Cyber Today

EDITION 1, 2025

THE FUTURE OF THE CYBER SECURITY INDUSTRY

AUSTRALIA'S KASPERSKY BAN: THE UNANSWERED QUESTIONS

HOW TO TRAIN YOUR CYBER JEDI

AISA


AISA
Cyber | smart · safe · secure
aisa.org.au
cyber voices
THE OFFICIAL AISA PODCAST
Celebrating the diverse voices of the Australian cyber community.

PUBLISHED BY :

EXECUTIVE MEDIA
NEW YORK | MELBOURNE | ADELAIDE | AUCKLAND
EST 1973

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
Edith Cowan University, SANS Training Australia, RMIT University, Deakin University

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

Contents

Foreword

A message from Craig Ford, Deputy Chair, AISA.

Craig Ford

As we approach the halfway point of 2025, the Australian Information Security Association (AISA) is looking to continue to grow valuable partnerships with government, academia and industry. We all know that in this industry, it is hard to protect both our organisations and ourselves from constantly evolving threats. The malicious hordes are really pushing forward, adopting new techniques and capabilities driven by artificial intelligence improvements.

As Deputy Chair of the AISA Board of Directors, I am truly honoured to work with my fellow board members to continue to drive this approach – setting a new path for the association on a level that we have not done before. As I said, it's a hard industry – one that is almost impossible to navigate well, especially when you go it alone.

We need to stand tall, shoulder to shoulder, and as one industry.

Government, academia and industry all must come together to solve the problems we have. We can do what the Romans once did to almost perfection in battle – they stood side by side, locking their shields. They moved as one when required, leaving no-one vulnerable. Move by move, they would push back their attackers and would win many battles that would, on the outside, seem impossible.

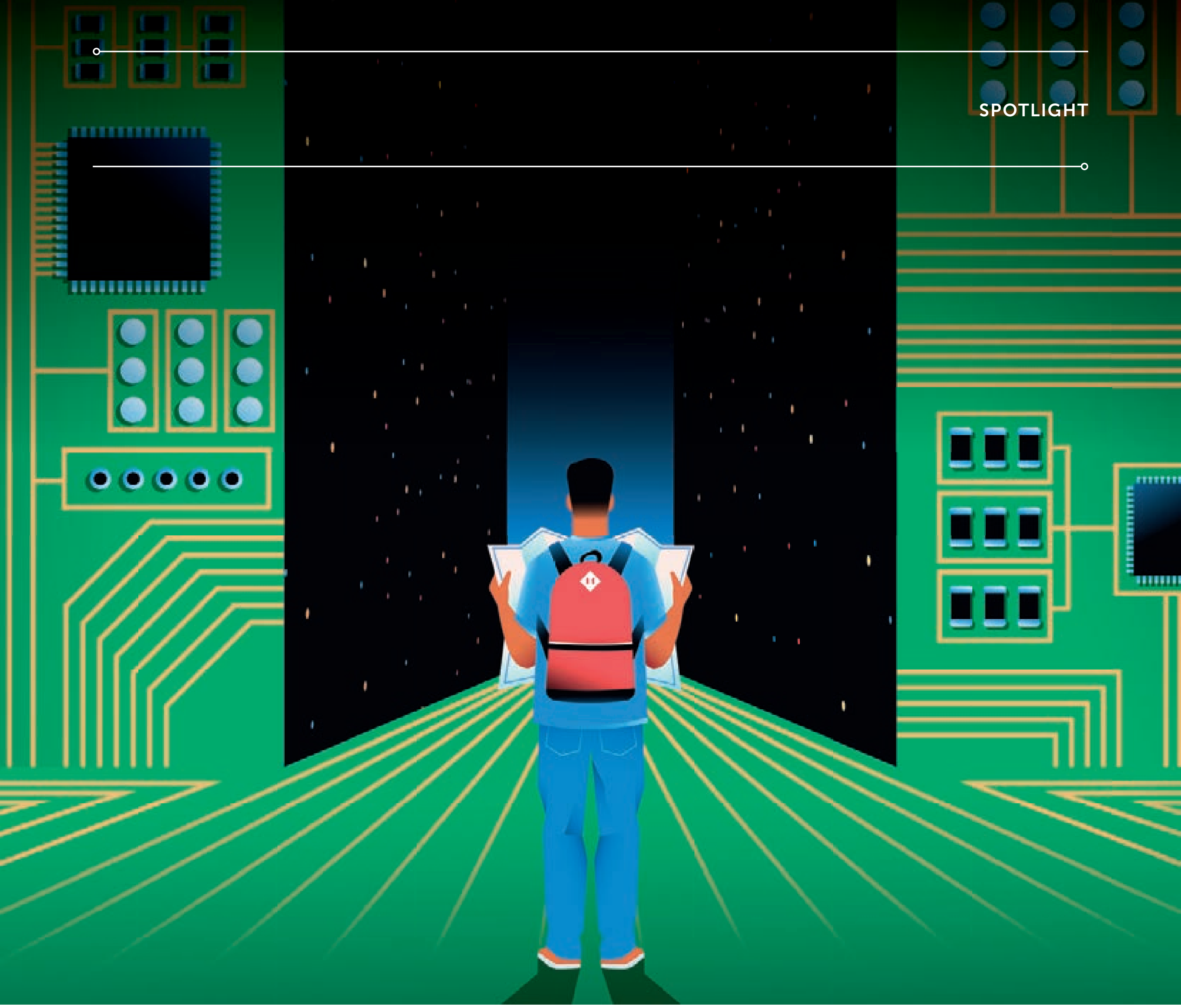
Cyber can be seen in a similar light; it can at times look impossible, like we have already lost. It would be like standing on a battlefield all alone, or maybe a couple of us together, not really working together, but at least trying to fight the same battle – the same enemy. It is no doubt that we would lose with an army of thousands or even millions against us.

But what if we changed tactics – what if we did as those Romans did? What if Australia's cyber industry stopped doing our own things, fighting our own battles one by one, and actually all came together to lock shields? What if we truly shared intel, helped each other perfect our defences and truly stood as one? We all stand firm, filling gaps if one forms in defences, adapting, helping each other move in unison as our attackers circle our defences, striking, stabbing, but never breaking through our lines.

If one does, they are immediately pushed back out via the inner layers of our wall. If one is pushed back, another steps in beside them to push back and back and back.

I know this sounds like a Hollywood movie scene; however, I needed to get my point across to really help everyone understand. This isn't about me, this isn't about AISA, this isn't about the government or even about you. It's about us. About our loved ones, the people we get up and do what we do to protect. They are why we need to find a real way, a way of coming together.

Are you with us?



The future of the cyber security industry

BY DR ADRIAN KAMINSKI

Navigating artificial intelligence and the quantum frontier.

Dr Adrian Kaminski

The past month has seen some major announcements in the artificial intelligence (AI) space. As such, I have been reflecting on the risks of AI-driven cyber attacks, such as adversarial machine learning and deepfake phishing.

Operationally, it seems like a distant and somewhat alien possibility given that some organisations are still grappling with fundamentals, such as two-factor authentication. Yet, the risk of AI-powered attacks are very real, and it is not a case of whether these threats will materialise, but rather how prepared we will be when they do. The National Institute of Standards and Technology has published new guidance and mitigation strategies to address these concerns, highlighting the four major areas of AI that adversaries can utilise: evasion, poisoning, privacy and abuse.

In 2024, a financial executive was duped by an AI-generated deepfake video call, leading to a fraudulent wire transfer of $25 million. This attack demonstrated the alarming potential of generative AI to convincingly mimic audio and video, weaponising social engineering attacks.

The rise of ransomware as a service further complicates the cyber security landscape. AI-driven automation is being used by ransomware groups to generate highly targeted attacks, leveraging vast datasets to identify vulnerabilities and craft even more convincing phishing messages. AI enables cybercriminals to scale their operations, making sophisticated attacks more accessible to less-skilled threat actors. In this evolving environment, the battle is shifting towards an AI versus AI cyber war, where defenders must develop AI-driven countermeasures to combat AI-powered threats, hopefully at the same pace as our adversaries.

Fortunately, AI is not just a tool for attackers; it is now being used for threat detection, response and automation. Microsoft's launch of security copilot agents at the end of April was initially aimed at privacy breach response, network supervision, security operations tooling recommendations, alert triage, and task optimisation to assist with forecasting and prioritisation of critical alerts, reducing alert fatigue, and potentially improving response and longer-term planning. Microsoft claims that agents not only alert, but also have the ability to take action.

For those not familiar with the technology, agentic AI is vastly different to a chatbot, possessing the ability to autonomously create plans and perform multi-step tasks on behalf of humans, as opposed to just answering questions about what it sees. Further advancements could see visual, verbal and spatial intelligence data being used to further train the AI model to respond to new threats.

The key difference with agentic AI is the level of autonomy and decision-making capabilities. Chatbots rely on predefined rules and scripts, while agentic AI systems can autonomously assess situations, formulate plans and execute actions to achieve the desired outcomes. Anecdotally, the feedback on the new Microsoft AI security stack has been mixed; but, to be fair, it is still early days, and it seems that there is great potential with agentic AI assisting human-led cyber teams.

This leads me to another fascinating question: As we increasingly place our

trust in machines, what will be the societal implications of combining quantum computing with AI? It is mind-boggling when thinking in the context of post-quantum cryptography.

Quantum computers could theoretically break many of the cryptographic algorithms that protect our data today, making sensitive information vulnerable. As technology advances at an unprecedented pace, there is a risk that it could outstrip our ability to understand and control it. AI systems, especially those enhanced by quantum computing, may present challenges in transparency, accountability and ethical decision-making. Will we reach a technological threshold where advancements become nearly incomprehensible to humans?

There may be a future war between adversarial AI versus cyber security AI; however, for now, the cyber security industry is very much human-led, and the importance of trained and dedicated cyber security professionals should not be overlooked. As we face uncertain economic and geopolitical times, a trend has emerged where organisations are merging generalist ICT engineering and management roles with cyber roles. I question the effectiveness of that approach, and I would argue that dedicated cyber professionals are now more important than ever before.

About the author

With more than two decades of experience driving innovation across cyber security, artificial intelligence, and ICT leadership, ***Dr Adrian Kaminski*** *is a recognised figure in Australia's cyber security landscape. Currently Cyber Security Leader at Ipswich City Council, Kaminski oversees the cyber resilience and strategic security posture of one of Australia's largest councils. His leadership has been instrumental in aligning organisational practices with global frameworks while championing a culture of security-first thinking across diverse teams.*

References

https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems

https://www.trendmicro.com/en_au/research/24/b/deepfake-video-calls.html

AI is reshaping cyber security – is your team prepared to respond?

Build artificial intelligence–ready cyber teams with practical, real-world training from SANS.

As generative artificial intelligence (genAI) continues to accelerate and evolve, it's fundamentally altering how cyberthreats emerge and operate. For CISOs and cyber security leaders, the challenge is no longer just about defending perimeters – it's about proactively preparing teams to adapt to threats that are faster, smarter and more dynamic than ever.

Traditional skill sets alone won't cut it. The rise of AI-powered attacks – from hyper-targeted phishing campaigns to self-learning malware – demands a shift in how we develop cyber talent.

The rise of AI-powered attacks – from hyper-targeted phishing campaigns to self-learning malware – demands a shift in how we develop cyber talent

The solution: targeted upskilling in AI-aware defence strategies

SANS Institute is at the forefront of this evolution, delivering an expertly designed curriculum that embeds AI and machine learning into its broader cyber security training portfolio. These offerings are tailored to meet the demands of today's cyber environment, balancing technical depth with strategic leadership skills.

For those at the beginning of their AI journey, SANS offers AIS247: AI Security Essentials for Business Leaders – a critical entry point course for CISOs, business leaders, security leads, and executives seeking to understand the opportunities and risks of integrating AI into their organisations. This course covers the fundamentals of genAI, explores its security implications, and provides guidance on ethical use, governance, and risk management – giving leaders the knowledge that they need to make informed decisions about AI adoption.

