chemicals circulating in our brains and bodies. The result is that we re-traumatise ourselves by constantly ruminating over past events and worrying about future ones. This cycle of chronic stress can reduce cognitive function and increase sickness and fatigue. It is for this reason that it's crucial to find ways to manage or mitigate this prolonged stress response effectively.

Neuroscience tells us that strategies supporting both our brain and body are key to managing stress. Regular physical activity, adequate sleep and a nutritious diet are vital for brain health, as they help manage the body's stress response. Mindfulness practices, deep breathing exercises and cognitive behavioural strategies can also calm the body. These practices help reduce the occurrence of stress-induced physical ailments and significantly improve mental wellbeing and cognitive performance. Andrew Huberman, a neuroscientist

at Stanford University, emphasises the 'physiological sigh' as a stress-reduction technique.[5] This breathing pattern consists of two quick inhales followed by a prolonged exhale. It rapidly oxygenates the brain and helps reset the respiratory system. While this sigh often occurs spontaneously during stress, using it deliberately can help alleviate stress or anxiety.

Periodic shifts in focus are also crucial for maintaining cognitive health and effectiveness. Neuroscience underscores the importance of shifting from deep focus to a broader view occasionally. This can be as simple as changing your gaze to the horizon or taking a walk. Some people say, 'I don't have time to meditate. It sounds great, but I don't have time.' But the interesting thing is whether you take 15 to 20 minutes in one big lump of time, or you take one or two minutes every hour, it's the same to your brain. Short, unstructured breaks are beneficial to the brain.
Dr Srini Pillay from Harvard endorses this idea, calling it 'Tinker, dabble, doodle time.'[6] It allows for daydreaming or simply doing nothing, which can spark generative thinking.

Ironically, another controversial perspective is to look at enabling the integration of artificial intelligence (AI) and security orchestration automation response (SOAR) technologies within security incident event management platforms in security operations centres. By automating repetitive tasks and streamlining incident response, these technologies alleviate the stress associated with the high-demand nature of the field. They enable more efficient use of resources, promote skill development, and enhance job satisfaction. Security teams empowered by AI and SOAR systems are better equipped to manage their workloads effectively, mitigate the risk of burnout, and maintain a healthier and more resilient workforce. Machine learning algorithms can analyse vast amounts of data quickly and accurately, identifying unusual patterns or anomalies that might indicate a breach. Automated response mechanisms can then mitigate threats before they cause damage. These systems can automatically investigate, contain and remediate security incidents, significantly reducing response times and human errors.

While automation is becoming more sophisticated, human expertise remains crucial in cyber security. The future may see increased collaboration between security professionals and AI systems. Human analysts will provide context, critical thinking and ethical considerations, while AI assists with data processing and pattern recognition.

In addition, fostering a healthy work culture in cyber security can be a protective factor preventing burnout. This involves creating an environment where professionals feel valued, supported and able to maintain a work-life balance. It entails promoting open communication, empathy and collaboration among team members, as well as recognising and appreciating their efforts. This is easy in theory, but in my experience, this is difficult to operationalise. Teams who shape themselves to be innovative, collaborative and inclusive wrestle with tension. As Susan Cain points out: 'Physiological safety holds hands with fear, innovation holds hands with failure, collaboration holds hands with conflict and inclusion holds hands with difference.'[7]

Building a great team culture involves building a team charter and agreeing on values and acceptable team behaviour, and having the courage to have difficult conversations when behaviour falls outside the team's charter. Navigating this requires understanding of human behaviour and workplace dynamics to work through conflict as it arises. This is where organisational psychology has a role to play in security. Through interventions like team-building workshops, conflict resolution strategies and communication skill development, organisational psychologists can foster a more cohesive and resilient security team. Additionally, organisational psychologists can assist in the design of job roles, workload management strategies and stress-reduction programs tailored to the unique demands of security operations. Their insights into motivation, leadership and organisational culture can further contribute to creating an environment where security professionals feel supported, motivated, and equipped to perform at their best, while maintaining their mental and emotional wellbeing.

Addressing burnout is multifaceted and complex. The answer might be found drawing insights from neuroscience and organisational psychology, and also by enabling advanced capabilities like AI and SOAR.

The challenges of our digital era have a profound impact on cyber security professionals. Their role in protecting our interconnected world is essential. Yet, it's the human element within this technical sphere that requires our utmost care and attention. By prioritising the mental and physical health of these professionals, we're investing in a resilient and sustainable future. Their health is integral to our digital safety strategy. Nurturing their wellbeing fortifies our digital frontiers, ensuring the health and wellbeing of our superheros. Their wellbeing is the bedrock and strength of our digital world.

About the author

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

References

1 Sekuro Mental Health Survey 2022.

2 2022. Title of the IBM Incident Responder Survey.

3 Reeves, A., Pattinson, M., Butavicius, M. (2023). *Is Your CISO Burnt Out Yet.*

4 Sapolsky, R. M. (2004). *Why zebras don't get ulcers: The acclaimed guide to stress, stress-related diseases, and coping* (3rd ed.). Holt Paperbacks.