Here are four additional SANS stand-out courses that deliver immediate value for both practitioners and leaders:

- **SEC503: Network Monitoring and Threat Detection In-Depth:** Delivers essential capabilities for defenders, combining foundational knowledge with AI-enhanced methods to identify and interpret advanced network threats.
- **SEC504: Hacker Tools, Techniques, and Incident Handling:** Trains security professionals to detect and respond to incidents with increased speed and efficiency by leveraging AI-assisted threat analysis and automation.
- **LDR512: Security Leadership Essentials for Managers:** Equips rising security leaders with tools to make informed decisions using AI-derived insights and to manage teams effectively in complex risk scenarios.
- **LDR514: Security Strategic Planning, Policy, and Leadership:** Focuses on embedding AI into cyber security governance and long-term planning, helping executives align policy with the realities of AI-driven threats.

Why it matters for Australia

As Australian businesses and agencies continue to embrace digital innovation, the security function must adapt in parallel. SANS provides a trusted and proven framework to develop AI-capable teams that are ready to anticipate, understand, and disrupt the next generation of cyberthreats. •

To learn how SANS can help your organisation build AI-ready cyber teams, email ANZ@sans.org or call 02 6174 4581.

SANS

Generative Artificial Intelligence (GenAI) and Machine Learning (ML) Courses Road Map

SANS Institute's engagement with GenAI and ML not only encompasses training and education but also extends to cutting-edge research, community building, and shaping industry standards.

GenAI/ML Technology-Focused Courses

SANS Institute develops specialised courses that equip professionals and organisations with the skills and knowledge needed to address AI-related complexities.

AIS247
AI Security Essentials for Business Leaders

AIS247 trains professionals to integrate AI into business safely and effectively, covering GenAI principles, applications, risks, ethics, and policy for responsible implementation.

SEC535
Offensive AI – Attack Tools and Techniques

SEC535 teaches AI for offensive purposes, covering security bypassing, exploit development, social engineering, automated attacks, and malware creation, with hands-on labs for practical application.

SEC595
Applied Data Science and AI/Machine Learning for Cybersecurity Professionals

SEC595 demystifies data science and machine learning with 70% hands-on problem-solving, focusing on practical AI/ML applications in cybersecurity and balancing theory with real-world solutions.

GenAI/ML Integration-Enhanced Courses

SANS incorporates GenAI/ML training across its broader cybersecurity education courses, equipping professionals with the necessary expertise to tackle AI-related complexities and effectively defend against sophisticated cyber threats.

CYBER DEFENSE

SEC497
Practical Open-Source Intelligence (OSINT)

SEC497 teaches cybersecurity professionals to use AI-enhanced techniques and tools for gathering and analyzing publicly available data for security intelligence and threat assessment.

SEC503
Network Monitoring and Threat Detection In-Depth

Delivers the technical knowledge, insight, and hands-on training you need to confidently defend your network

SEC587
Advanced Open-Source Intelligence (OSINT) Gathering and Analysis

SEC587 trains professionals to use GenAI/ML for OSINT, focusing on advanced techniques to analyze and validate data from various sources.

FORENSIC & INCIDENT RESPONSE

FOR518
Mac and iOS Forensic Analysis and Incident Response

FOR518 teaches professionals AI-enhanced forensic techniques for Apple devices, improving accuracy in artifact analysis and security incident identification.

FOR577
LINUX Incident Response and Threat Hunting

FOR577 uses AI to enhance forensic investigations on Linux systems, improving validation and streamlining processes for more effective security incident detection and response.

FOR585
Smartphone Forensic Analysis In-Depth

FOR585 trains cybersecurity professionals in advanced, AI-enhanced techniques for analyzing and extracting forensic data from smartphones, enhancing mobile security incident detection and investigation.

OFFENSIVE OPERATIONS

SEC504
Hacker Tools Techniques and Incident Handling

SEC504 trains cybersecurity professionals in identifying and responding to threats, using AI to enhance detection, analysis, and automated response capabilities.

SEC598
Security Automation for Offense Defense and Cloud

SEC598 trains professionals to use advanced AI and automation to enhance offensive and defensive cybersecurity strategies in cloud environments.

CYBERSECURITY LEADERSHIP

LDR512
Security Leadership Essentials for Managers

LDR512 trains leaders to manage cybersecurity defenses strategically, using AI insights to improve decision-making and security policy development.

LDR514
Security Strategic Planning, Policy, and Leadership

LDR514 trains cybersecurity leaders in advanced strategies and policy development, using AI-driven data analysis to improve security governance and decision-making.

To find out how SANS can help your organisation build AI-ready cyber teams, contact us at **anz@sans.org** for more information | **+61 2 6174 4581**

Security strategy: decision-making on the Australian information highway

BY DR SRIRAM RAGHAVAN

The modern landscape of security strategy – much like the winding, often unpredictable Australian highway – demands constant vigilance, adaptability and a deep understanding of the environment.

Dr Sriram Raghavan

Both the Australian highway and security strategy are characterised by inherent risks, evolving threats, and the need for proactive decision-making to ensure safety and successful navigation. While one deals with digital fortresses and geopolitical tensions, and the other with asphalt and automotive traffic, the underlying principles of risk assessment, situational awareness, and strategic response share a striking resemblance.

The realisation that driving – which is a seemingly unexciting activity – can involve such intricate strategic thinking led me to consider the parallels in cyber security. The need for dynamic adaptation, real-time decision-making, and a holistic understanding of the environment are essential in both domains. Just as a driver on the highway must anticipate and react to the unpredictable nature of the road, a security professional on the digital namesake must navigate the ever-evolving landscape of cyberthreats; it involves a subtle combination of strategy and tactics.

Both the Australian highway and security strategy are characterised by inherent risks, evolving threats, and the need for proactive decision-making to ensure safety and successful navigation

For instance, when one finds themselves right behind a B-double truck, irrespective of the speed limits, it may be appropriate to momentarily risk acceleration to overtake the vehicle as it represents an obstacle in one's path. This obstacle limits one's ability to assess ambient road conditions as one's vision is blocked. It's an understanding that a one-size-fits-all approach rarely works on the road, and the same can be said about the cyber world. Both domains require a constant vigilance, state of adaptation and a deep understanding of the variables at play. In this article, I conduct a spirited comparison between the deep entrenched world of security and business strategy against those that one needs to contend with on the treacherous Australian highways.

Strategic decision-making: the perilous road

Navigating the Australian highway – a long stretch of asphalt cutting through diverse landscapes – becomes a dynamic exercise in real-time strategic decision-making. Driving here transcends mere steering; it's a continuous, fluid assessment of risk, opportunity and the ever-shifting variables of the road. Before even turning the ignition, strategic planning commences. Route selection, weather checks, rest stop planning and fuel calculations mirror the initial threat assessment in security.

During long drives, maintaining vigilance against fatigue is paramount. This requires proactive rest stops, hydration and mindful driving, drawing parallels with a long-term strategic security posture – requiring constant monitoring and adjustments. Merging onto a busy highway demands swift acceleration and precise timing, much like the rapid response required during a security incident. Judging the speed of oncoming traffic, finding gaps and smoothly integrating requires quick, accurate data processing akin to analysing threat intelligence. Energy levels play a role here; when tired, a more cautious approach is necessary.

Overtaking requires a calculated risk assessment. Is the road clear? Is your vehicle capable of a safe and swift manoeuvre? Are there potential hazards ahead? This parallels the decision to implement a specific security control or countermeasure, where the potential benefit must outweigh the risk. Speed cameras and patrol vehicles introduce a layer of regulatory risk, forcing a cost-benefit analysis, similar to the regulatory landscape in cyber security. Recognising when to slow down, yield ground or let another vehicle overtake is a crucial aspect of defensive driving, sustaining long-term survival. For instance, when one finds themselves behind a B-double truck, it presents an obstacle that directly impacts one's ability to maintain long-distance vision, and, consequently, one's vision is summarily blocked. This obstacle limits one's ability to assess road conditions, oncoming traffic and, in general, plan next steps. In such a situation, irrespective of the speed limits, it may be appropriate[1] to momentarily accelerate to

1 Please note that the author does not advocate for this activity.

overtake the vehicle to restore normalcy, as applicable.

When faced with such a unique situation, a driver may assess that the increased risk associated with momentary speeding in order to restore one's ability to see the road ahead to achieve one's strategic goals and develop future plans is acceptable. Conversely, if we are driving behind a small car, as long as the vehicle is keeping up with the ambient traffic speeds, and maintains a steady lead, a driver may be sufficient to simply follow the vehicle because one is still making steady progress and the vision is not obstructed. This reflects the need for flexibility and adaptability in security strategy; sometimes, the best course of action is to concede ground to mitigate a greater risk.

As a comparison, when the ambient technology landscape is saturated, it may be worthwhile considering experimentation with an up-and-coming technology, provided it is intended for a specific duration to yield a specific result, such as provide a clear path of its future use, or for discarding, as the case may be. In a similar vein, if there is a small organisation that is progressing successfully with experimentation of a new technology, it may be worthwhile copying their approach and not attempting to upstage their success. An organisation's priority with regard to how the strategy is designed is key in such scenarios; however, open experimentation with an untested technology can be damaging as one is not clear on when to 'pull the plug'. Therefore, the scope, investments and their impact threshold[2] must be established beforehand.

Ambient traffic plays a large role; aggressive drivers necessitate a more defensive posture. The ability to seamlessly transition between these decision points is the hallmark of a skilled driver. Energy levels, fatigue, and external factors like weather and traffic flow all influence these decisions. A one-size-fits-all approach is rarely effective. A reliable long-term driver understands that they must adapt to the road, and their own condition, to survive the long haul. The kinetic algorithm of highway driving translates surprisingly well to the complexities of security strategy. Just as a driver constantly scans their surroundings, security professionals must maintain comprehensive situational awareness of their networks and threat landscape. The decision to overtake or yield is a real-time risk assessment, similar to evaluating the potential impact of a cyberthreat. Adapting to changing road conditions and traffic patterns mirrors the need for security strategies to evolve in response to emerging threats. Fuel management and energy management are like budget and personnel management. Adhering to traffic laws is analogous to complying with data privacy, corporate compliance norms and applicable regulations. Fatigue, stress and distractions can impair driving performance, just as they can compromise security decisions.

As a comparison, if the organisation has just emerged from an exhausting reorganisation of staff and/or their business division, or that of a merger, it can be a difficult time to just jump into high gear and drive delivery using innovative methods, as both management and staff may be weary. In those situations, decisions have not been fully assessed. This may simply be an opportunity to let things get back to normal by doubling down on one's strengths, while gaining their energy back. This time can be utilised for re-establishing organisational objectives, human resource training, or plain old research, just until the organisation is ready to pounce again. Strategically, providing the organisation sufficient funds for sustaining trivial pursuits may be as significant as some quick shut-eye for a weary driver at a rest stop.

The terrain: defining the modern security landscape and the Australian highway

Modern security strategy grapples with a complex web of threats – ranging from cyber attacks and data breaches, to geopolitical instability and terrorism. The digital realm, once a frontier of boundless opportunity, has become a battleground where adversaries exploit vulnerabilities with increasing sophistication. Organisations face the daunting task of protecting sensitive data, maintaining operational continuity, and safeguarding their reputation in a world where information is both a valuable asset and a potent weapon. Similarly, the Australian highway system, spanning vast

2 Key performance indicators (KPIs)

distances and diverse terrains, presents its own unique set of challenges. Drivers must contend with varying weather conditions, unpredictable traffic patterns and the ever-present risk of accidents. The sheer volume of vehicles, coupled with the speed and complexity of modern transportation, creates a dynamic and potentially hazardous environment. Both domains are characterised by:

— *Dynamic and evolving threats:* Just as malicious cyber actors constantly develop new attack vectors, the Australian highway experiences fluctuations in traffic flow, construction zones, and unexpected hazards.
— *Interconnectedness and systemic risk:* A single security breach can have cascading effects across an organisation's network, much like how a traffic accident can trigger a chain reaction of delays and congestion on the highway.
— *The importance of situational awareness:* Security professionals must monitor threat intelligence and network activity to detect anomalies, while drivers must remain alert and aware of their surroundings to anticipate potential hazards.
— *The need for proactive planning:* Organisations must develop robust security strategies and incident response plans, while drivers must plan their routes, check weather conditions, and maintain their vehicles.

Risk assessment and mitigation: mapping the dangers and building defences

Effective security strategy begins with a thorough risk assessment, identifying potential threats and vulnerabilities. This involves analysing data, conducting penetration testing and evaluating the organisation's security posture. Similarly, navigating the Australian highway requires drivers to assess risks, such as fatigue, weather conditions, and the behaviour of other drivers. Key aspects of risk assessment and mitigation in both domains include:

— *Identifying vulnerabilities:* In cyber security, this involves identifying weaknesses in software, hardware and human behaviour. On the highway, it means recognising potential hazards like blind spots, slippery roads, and distracted driving.
— *Prioritising risks:* Not all threats are created equal. Security professionals must prioritise risks based on their potential impact and likelihood of occurrence. Drivers must prioritise risks based on the potential severity of the hazard.
— *Implementing controls:* Security controls – such as next-generation firewalls; user entity behaviour anomaly detection systems; and identity and access management controls, including multi-factor

authentication – are implemented to mitigate risks. Similarly, drivers employ defensive driving techniques, maintain safe following distances and adhere to traffic laws.

— *Developing contingency plans:* Incident response plans are essential for responding to security breaches and minimising damage. Emergency procedures and alternate routes are vital for highway driving in the event of accidents or road closures.

In the case of signal loss (i.e., absence of event audit logging or the greater risk of erasure of existing audit logs and associated anti-forensic techniques), organisations must prepare for the eventuality of expecting the presence of an intruder in their midst and anticipate their next moves in the absence of data. Decision-making in such a situation can be challenging, but one needs clarity on their Level Zero assets (aka crown jewels) and how these are protected from impact. Standard incident response tabletop exercises are a good start, but more realistic scenarios can be envisioned to ensure business and security strategies do not suffer.

Situational awareness: maintaining vigilance in a complex environment

Maintaining situational awareness is crucial for both security professionals and drivers. In the realm of cyber security, this involves monitoring network activity, analysing threat intelligence and staying abreast of emerging threats. On the highway, it means constantly scanning the environment, anticipating the actions of other drivers and adapting to changing conditions. Key elements of situational awareness include:

- *Data collection and analysis:* Security professionals rely on logs, alerts and other data sources to detect anomalies. Drivers rely on their senses, mirrors and instruments to gather information about their surroundings.
- *Pattern recognition:* Security analysts look for patterns of malicious activity, while drivers look for patterns in traffic flow and the behaviour of other vehicles.
- *Real-time monitoring:* Security operations centres monitor networks and systems in real time, while drivers constantly monitor their surroundings and adjust their driving accordingly.
- *Adaptive response:* Security professionals must adapt their defences to evolving threats, while drivers must adapt their driving to changing road conditions and traffic patterns.

In both security and driving, the human factor plays a critical role. Security awareness training is essential for mitigating the risk of human error in cyber security, while driver education and training are crucial for preventing accidents on the highway

Strategic decision-making: navigating the uncertainty and making informed choices

Both security strategy and highway driving require strategic decision-making in the face of uncertainty. Security professionals must weigh the costs and benefits of different security measures, while drivers must make split-second decisions in response to unexpected events.

Key aspects of strategic decision-making include:

- *Information gathering:* Security professionals gather information from various sources, including threat intelligence feeds, incident reports, and industry best practices. Drivers gather information from road signs, maps and GPS navigation systems.
- *Risk assessment:* Security professionals assess the potential impact of different threats, while drivers assess the risks associated with different driving manoeuvres.
- *Decision analysis:* Security professionals evaluate different security options, while drivers evaluate different driving options.
- *Implementation and evaluation:* Security professionals implement security measures and monitor their effectiveness, while drivers execute their driving manoeuvres and evaluate their outcomes.

The human factor: the importance of training and awareness

In both security and driving, the human factor plays a critical role. Security awareness training is essential for mitigating the risk of human error in cyber security, while driver education and training are crucial for preventing accidents on the highway. Key aspects of the human factor include:

- *Training and education:* Security professionals require specialised training to develop the skills and knowledge necessary to protect against cyberthreats. Drivers require driver education and training to develop the skills and knowledge necessary to drive safely.
- *Awareness and vigilance:* Security awareness training helps employees recognise and avoid phishing attacks and other social engineering tactics. Driver education emphasises the importance of staying alert and avoiding distractions.
- *Communication and collaboration:* Effective communication and collaboration are essential for responding to security incidents and coordinating emergency response on the highway.
- *Fatigue and stress management:* Both security professionals and drivers can experience fatigue and stress, which can impair their judgment and decision-making.

The technological landscape: leveraging technology for enhanced security and safety

Technology plays a vital role in both security strategy and highway safety. Security tools, such as firewalls, intrusion detection systems and encryption, are essential for protecting against cyberthreats. Advanced driver-assistance systems, such as lane departure warning and adaptive cruise control, are enhancing safety on the highway. Key technological advancements include:

— *Artificial intelligence (AI), machine learning (ML) and generative AI (genAI):* AI and ML models are being regularly used across various security vendors and solution providers to detect and respond to cyberthreats, as much as the use of genAI to summarise information and create new content is being trialled across the world, as well as to improve traffic flow and safety on the highway.

— *Public cloud computing:* Cloud infrastructure is enabling organisations to store and process data more securely and efficiently, to the point where it has become a major ingredient of modern organisations. It also allows for the collection and analysis of traffic data for real-time updates.

— *Internet of Things (IoT):* IoT devices are being used to monitor traffic conditions, detect hazards, and provide real-time information to drivers. IoT devices are also being used to monitor and secure industrial control systems.

— *Big data analytics:* Big data analytics is being used to identify patterns and trends in security data and traffic data, enabling security professionals and traffic managers to make more informed decisions.

The regulatory environment: navigating the legal and ethical landscape

Both security strategy and highway driving are subject to a complex regulatory environment. Security professionals must comply with data privacy laws and industry standards, while drivers must adhere to traffic laws and regulations. Key regulatory considerations include:

— *Data privacy laws:* Organisations must comply with data privacy laws, such as the General Data Protection Regulation and California Consumer Privacy Act, to protect sensitive data. Drivers must comply with traffic laws, such as speed limits and seat belt regulations.

— *Industry standards:* Security professionals must adhere to industry standards, such as ISO 27001 and the National Institute of Standards and Technology Cybersecurity Framework. Drivers must adhere to vehicle safety standards and regulations.

— *Ethical considerations:* Security professionals must consider the ethical implications of their actions, such as the use of surveillance technology. Drivers must consider the ethical implications of their driving behaviour, such as driving under the influence.

— *Liability and accountability:* Organisations are held liable for security breaches, while drivers are held liable for traffic accidents.

Conclusion: a shared journey of constant adaptation

The modern age of security strategy and the Australian highway, while seemingly disparate domains, share a common thread: the need for constant adaptation in the face of evolving threats and challenges. Both require proactive risk assessment, vigilant situational awareness, and strategic decision-making. By understanding the parallels between these two domains, we can gain valuable insights into the principles of effective risk management, and navigate the perilous paths of our increasingly complex world with greater confidence and resilience. The core principles of preparation, vigilance and adaptation are not just applicable to cyber security professionals or drivers on the highway, but are fundamental to navigating any complex system where risk and reward are constantly in flux. •

About the author

Dr Sriram Raghavan *is the accomplished architect of threat-informed defence engineering (TiDE) strategies, most recently at Telstra. He is also a recognised author, and a member of the MITRE Engenuity and the CSA Top Threats working groups. He holds a PhD in computer science, and specialises in cyber security and digital forensics.*

Fifty shades of deception

BY DR XINGLIANG YUAN, ASSOCIATION PROFESSOR, THE UNIVERSITY OF MELBOURNE

Fighting back against deceptive patterns on the internet.

Dr Xingliang Yuan

Every time you try to unsubscribe from a service and cannot find the exit, or you get lured into clicking a button that's really an advertisement, you have encountered deceptive patterns – i.e., user interface (UI) tricks designed to manipulate users' decisions.

In an era where online platforms compete relentlessly for user attention and retention, deceptive patterns have become increasingly sophisticated. Now, a new study from my team at The University of Melbourne, in collaboration with CSIRO's Data61, sheds critical light on this growing issue, and provides a new tool built from multimodal large language models (MLLMs) to fight back.

A unified front against manipulation

Our study introduces a unified taxonomy that redefines how deceptive patterns are understood, particularly from a security and privacy perspective. Previous studies catalogued these design tricks, but rarely connected them to more serious consequences – like data leaks, privacy violations or financial exploitation.

By systematically reviewing prior taxonomies and identifying inconsistencies, our team constructed a comprehensive classification taxonomy of deceptive patterns that includes 21 categories, such as 'forced enrolment', 'hidden costs', 'false hierarchy', and 'toying with emotion'. These categories not only capture visual manipulations, but also capture the underlying intent and potential harms.

This taxonomy serves as a foundation for protecting user autonomy and enhancing digital trust in an increasingly manipulative internet environment.

DPGuard: generative artificial intelligence for UI deception detection

At the heart of our study is DPGuard, an innovative detection tool that uses MLLMs to spot deceptive patterns in mobile apps and websites.

Traditional methods relied on manual inspection or rule-based systems that could not keep up with evolving tricks of deceptive patterns. DPGuard changes the game by combining a binary classifier (to flag suspicious designs) with an MLLM that uses prompt mutation (i.e., an adaptive way to fine-tune how the model interprets and classifies tricky interface elements).

In tests across more than 12,000 real-world UI screenshots, DPGuard outperformed the state-of-the-art tools like AidUI and UIGuard, achieving detection F1 scores of more than 73 per cent on mobile and nearly 50 per cent on web-based deception.

A massive dataset to train the next generation of defenders

To build such a model with high utility, we created a dataset (the largest dataset so far) on deceptive patterns – more than 10,000 deceptive instances across 6700 UI images from mobile and web platforms.

Importantly, the dataset includes not just historical examples, but also new, real-world cases captured from 2000 of the most popular apps and websites in 2024. This ensures that the model remains effective against the latest deceptive patterns.

Our finding reveals that nearly 50 per cent of websites and more than 25 per cent of mobile apps contained at least one deceptive pattern. What's worse is that many used multiple tricks simultaneously.

Security implications

While many users see deceptive patterns as annoyances, our paper makes a strong case that they pose serious security and privacy threats. For instance, 'forced enrolment' (which requires users to sign up without an opt-out) can lead to involuntary data exposure. 'Hidden information' obscures critical terms in tiny text or hyperlinks, enabling uninformed consent. And 'toying with emotion' preys on urgency or guilt to pressure quick decisions, often bypassing rational scrutiny.

These tactics are not just unethical; they can be exploited by attackers to phish for data, install malware, or harvest private information.

By integrating these risks into their taxonomy and detection methods, we bridge the gap between user experience manipulation and cyber security – a crucial step forward.

Looking ahead: tools for regulators, developers and users

With legal and regulatory pressure mounting, such as General Data Protection Regulation's stance on misleading consent banners, tools like DPGuard offer a timely assist. Regulators can use it to audit user interfaces at scale, developers can test designs before release, and advocacy groups can monitor bad actors more effectively.

Our team has also made its tool open source, allowing others to extend and adapt it for different platforms and regions. DPGuard is just the beginning. Our goal is to give power back to the users and to build trust and support transparency across the digital ecosystem. •

This article covers the research of the author's PhD student, Zewei Shi, in collaboration with Feng Liu from The University of Melbourne, and Jason Xue, Jieshan Chen and Ruoxi Sun from CSIRO's Data61. It has been published in ACM Web Conference 2025, and can be found at https://arxiv.org/pdf/2501.13351

The author gratefully acknowledges the contribution of Dr Suelette Dreyfus in writing this article.