5 Huberman, A. (2023). *Huberman Lab* Podcast Series February 19, 2023. 'How to Breathe Correctly for Optimal Health, Mood, Learning & Performance'.

6 Dr Srini Pillay. 'Unfocus and become more productive' https://tinkerdabble.com

7 Cain, S. (2022). *Bittersweet: How sorrow and longing make us whole.* Penguin Books.

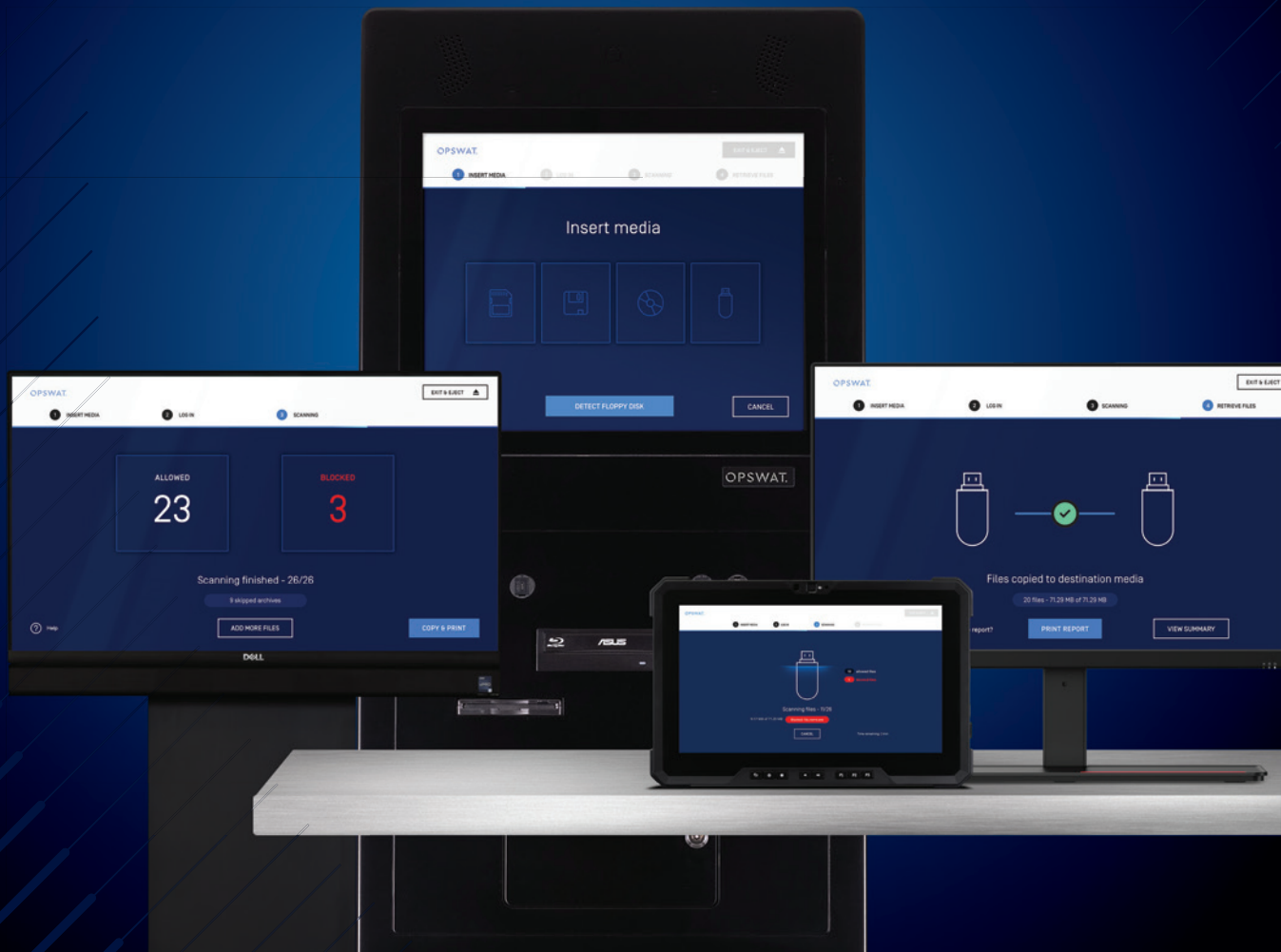

AUSTRALIAN CYBER CONFERENCE
2024
FUTURE IS NOW
AUSTRALIA'S LEADING CYBER SECURITY CONFERENCE
5,000+ delegates | 400+ speakers | 150+ exhibitors
Early bird discount available until 31 July 2024.
REGISTER TODAY | cyberconference.com.au
MELBOURNE | 26-28 NOVEMBER 2024
AISA

OPSWAT.

REMOVABLE MEDIA SECURITY

Trust at the Point of Entry

Wherever you need it, with any of the MetaDefender Kiosk models.



Talk to one of our experts today.

Scan the QR code or visit us at:
opswat.com/get-started
sales@opswat.com