About the author

***Dr Xingliang Yuan** is an Associate Professor at The University of Melbourne. He has a keen interest in designing systems and protocols to address real-world privacy and security challenges. His research has been supported by the Australian Research Council, CSIRO, the Australian Department of Home Affairs, the Australian Department of Health and Aged Care, and the Oceania Cyber Security Centre. His work has been published in major venues of computer security and systems, such as CCS, S&P, USENIX Security, NDSS, TDSC, and TIFS.*

Australia's Kaspersky ban: the unanswered questions

BY DINESH VELUSAMY

A cyber security turning point or just the beginning?

Dinesh Velusamy

The Australian Government's decision to ban Kaspersky products marks another milestone in the ongoing global crackdown on foreign cyber security threats. While the ban is a decisive move aimed at safeguarding national security, it raises many pressing questions: What happens to individuals and businesses that already have Kaspersky installed? How does Australia manage foreign travellers who bring in devices running the software? If Kaspersky poses a genuine threat, can it still exploit active machines within the country? The implications extend far beyond a simple prohibition.

The Australian Cyber Security Centre has long advised organisations to conduct risk assessments on foreign software providers, particularly those linked to governments that may act against national interests. Kaspersky's connections to Russia have been scrutinised globally, with several nations restricting or outright banning its usage in government and critical sectors. The concern extends beyond its origins, focusing on the potential for coercion by foreign state actors.

The ban on Kaspersky signals a growing shift towards digital sovereignty, where governments are increasingly cautious of foreign influence over cyber security tools. This could begin a broader movement to reassess security software and the entire digital supply chain

A digital Trojan horse? The lingering threat of legacy installations

If Kaspersky is indeed a cyber security threat, the continued presence of its software on Australian devices presents a significant ongoing challenge. With its extensive system access, security software can be both a powerful defence and a potential risk for exploitation. Even after a ban, existing installations can continue receiving updates, accessing sensitive information, and interacting with networks – posing significant risks. This raises a crucial question: Does prohibiting new sales adequately address the issue if the software remains operational on numerous Australian devices?

The potential risks are not merely theoretical. Security firms and intelligence agencies around the globe have highlighted the dangers of foreign software with privileged access to data. If exploited through remote updates, a compromised cyber security suite could pave the way for data exfiltration, unauthorised surveillance or cyber sabotage. If a backdoor were introduced via an innocuous software patch, organisations using Kaspersky might unwittingly find themselves vulnerable to a state-sponsored attack. The concern isn't just about what the software is doing now, but also what it could potentially do in the future.

Apart from domestic installations, the issue of foreign devices entering Australia represents another oversight. Travellers and business professionals arrive daily with laptops and smartphones loaded with software from their home countries. Should Australian authorities begin screening devices at the border now that Kaspersky is restricted? Although physical inspections of electronic devices are still rare outside of extremely sensitive national security situations, the ban prompts the question of whether enforcement should apply to users beyond domestic ones. Banned software could breach corporate networks and government systems through personal devices without rigorous measures, bypassing the restrictions.

One potential enforcement strategy involves requiring companies and government agencies to conduct security scans on all external devices before granting them access to corporate or government networks; however, rolling out such policies at scale poses logistical challenges. Companies must invest in new endpoint detection systems and ensure employee compliance, while government agencies must guide secure software alternatives.

Cyber crackdown or geopolitical strategy? The future of foreign tech in Australia

The enforcement of regulations presents a multifaceted challenge. The government may consider collaborating with internet service providers to prevent Kaspersky from receiving updates or transmitting data within the borders of Australia; however, such measures would require significant technical oversight. Organisations, particularly those within critical infrastructure and financial sectors, may need to be mandated to conduct audits of their cyber security frameworks and eliminate any software subject to regulatory scrutiny. Corporate IT departments are likely to assume a leadership role in ensuring compliance, with potential penalties for noncompliance. Nevertheless, the overarching issue remains: If Kaspersky represents a security risk today, has it always posed a risk? Furthermore, what damage may have already transpired if that is the case?

Cyber security experts have indicated that, although Kaspersky has not been definitively shown to be involved in any malicious activities, the potential risks associated with software that foreign governments may influence are challenging to dismiss. Some contend that, rather than implementing outright bans, conducting independent audits and maintaining continuous monitoring of foreign security software could represent a more practical approach. Nonetheless, the evolving dynamics of global cyber warfare and the rising frequency of nation-state attacks allow minimal tolerance for ambiguity.

The ban on Kaspersky signals a growing shift towards digital sovereignty, where governments are increasingly cautious of foreign influence over cyber security tools. This could begin a broader movement to reassess security software and the entire digital supply chain. The question remains: Will Australia extend this scrutiny to other foreign tech providers, and how does it balance national security concerns with the realities of a globally interconnected cyber ecosystem?

This situation isn't unique to Australia. In 2017, the United States banned Kaspersky from federal networks due to national security concerns. The European Union has also taken a cautious approach, with various member states gradually removing Kaspersky products from government infrastructure. The global trend indicates that nations will continue to prioritise software developed within allied regions as cyber security threats become more sophisticated. At its core, this isn't merely a software ban; it's a national security move with far-reaching consequences. If Kaspersky poses a genuine threat, decisive action must go beyond blocking new installations. The challenge lies in managing legacy installations, monitoring incoming devices and ensuring that the measures designed to enhance security do not unintentionally create new vulnerabilities. As Australia navigates this transition, the rest of the world will be watching closely, weighing the balance between cyber security and the globalised nature of modern technology.

At its core, this isn't merely a software ban; it's a national security move with far-reaching consequences. If Kaspersky poses a genuine threat, decisive action must go beyond blocking new installations

The reality is that removing Kaspersky from the Australian market does not automatically ensure the country's safety from cyberthreats; it raises the question of what should come next. Will other foreign cyber security providers face similar scrutiny? How can Australian businesses ensure their cyber security solutions remain resilient against evolving digital threats? And, most importantly, will this ban genuinely make Australia safer, or is it just the beginning of a much larger debate about who controls the digital infrastructure of the future? •

About the author
Dinesh Velusamy *is a technologist, entrepreneur and business leader with more than 20 years of international experience in cyber governance, risk and compliance; artificial intelligence; and information technology service management. Currently pursuing a PhD, he also holds master's degrees in IT and cyber security. Velusamy is passionate about cyber security policy reform and the ethical application of emerging technologies.*

Cyber security in SMEs: a leadership imperative

BY GLAUCO GEORGINI

Cyber risk is no longer just a technical issue in an increasingly digital business environment. For small and medium-sized enterprises, it has become a matter of governance, continuity, and reputation.

Glauco Georgini

Despite the common belief that smaller businesses fly under the radar, the data suggests otherwise. Small and medium-sized enterprises (SMEs) are frequently targeted precisely because their defences are typically less sophisticated than larger organisations. According to recent industry reports, more than 60 per cent of small businesses that suffer a significant cyber attack close their doors within six months – a stark reminder of what's at stake.

This article offers a strategic perspective for boards, executive leaders and business owners seeking to lead with digital responsibility, while providing guidance for IT and security professionals on how to effectively support SME leadership in this crucial journey.

Start with visibility: understand your risk profile

Effective decision-making begins with clarity. Regular cyber risk assessments – targeting critical digital assets, third-party vulnerabilities and operational continuity – establish a strong foundation for informed strategic planning.

Boards should ask: What assets are most critical to our operations? What's the financial and reputational impact of a cyber disruption? Do we have an incident response plan that's been tested and proven effective?

Security and IT professionals should collaborate closely with business leaders to align critical assets with key business functions. By translating technical vulnerabilities into clear, business-focused risks – free from jargon – they can foster shared understanding and informed decision-making. Regular risk assessments should go beyond identifying technical gaps to emphasise the potential impact on operations, reputation and strategic objectives.

Your people are your front line

More than 80 per cent of cyber incidents exploit human error. Security should not be isolated in the IT department – it must be embedded in the company culture, championed by leadership, and embraced across all functions.

Action points are as follows:

— Deliver clear, engaging and contextual training regularly.
— Run phishing simulations and social engineering tests that reflect real-world scenarios.
— Foster a culture of reporting, not blaming.
— Celebrate security wins and learning moments.

Security professionals should work hand in hand with department heads to understand their unique challenges. Appointing security champions within each team helps connect IT security with everyday business operations. When it comes to training, it's far more effective when it ties directly to what people do in their day-to-day roles, rather than focusing on abstract or overly technical ideas.

Adopt a framework that matches your maturity

Frameworks like the Essential Eight, ISO/IEC 27001, or the National Institute of Standards and Technology Cybersecurity Framework should be adapted to your business reality. These aren't mere checklists – they're strategic tools that can be scaled according to your organisation's needs and maturity.

SMEs without internal expertise may benefit from a virtual CISO offering flexible, high-level guidance aligned with board expectations and business objectives.

Security and IT professionals can focus on progressive implementation that addresses the most significant risks first, rather than aiming for framework perfection immediately. A road map demonstrating continuous improvement aligned with business growth objectives will gain more traction with leadership. Getting involved in local security communities and professional networks also helps teams to share real-world experiences and best practices tailored to the challenges that SMEs face.

Backup and recovery: test it before you need it

No resilience plan is complete without strong, tested backups and a business continuity strategy. Cyber incidents – particularly ransomware – can halt operations in minutes, making the difference between quick recovery and business failure.

Executives should ask: How long would it take us to restore operations after an attack? What is the cost of that downtime? Have we tested our recovery processes under pressure?

Security and IT professionals can implement the 3-2-1 backup rule (three copies, two different media types, one offsite) and regularly test restoration processes with business stakeholders present. Documenting recovery time objectives for each critical system and validating these timelines against operational requirements ensures that business continuity plans remain realistic and effective.

Compliance as a competitive advantage

In Australia, regulations like the Privacy Act and mandatory breach reporting under the Notifiable Data Breaches scheme are shaping how businesses manage information security.

Demonstrating compliance isn't just about avoiding fines – it's about maintaining trust with clients, investors and partners. Forward-thinking SMEs are leveraging their security posture as a market differentiator when competing with larger enterprises.

Security and IT teams can stay up to date with local regulations by staying active in industry associations and professional groups. Using simple dashboards to track compliance progress makes it easier for leadership to see where things stand. And when you show how security investments directly support compliance goals, it's much easier to make the case for the budget and resources you need.

Simulate before you're surprised

Penetration testing, vulnerability assessments and red team exercises offer visibility into real-world vulnerabilities before attackers exploit them.

Directors should expect regular updates and executive-friendly reporting that clearly outlines the business impact and risk mitigation. These simulations should evolve as your business grows and your threat landscape changes.

Security and IT professionals can build relationships with trusted security testing partners who understand the SME environment. Creating clear scopes for testing that align with business priorities ensures that resources are well spent. Translating findings into business impact statements helps non-technical leaders understand the significance of identified vulnerabilities.

Build community connections

SMEs benefit tremendously from community engagement around cyber security. Industry associations, government programs like the Australian Cyber Security Centre's Small Business Cyber Security Guide, and local business networks offer resources specifically designed for organisations with limited security budgets.

Security and IT professionals can actively participate in local security meet-ups, forums, and information-sharing communities. Establishing or joining informal networks of security professionals working in SMEs creates valuable support systems. Bringing community resources back to leadership teams helps SMEs stay current without reinventing the wheel.

Conclusion

For C-level leaders, cyber security is not an IT problem – it's a business priority. Building a resilient organisation is about enabling long-term growth and protecting your most valuable assets: trust, reputation and continuity.

Effective cyber security governance starts at the top. But its success depends on collaboration between leadership, IT professionals and the entire workforce. The businesses that treat cyber security as a strategic pillar – rather than a technical check box – will lead the future. •

About the author

Glauco Georgini *brings over 25 years of global experience in information technology, with the past decade dedicated to leading cyber security strategies, uplift programs, and GRC initiatives across more than 15 countries. In Australia, he has held executive roles as Head of IT and CISO for major insurance providers, and now delivers strategic advisory through The Black Belt CISO Pty Ltd.*

References

U.S. National Cyber Security Alliance (NCSA) and Ponemon Institute study (2023)

Verizon Data Breach Investigations Report (2023)

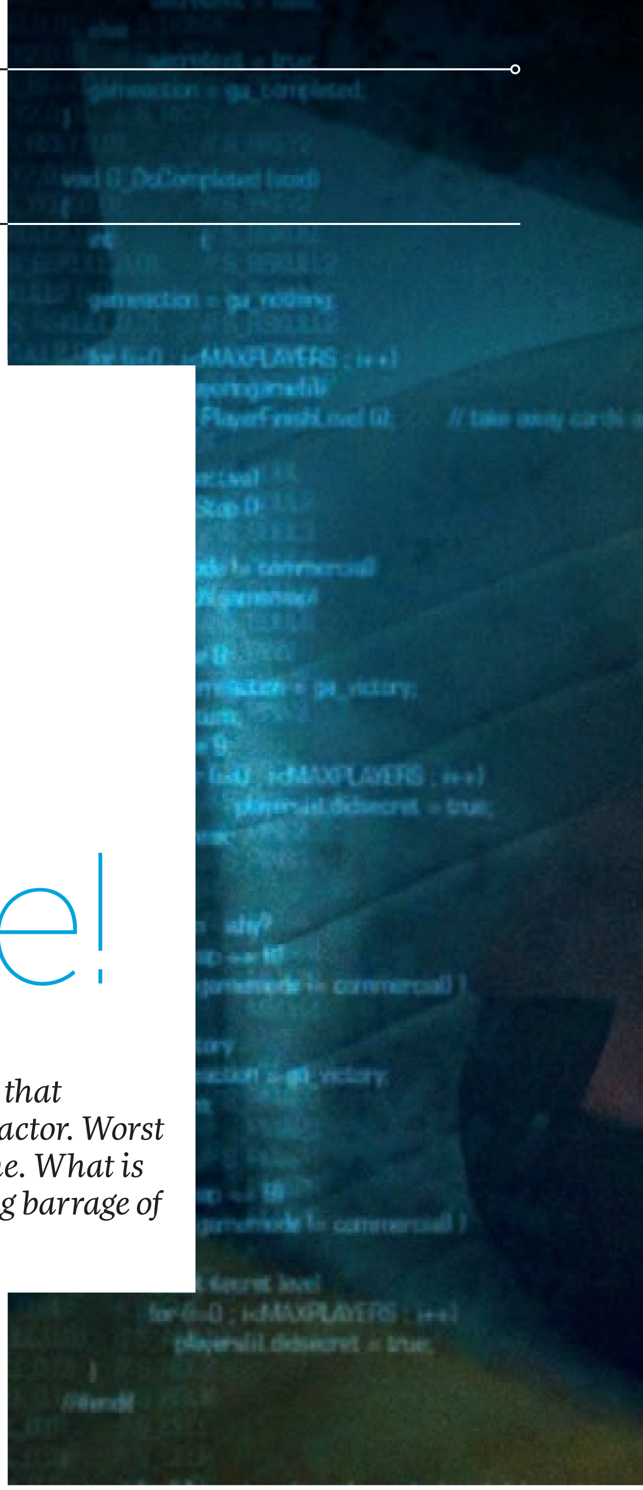
World Economic Forum's Global Risks Report (2023)

National Institute of Standards and Technology (NIST) Special Publication 800-34

Australian Cyber Security Centre's Essential Eight framework

Office of the Australian Information Commissioner (OAIC)

Australian Cyber Security Centre's – Small Business Cyber Security Guide



Help, the paranoids are after me!

BY WAYNE TENTORI

I have found it hard to sometimes stop myself from thinking that whenever I have a computer glitch, it is the work of a threat actor. Worst still, a threat actor from another country that is targeting me. What is triggering this mental anguish? I think it's the overwhelming barrage of cyber incidents that I see daily. So, how do I combat this?

Wayne Tentori

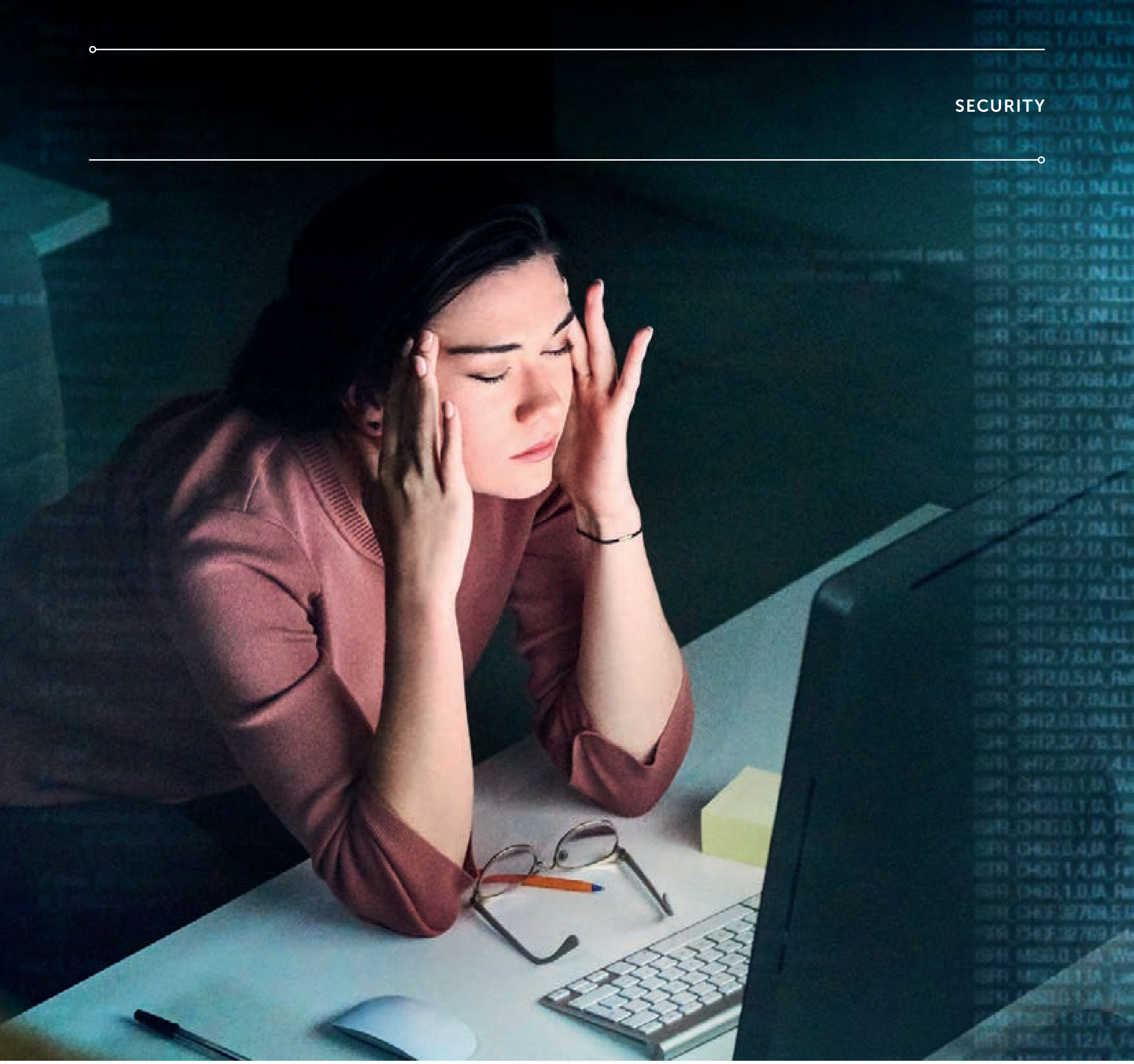
I'm not a psychologist, or any sort of medical practitioner, so any advice I give comes with the caveat that it is from my life experience, and it's something that works for me.

It is so easy to become paranoid when you read so many cyber security reports every single day. Threat actors can be sitting in your network for months, if not years. They can easily steal your communications, network traffic and bank account details. They can simply edit a photograph or video to make it something completely different. They can intercept invoices and change the bank details. Phishing, distributed denial of service attacks, ransomware, malware, romance and investment scams, keyloggers, exploits ... stop the ride, I want to get off!

Yes, sometimes it could very well be a threat actor causing issues; but it could also be a computer just being a computer. Ever had that urgent email you had to send or report you had to finish, and the computer or the software decides to hang, making you miss a deadline? So, which is it: hardware, software, electrical or internet failure? Quick, call the IT guy! (Sigh ... that's me.) Okay, not a computer glitch – maybe it's something more sinister? Call the IT guy! (Yeah, that's me again.) Let the investigation, isolation of endpoints, virus checking and so on begin.

One question I do ask myself is, 'Why am I a target?' Threat actors and scammers will firstly go for the low-hanging fruit. Have I made it too easy for them? Maybe I should set up a stronger password or get around to setting up multi-factor authentication. Have I left myself logged in and walked away from my PC? Maybe I should not have connected to the free wi-fi at the coffee shop and just used my phone's 5G network to hotspot. I must stop taking shortcuts.

Am I a stepping stone onto the wider network? Do they want to impersonate me to get higher up the corporate chain? Do I have



privileged logins? Are they after the keys to the kingdom? I think I had better make myself more diligent with what information I give out and to whom, and I must guard my knowledge and logins more closely.

Am I suffering from a moment of weakness? It's late in the afternoon, you are tired, your brain has been overloaded all day. A scammer rings you at that tiring moment or at a time you are stressed with 15 things that must be done in the next 20 minutes. Scammers love to interact with people who are at their lowest point or stressed. They know that you haven't got the time and are likely just to give them whatever they want, just to get them out of your hair. Time to switch into risk management mode.

Okay, I'm tired or stressed; I must make time to do something about it. More coffee? Chocolate? Water? Maybe a quick walk outside in the fresh air? Should I splash some cold water on my face? Whatever works to combat that tiredness or stress. Even take three deep breaths, filling your lungs fully to get oxygen to that think tank in your head. Right, ready for that scammer call. Now I can give them a piece of my mind and not my bank account details. •

About the author

Having spent 20 years in the Navy, and a further 24 years as a technician and data administrator in the Education Department of Western Australia, ***Wayne Tentori*** *is currently studying cyber security with a goal of a career change. He calls on his vast experience to help with his current studies, work, and to develop his keen interest in computer forensics and intelligence.*

Risk education for cyber leaders

BY DENNY WAN AND DR PRANIT ANAND

While risk, and therefore risk management, is intrinsic to an organisation and its operations, the evolving threat landscape challenges us to think about risk management in more creative ways.

Effective risk management is crucial to safeguarding the continuity of essential services and operations. This article explores contemporary risk management with a particular focus on the role of training and education, meaningful institutional collaborations, and application of appropriate tools and frameworks, aligning these with the recently released Australian Government's Protective Security Policy Framework (PSPF).[1]

Risk management

As our presence within the digital space increases, so too does our exposure to an evolving landscape of threat and risk. While the management of risk is a normal part of organisational operations, the increasing complexity of these risks requires careful consideration. Risk, in a nutshell, is any activity that has the potential to disrupt normal operations. Based on this simple definition, organisations have been doing risk management for a long time; however, the nature and complexity of contemporary risks, spurred on significantly through our digital and complex operations, puts many of these risk management strategies on notice, requiring a rethink about how we go about risk management. Effective risk management, therefore, is crucial for safeguarding sensitive information, and ensuring ongoing competitiveness and continuity of essential services.

While our digital presence and technologies increase our exposure to complex risk landscapes, it also presents us with opportunities for more transparent and informed risk management across all levels of an organisation. Leveraging advanced technologies for data collection, analysis and reporting enables stakeholders across all levels of an organisation to make better informed decisions, factoring in cyberthreats, regulatory changes, and geopolitical uncertainties. These technologies also enhance the organisation's ability for ongoing monitoring and review, enabling timely adjustments and improvements, and ensuring that the risk management strategies remain relevant and effective in the face of evolving threats.

The most significant piece in this, however, is education and training for all decision-makers. While having access to timely information is crucial, understanding how to decipher these for business continuity remains paramount to ensuring that organisations are responding in the most informed way, and that they can pivot appropriately as these requirements evolve. While it's encouraging to see risk management entering boardroom discussions, many executive-level decision-makers may not have the nuanced expertise to respond to contemporary risk-related data. Focused executive-level education and training around risk management may help to bridge this gap.


Denny Wan


Dr Pranit Anand

... organisations have been doing risk management for a long time; however, the nature and complexity of contemporary risks, spurred on significantly through our digital and complex operations, puts many of these risk management strategies on notice, requiring a rethink about how we go about doing risk management

PSPF Release 2024: a risk-led security management approach

The PSPF sets the Australian Government's minimum protective security standards to achieve effective and efficient secure delivery of government business, both domestically and internationally. PSPF Release 2024 has been expanded to include the risk and technology domains.

The rest of this article examines some contemporary risk education available for cyber leaders to equip them to manage and deliver in the risk domain.

The University of New South Wales (UNSW) Business School[2] was named the best Business School in Australia in the annual *Australian Financial Review* BOSS rankings[3] in 2024, where UNSW Sydney retained its Top 20 position in QS

World University Rankings[4]. The UNSW Business School has a long-established reputation in providing risk education to business leaders and equipping them with cyber security knowledge. The school is committed to providing risk education to cyber leaders, equipping them with risk language to enable effective business communication and supporting collaborative investment decisions on cyber resilience.

Security risk management is logical, systematic and transparent, and forms part of the enterprise risk management process. Risk tolerance describes the acceptable risk, after treatments are in place, to achieve an objective or manage a category of risk. It is highly dependent on the entity's unique context and the Accountable Authority's judgement. The Accountable Authority of a Commonwealth entity is defined under section 12 of the Public Governance, Performance and Accountability Act as the person or group of persons responsible for, and with control over, the entity's operations. The CISO is accountable to the Accountable Authority for cyber security. The Accountable Authority and Chief Security Officer are ultimately responsible for fostering a positive security culture. They are supported by the CISO and security practitioners to promote a culture where personnel value, use, and protect entity information and resources appropriately.

> The rapidly evolving man-made nature of cyber attacks without correlation with natural climate cycles or economic fundamentals amplifies the difficulty in measuring cyber risks and the expected financial loss

Cyber risk education for cyber leaders

Cyber risk education and training plays a key role in our ability to respond to the evolving risk landscape we continue to face. Appropriately designed cyber risk education and training programs enable organisations and individuals to recognise and respond to potential risks effectively. While many cyber security professionals may already possess an understanding of cyber security principles, contemporary cyber risk education programs also address the gap around risk assessment techniques, including use and application of advanced technologies and emerging frameworks. These enable organisations and individuals to anticipate and act proactively to potential threats, rather than reacting to existing incidents. An appropriately trained and educated workforce, capable of managing risks, ensures business continuity and adherence to regulatory requirements – critical to maintaining secure digital environments.

While various mainstream education programs provide introductory-level engagement with contemporary risk management, an emerging education landscape that focuses on just-in-time training and short courses expands the opportunities for training and development to more diverse groups within organisations. Short courses and micro-credentials provide professionals with the opportunity to pivot their training and development needs as and when needed, enabling ongoing progression with their careers, and ensuring that they are keeping abreast with the contemporary ideas around cyber risk as it evolves. For example, individuals can opt to undertake a micro-credential course specific to an area of risk management that their organisation needs. Short courses and micro-credentials further expand the opportunities for senior executives involved in crucial decision discussions about cyber risks and business continuity.

Overall, cyber risk education is a foundational element of contemporary risk management, enabling organisations to build resilient cyber security frameworks and protect against the ever-evolving landscape of cyberthreats.

Measure what needs to be managed

Business management is, in simple terms, managing risks in the business to ensure its proper operation and profitability. The UNSW Business School has a proven track record in delivering risk education to many generations of Australian business leaders. Cyber risk management is not dissimilar to the management of other risks, but measuring cyber risk is often considered to be more challenging than measuring other business risks (such as financial risks, contract risks or regulatory risks). These risk measurements are often guided by extensive history case laws, settlement payouts and regulatory decisions.

Cyber is a relatively new risk category without the benefit of these historical records for guidance. In addition, the rapidly evolving man-made nature of cyber attacks without correlation with natural climate cycles or economic fundamentals amplifes the difficulty in measuring cyber risks and the expected financial loss.

The FAIR Institute risk quantification standard[5] was developed to provide a structured, consistent, data-driven and defensible methodology to measure cyber risks independently and methodically. This consistent methodology for cyber risks enables investment in cyber resilience uplift to be managed effectively under the enterprise risk management (ERM) in the same manner as other business risks mentioned previously. It is unsurprising that the National Institute of Standards and Technology[6] named FAIR as the enabler to integrate cyber security with ERM. By introducing FAIR into the business risk management curriculum, cyber leaders can be trained to manage and report cyber risk to the executive team and business board. This breakthrough in the uplift in the risk education program equips cyber professionals to communicate with business leaders in prioritising and tracking investment in cyber resilience, measured in return on investment.

The common axiom is 'manage what can be measured'. Cyber risk management has been relegated to the 'too hard basket' until recently. The CrowdStrike global outage in 2024[7] was a wake-up call to the board that cyber risk is a business risk and not merely a technology problem or inconvenience. Failure to manage cyber risk can result in regulatory actions against company directors. The landmark Australian Securities and Investments Commission prosecution against RI Advice for its failure to manage cyber security is a sign of the times. •

About the authors

Denny Wan *is an AISA Fellow recognised for his leadership and community effort in raising awareness of the Open FAIR risk quantification standard. Open FAIR, as a business language, enables effective communications between business and cyber leaders. He is a member of the FAIR Institute standards committee, tasked with driving innovation of the FAIR standards. He was named the FAIR Ambassador, recognised for his achievement in connecting business and cyber leaders to improve the communications of cyber risks. He has also been appointed as the CI-ISAC Ambassador for Risk Measurement, bringing the decision science to threat-led defence informed by risk intelligence. Wan applied FAIR to assert reasonable security, which is a balance between the burden from control enforcement and the resultant measurable reduction in financial loss. This balance enables business and cyber leaders to align their priorities with investments in cyber security controls. He founded the Reasonable Security Institute to encourage the practice of this transformative risk management paradigm.*

Dr Pranit Anand *is a Senior Lecturer at the UNSW Business School, Member of the Australian Computer Society and a Senior Fellow of the Advanced Higher Education (United Kingdom). He is part of the teaching and research team within their cyber security specialisations. His research sits at the nexus of application and education of cyber security, continuously exploring opportunities to make cyber education accessible for diverse and under-represented groups, and through that is aiming to make understanding of and our responses to cyberthreats and risk as diverse as possible.*

References

1 https://www.protectivesecurity.gov.au/

2 https://www.unsw.edu.au/business

3 https://www.unsw.edu.au/news/2024/10/unsw-named-best-business-school-in-australia-in-annual-afr-boss-?utm_source=linkedin&utm_medium=social

4 https://www.unsw.edu.au/newsroom/news/2024/06/UNSW-Sydney-retains-Top-20-position-in-QS-World-University-Rankings

5 https://www.fairinstitute.org/what-is-fair

6 https://csrc.nist.gov/pubs/ir/8286/final

7 https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/widespread-outages-relating-crowdstrike-software-update

PARTNER CONTENT

Deakin’s global approach

Cyber security is no longer a niche concern – it is essential to global stability. With artificial intelligence, big data and digital transformation reshaping industries, organisations worldwide face an escalating battle against cyberthreats. Yet, the industry continues to experience a significant skills shortage^. How can we ensure the next generation of cyber security experts is prepared to tackle this evolving landscape?

By putting together a team of award-winning academics, industry professionals, and globally recognised multidisciplinary researchers, Deakin is tackling the challenges of the new digital landscape and ensuring its graduates are prepared for real-world threats. Deakin established one of Australia’s earliest dedicated cyber security master programs – the first to receive specialist cyber security accreditation from the Australian Computer Society. The program is also aligned with certifications from ISC2 and EC-Council, valued by professionals and employers around the world.

‘The cyber security landscape is rapidly changing. Our goal is to equip professionals with not just technical expertise, but also strategic thinking and leadership skills to tackle emerging threats,’ says Dr Adnan Anwar, Course Suite Director of Cyber Security at Deakin.

The cyber security sector is no longer confined to IT alone – it is integral to finance, health care, government and beyond. Deakin’s strong partnerships with industry, including its collaboration with the Australian Information Security Association, ensure its curriculum remains at the forefront of industry demands. The Deakin Cyber Research and Innovation Centre also brings cutting-edge research into the classroom – advancing cyber security technologies, shaping legal and strategic policies, and collaborating with industry, business, and government to tackle emerging threats and crime.

‘Industry alignment is key. Our students don’t just learn theory; they engage with real-world challenges through hands-on projects, internships and cutting-edge research,’ says Anwar.

Deakin’s specialised cyber security labs provide an immersive learning environment where students develop expertise in red and blue teaming, digital forensics, and advanced threat detection. Through work-integrated learning opportunities and industry placements, students gain exposure to real-life security challenges and hands-on experience in developing solutions before they graduate.

But cyber security is more than just technical expertise – it requires a global perspective. Deakin is expanding its impact through its international campuses in India and Indonesia, bringing world-class cyber security education to new markets. Deakin’s GIFT City Campus in India places students at the heart of a global financial and technology hub, where they engage with industry partners and gain invaluable real-world experience. This international presence reflects Deakin’s commitment to addressing cyber security challenges on a global scale.

With ICT security specialist roles projected to grow by 24.7 per cent in the next decade*, Deakin’s future-ready approach ensures that graduates are not just employable, but also indispensable. By integrating technical excellence with leadership skills and global insights, we’re shaping the cyber security leaders of tomorrow. ●

To find out more about Deakin’s Master of Cyber Security and how it can advance your career, visit www.deakin.edu.au/course/master-cyber-security-professional

^Occupation Shortage List, Jobs and Skills Australia.

*2024 Employment Projections – for the 10 years to 2034, Jobs and Skills Australia.

DEAKIN UNIVERSITY

Stay ahead in Cyber Security

Cyber threats are evolving – are you ready to tackle them?

The digital landscape is rapidly changing, and organisations worldwide are in urgent need of cyber security professionals who can stay ahead of emerging threats. Deakin's Master of Cyber Security (Professional) equips you with the technical expertise, strategic insight, and hands-on experience to tackle modern security challenges head-on.

Why study at Deakin?

- Awarded Australia's first ACS specialist accreditation in cyber security
- Aligned with global certifications from ISC2 and EC-Council
- Access to specialised cyber security labs for hands-on learning
- 100+ hours of industry placements and work-integrated learning
- Collaboration with AISA and leading industry partners
- #1 Victorian university for postgraduate teaching quality*
- Top 150 in the world for Computer Science and Engineering^
- Postgraduates earn more with a Deakin degree#

Step into one of the world's fastest-growing industries with the skills, confidence, and connections to lead in cyber security.

deakin.edu.au/course/master-cyber-security-professional

*2023 Student Experience Survey, Quality Indicators for Learning and Teaching.
^Shanghai Ranking's Ranking of Academic Subjects 2024.
#Graduate Outcomes Survey 2023, Quality Indicators for Learning and Teaching (QILT), based on Deakin domestic postgraduates' full-time median salary being the highest of all Victorian universities.
Deakin University CRICOS Provider Code: 00113B

Transforming cyber security's perception key to enhancing Australia's future cyber capabilities

BY JACQUI KERNOT, VICE PRESIDENT, CYBERSECURITY, THALES AUSTRALIA AND NEW ZEALAND

Australia is facing a significant shortfall in the number of cyber security professionals needed to defend people, governments and businesses.

Jacqui Kernot

With AustCyber forecasting a shortfall of almost 17,000 cyber security workers by 2026, current efforts by the conventional pathways of education and previous technical skills alone will fall well short of filling that gap.

Tackling the cyber security skills shortage requires multiple strategies that will attract new workers to the industry. These efforts must provide diverse entry points to attract workers and create pathways to make cyber security attractive, so that people from all backgrounds see cyber security as not just a lucrative career, but as one that offers rich experiences and job satisfaction.

Broadening the perception of cyber security careers

For many people, the image of a cyber security professional is taken straight from *The Matrix* with a figure – typically a male – in a darkened room hunched over a screen filled with computer code. And while technical roles are important in cyber security, the reality is that there is far more diversity in the types of roles that are needed.

Cyber security is not just about solving technical problems. A look at the modern threat landscape tells us that cyber security encompasses everything from psychology and human behaviour, through to education and strategic planning. While technical skills are important, not all cyber security roles are dependent on software engineering or hacking skills.

Overcoming the cyber security skills shortage requires an industry-wide rethink of how cyber security careers are portrayed. Today, cyber touches all aspects of life and business, and there are opportunities for specialities in engineering, legal and regulatory, auditing, teaching and communications, just to name a few.

The Australian Government's goal of becoming the most cyber-secure country in the world by the end of 2030 will not be achieved by only focusing on technical skills.

Embracing diversity and inclusion

Today's attackers come from many different cultural backgrounds. They are often highly educated and bring diverse experiences. According to research from RMIT, just 17 per cent of cyber security jobs are held by women. Yet, cybercrime affects every Australian regardless of gender or cultural background. The average cost of cybercrime for small businesses has risen by eight per cent to $49,600, as published by the Australian Signals Directorate's Cyber Threat Report.

The Australian Government's goal of becoming the world's most cyber-secure nation by 2030 will not be achieved unless we find ways to address the growing skills deficit. While the education system plays a significant role, there are more benefits to be reaped if we can explore the potential of full participation of Australia and New Zealand's workforce. Including return-to-work groups, re-skilling and cross-skilling. We can only breach the skills gap by bringing more people into the industry, and that is something every organisation in the sector can contribute to.

As cyberthreats increasingly target small businesses and individuals rather than just large organisations, it becomes our responsibility to attract and recruit individuals from non-traditional backgrounds. This diversity will enhance the integrated skill sets needed to tackle complex challenges.

Expanding the talent pool

With a limited number of cyber security graduates expected to finish their studies by 2026, it is evident that the education sector alone cannot fix the skills deficit. Attracting people from diverse backgrounds and other disciplines could make a significant impact.

It starts with how cyber security positions are advertised, acknowledging that people from different backgrounds may automatically exclude themselves from considering roles based on how they perceive a job description. Rather than solely emphasising technical expertise, job postings can highlight abilities like problem-solving, communication, teamwork, and a proactive attitude towards learning.

There are many examples of people who have successfully transitioned from non-related industries, leveraging their valuable skills to become exceptional cyber security professionals. These skills are often distinctive, essential to cultivate and frequently transferable to cyber positions. For instance, a nurse with experience managing an emergency department possesses the capability to thrive in high-pressure environments, effectively allocate and oversee resources through triage, and ensure the successful resolution of critical situations. These competencies are equally vital for roles such as cyber incident response management, where technical expertise is not the sole defining attribute.

Cyber security is an ever-changing industry, and the ability to find individuals who demonstrate strong interpersonal skills and a willingness to develop technical skills is valuable. It may seem risky to hire someone from outside the industry, but we will not grow the industry if organisations simply circulate from the existing pool of professionals among themselves.

The role of government and business in promoting diversity

Governments at all levels have an important leadership and advocacy role to play. It is now critical to seek talent suppliers who are committed to diversity targets and positive action.

Just as the tools, techniques and procedures used by attackers evolve, the skills and tools needed by cyber security professionals must keep pace. Short, intensive training courses and credentials can be delivered quickly by accredited private and public training providers who can use current industry experience with the agility required by both the learner and organisation.

We need the public and private education sectors, and vocational and higher education providers, to acknowledge that they have complementary parts to play in addressing the skills deficit that the cyber security industry faces.

Whether we are considering multi-year degrees, shorter programs or micro-credentials, it is essential to make these attractive to a broader cross-section of potential students. That means ensuring that educational programs use inclusive language, employ instructors from diverse backgrounds, and are designed with input from groups that are under-represented in cyber security.

There's an unexplored opportunity to establish programs targeting skilled immigrants who may need significant time for retraining or reaccreditation upon relocating to Australia to validate their career experience (e.g., lawyers, medical practitioners, accountants). Maximising our vast land to connect remote centres of work will encourage and boost numbers outside of our current business districts. Government programs could potentially provide further support for re-skilling opportunities, such as offering entry-level transitions into private organisations, who can then utilise their established resources for further upskilling. •

About the author

Jacqui Kernot *is one of Australia's most experienced cyber security and risk professionals, with a strong strategic understanding of the cyber sector. Her career spans nearly three decades across various verticals, including defence, space, intelligence, telecommunications, financial services and government in Australia, the United Kingdom and Europe.*

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/cyber-security

Become a leader in cyber security at RMIT University

Secure the future and lead the digital frontier.

In an era where cyberthreats are escalating in complexity and frequency, RMIT University's Master of Cyber Security program positions you at the forefront of digital defence. Designed for aspiring cyber security professionals, this program offers a comprehensive curriculum that blends technical expertise with strategic acumen, preparing graduates to protect and advance the digital infrastructures of tomorrow.

Why choose RMIT's Master of Cyber Security?

1. **Comprehensive curriculum:** RMIT's program provides a robust education that combines strong theoretical foundations with hands-on, practical experience. You'll delve into key areas, such as:
   — ethical hacking
   — digital forensics
   — cryptography
   — cyber security risk management
   — network security
   — software security
   — human factor security.
2. **Specialisation opportunities:** Tailor your learning through electives in threat analysis, cryptanalysis, security governance, risk management and compliance, or blockchain technologies
3. **Real-world experience:** Engage in realistic simulations and capstone projects that mirror the challenges faced by cyber security professionals. RMIT's strong industry connections allow you to work on projects that provide valuable, real-world experience, enhancing your job-readiness and employability.
4. **Industry engagement:** Benefit from RMIT's extensive network of industry partners. Through work-integrated learning experiences, you'll have the opportunity to apply what you learn in a professional setting, gaining insights and feedback from industry experts.
5. **State-of-the-art facilities:** Utilise cutting-edge cyber security software and simulated exercises to develop your skills. RMIT's facilities are designed to provide you with the tools and environment needed to excel in the field of cyber security.
6. **Global recognition:** RMIT University (ranked 123rd in the world by QS World University Rankings) is renowned for its high-quality education and research. Its Master of Cyber Security program is recognised globally, making you a competitive candidate in the international job market.

Program structure

The Master of Cyber Security is a two-year full-time or four-year part-time program. The curriculum includes 10 core subjects, covering essential topics such as software security, encryption standards, authentication mechanisms, and risk and controls mechanisms. The program also offers elective courses, allowing you to tailor your education to your specific interests and career goals.

Career opportunities

Graduates of the Master of Cyber Security will be well-prepared for a variety of roles in the cyber security field, including:
— penetration tester
— cyber security risk analyst/consultant
— cyber security consultant
— network security engineer/consultant
— secure software engineer or DevSecOps consultant
— digital forensics analyst
— security auditor.

With the increasing importance of cyber security across all industries, your expertise will be in high demand, ensuring a rewarding and impactful career.

Join RMIT University

Embark on a journey to become a leader in the fight against cyberthreats. With RMIT's Master of Cyber Security, you'll gain the skills and knowledge needed to protect critical digital assets and ensure the resilience of information infrastructures. Apply now and take the first step towards a secure and successful future. •

RMIT UNIVERSITY

Ready for what's next

Explore Cyber Security at RMIT

CRICOS: 00122A | RTO: 3046

Impact and influence

BY AJ KULATUNGA

Accelerating the CISO's path to the C-suite.

AJ Kulatunga

The world's top CISOs aren't recognised just for their technical skills and knowledge. They build high-performing teams, serve as trusted strategic advisers to the C-suite, and share their passion for cyber in a way that others want to lean in to learn more. But how exactly do they achieve this level of influence?

As a former technologist turned professional speaker, I have worked with senior leadership teams across seven countries to help them take bold action on big ideas. Accordingly, I have been fortunate to observe the elements involved in successfully impacting and influencing key decision-makers. These insights have been distilled into what I call the TLC Framework – a road map for cyber leaders looking to accelerate their journey to the C-suite.

T: Think to support others

There's this saying, 'If you're the smartest person in the room, you're in the wrong room.' I totally disagree. Often in our roles, we are the smartest people in the room on our subject matter. The critical question is, what are we doing with that knowledge?

Early in my technology career, I noticed a concerning pattern among several of my IT colleagues. They would look down upon anyone else within the organisation who lacked technical knowledge and came to them for help. This superiority complex is the quickest way to kill influence. No-one wants to be spoken down to and made to feel terrible because they lack anything. Great leadership is about identifying knowledge gaps, but also using your

expertise to elevate others and support them to fill those gaps.

Instead of asking 'How can I show I know more?', when cyber leaders ask themselves, 'How can my knowledge help others succeed?', the door to influence swings wide open. Your knowledge becomes a bridge, not a wall, and magical things happen.

Key insight: use what you know to help others shine, not to prove you are smarter.

L: Look like you belong at the table

Here's a hard truth that I learnt from the world of professional speaking: event managers don't necessarily book the best speakers; they book speakers who won't get them fired. Psychologists call this 'loss aversion theory'. Humans tend to prioritise avoiding loss over pursuing gains. I always believed that improving my skills and content would naturally lead to more speaking opportunities; however, in reality, I was being judged on how risky I seemed, not just my skills and talent.

This same idea applies directly to C-suite advancement. Beyond qualifications, achievements and accreditations, decision-makers evaluate whether you will fit cohesively within the existing leadership team. This 'fit' encompasses subtle signals that don't form part of the official criteria. They include things like: Does your speaking style match the pace and tone of the existing executives? Does your energy uplift a room or kill the buzz quickly? Do you make others feel comfortable and confident in your presence?

These people skills aren't just nice to have – they're core signals we humans use when deciding who we want in our inner circles. A common myth is that you have to be extroverted with a large personality to rise up through the ranks, but that's not true. It's more about making others feel that your presence enhances the team in everything that it does. The one caveat you have to keep in mind is that if your organisation's C-suite resembles a 'sea of sameness', breaking in may require additional work to establish trust and reduce perceived risk because the foundations of change simply aren't there yet.

Key insight: work towards being seen as a safe choice for a seat at the table.

C: Communicate – from others' perspectives

The last piece of the puzzle is mastering how to shift perspectives when you communicate. Most people communicate from their point of view of the world, while great leaders

communicate from the other person's perspective. Here is a personal story that I often share on stage that highlights this principle in action.

My father was an ex Army Officer in the Sri Lankan Army when the British ruled Sri Lanka. So, my childhood was essentially boot camp. Dad, like many Asian parents, believed academic excellence equated to life fulfilment. Unfortunately for me, I was anything but academic in school, and this was a major source of conflict between us.

I remember one time during a visit home from university, I accidentally got locked in my bedroom and broke the door handle trying to get out. Dad came running up and started yelling at me: 'Look at what you've done – you've broken the door, you useless fellow. Now I'll have to call Shantha Ayiah to come and fix it.'

I responded, 'Dad you don't need to call Shantha Ayiah, I can fix this myself!'

Immediately, he fired back, 'You? You studied IT! How can you fix something like this?'

In that moment, there was a million things that I could have said to my dad, but what came out of my mouth in that precise moment even surprised me: 'Okay, you don't believe I'm qualified to fix the door, how about I show you how to fix it, and you can fix it instead.'

'Ah okay, that makes sense.'

So we went to Bunnings, grabbed a new door handle, went back to the house, and I showed him how to fix it – and he fixed the door perfectly!

This approach worked brilliantly because it aligned with my father's self-image as a leader of men and a proud problem-solver. Instead of arguing with him from my point of view that he always looks down upon me, I tapped into that higher identity and used it to influence the situation into an outcome we both wanted.

Key insight: bring people along on the journey with you, but move people from where they're at, not where you're at.

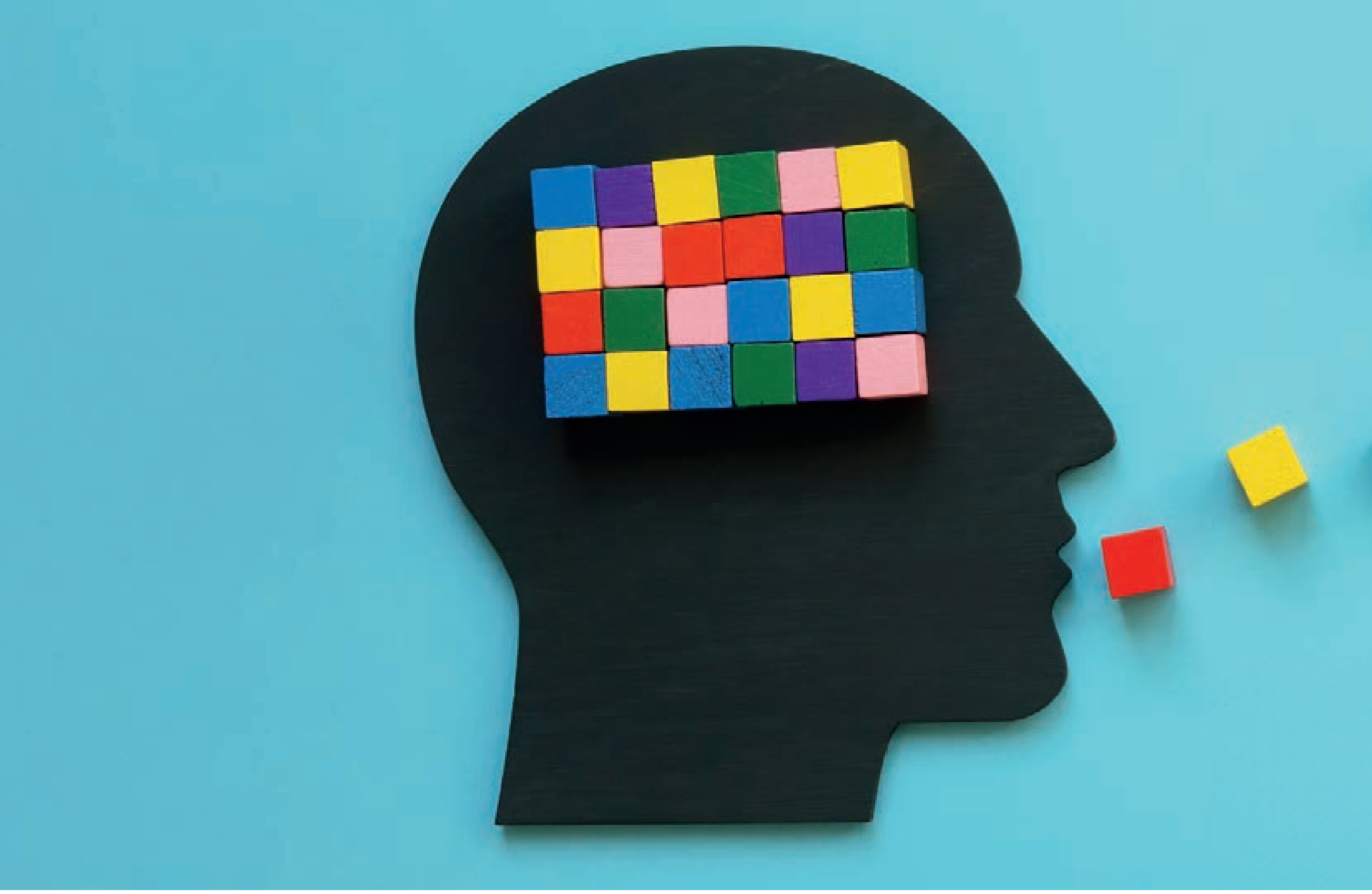
Starting your journey to influence

The path to increasing your impact begins with small, deliberate steps. Start by auditing your voice. Have a conversation with a colleague or a friend and ask them about your vocal tone: Is it high-pitched, low-pitched or balanced? Do you speak in a monotone voice or sing your words?

Last year, I spoke at the CISO Boot Camp, and the following day an attendee reported back that they had audited their voice and adjusted their vocal tonality during a team meeting. As a result, they were able to get their whole message across with more impact, which resulted in considerably higher engagement from the rest of the team. The philosophies I've shared will give you a bunch of little wins that, when stacked up, lead to bigger outcomes.

I'd like to leave you with one final thought: If you could have a phrase, quote or message on a billboard in the middle of Times Square where everyone would walk past and take note of whatever was on there, what would that message be? Once you have that message, remember that you are a living version of that billboard. Leverage the power of the TLC Framework to impact and influence your way to achieving what you want, and go make tomorrow better than today! •

About the author
AJ Kulatunga is a business strategist and global keynote speaker who impacts and influences senior leaders around the world to take big action on bold ideas. Follow his adventures on LinkedIn.



How to train your cyber Jedi

BY KYLE WATERS

The importance of mentoring in cyber security.

People often think that a mentor is a sort of teacher that takes on a single student and trains them to be their equal, or near enough, so they might be able to continue and train their own student.

This is not entirely incorrect, nor is it entirely accurate, either. The mentor–mentee relationship is one of mutual guidance and learning, empowers personal growth, and, in the case of many, professional development. This is possible because a mentor guides their mentee from a place of experience, hard-learnt lessons in their lives, and from their own mentor; however, it is not a one-way street, because a mentee guides their mentor, in turn, from a place of enthusiasm, openness to learn and contribute a fresh perspective, and mutual respect.

These relationships can not only have a profound impact on the individual mentor and mentee, or the industry they're in, but it can also also have a profound effect on the communities surrounding them, and in some cases, it can have a wider effect on civilisation itself.

One of the earliest examples of an impactful mentor–mentee relationship comes from ancient Greece, in the form of Socrates and Plato. Socrates (a well-known philosopher) was known for asking seemingly simple questions to get people thinking differently – not just considering what they thought about, but how they thought about them. And it wasn't just his pupils that he passed this knowledge onto, but, more specifically, his mentee, Plato, who went on to become one of the most well-known – and possibly the most influential – philosophers throughout history. Plato then went on to mentor Aristotle. It is in this continuing legacy of philosophical mentorship that has shaped a great deal of Western thought for centuries.

What this example teaches us is that by guiding others within our industry, we can improve things for everyone. If we choose to pass on what we know to others and guide them through their learning while we develop in our own, then many others can benefit – whether people in our own industry, people in other industries, or future generations that may not be aware of their mentor's mentor who passed on a specific lesson that they now rely upon.

So, how does this sort of relationship help us in cyber security?

Well, the answer to that is simple: knowledge acquired is just as valuable as knowledge earnt, but when both are brought together, cultivated and refined, then it becomes something incredible, and often the basis for understanding.

I have a mentor who has helped shape and guide my career in cyber security. This mentor–mentee relationship was not intentional – it was born out of mutual respect, friendship, varied life experience, a deep appreciation for the written word, a passion for education, and a mutual goal of helping our community through our industry.

Kyle Waters

This relationship has been invaluable to both parties. For my part, I have received guidance that mere education and experience alone was not able to provide – guidance of what path I wanted to follow in cyber security, guidance to find my voice and put myself out there within the industry, and guidance through writing articles, such as in this publication, but also through the delivery of presentations at conferences. As a result of this guidance, I am now sought after to deliver talks to local and international audiences, and, at the time of writing this, I am a finalist for a prestigious cyber security award.

All of this would not have been possible without my mentor's guiding hand, passing on relevant knowledge to me, helping me to recognise an opportunity and encouraging me to make the decision to pursue it, not giving me the answers to every question, but instead allowing me to discover the knowledge myself. More than this, he also seeks out and listens to the knowledge that I have, and values my input and insight when it comes to things that he could use a different perspective on.

Within our industry, I often see the massive gap between those with knowledge and experience, and those trying to gain them. Up until a few years ago, I was the latter. Since then, the most common question I am asked by students and others who are still looking is, 'How do I gain that knowledge and experience?' The reality of this is that there are two answers. The first is to take the long way around by getting official training and certification, attending conferences and workshops, networking within the cyber community like crazy, working in the cyber industry from the ground up until you are in demand, and learning every lesson along the way. The other still involves getting official training and certification, attending conferences and workshops, and, most importantly, finding a mentor to help guide your path.

I do not see myself as being at the level of full-time mentor yet, but when I was in my 20s, I was formally trained as a mentor though the Raise Foundation – a group that understands that kids can gain huge value out of the life lessons of adults who have either been in their shoes, or can help shine a light for them, guiding them through to the path of living up to their full potential.

So, for those who want to mentor, there are some key aspects and skills you must have before considering taking on a mentee. A mentee must:

— be a good listener/sounding board
— be adaptable
— value and contribute to perspectives other than your own
— be knowledgeable/informed
— be patient
— be constructive in feedback
— be honest, open and candid
— be willing to spend time developing others
— have an eagerness to learn as well as to teach.

The attributes/qualities of a good mentee are not too dissimilar. A mentee must:

— be a good listener/sounding board
— be adaptable
— be accepting of other's perspectives
— have humility and a willingness to learn
— be constructive in receiving and giving feedback
— have curiosity and openness
— be proactive when required, and patient when not
— have effective communication
— exhibit gratitude and respect
— be self-aware of limits, abilities, knowledge and the drive to improve on them.

If our industry is to thrive, we need to bridge the gaps by guiding the future cyber Jedis in their career paths. For those looking for their cyber mentors, keep searching, ask questions, get involved in conversations with people in the industry, and when (not *if*) you find your mentor, you will both prop each other up, adding the value and perspectives that the other needs, and become an integral part of each other's lives ... like my mentor and I. ●

About the author

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

SANS

Generative Artificial Intelligence (GenAI) and Machine Learning (ML) Courses Road Map

SANS Institute's engagement with GenAI and ML not only encompasses training and education but also extends to cutting-edge research, community building, and shaping industry standards.

GenAI/ML Technology-Focused Courses

SANS Institute develops specialised courses that equip professionals and organisations with the skills and knowledge needed to address AI-related complexities.

AIS247
AI Security Essentials for Business Leaders

AIS247 trains professionals to integrate AI into business safely and effectively, covering GenAI principles, applications, risks, ethics, and policy for responsible implementation.

SEC535
Offensive AI – Attack Tools and Techniques

SEC535 teaches AI for offensive purposes, covering security bypassing, exploit development, social engineering, automated attacks, and malware creation, with hands-on labs for practical application.

SEC595
Applied Data Science and AI/Machine Learning for Cybersecurity Professionals

SEC595 demystifies data science and machine learning with 70% hands-on problem-solving, focusing on practical AI/ML applications in cybersecurity and balancing theory with real-world solutions.

GenAI/ML Integration-Enhanced Courses

SANS incorporates GenAI/ML training across its broader cybersecurity education courses, equipping professionals with the necessary expertise to tackle AI-related complexities and effectively defend against sophisticated cyber threats.

CYBER DEFENSE

SEC497
Practical Open-Source Intelligence (OSINT)

SEC497 teaches cybersecurity professionals to use AI-enhanced techniques and tools for gathering and analyzing publicly available data for security intelligence and threat assessment.

SEC503
Network Monitoring and Threat Detection In-Depth

Delivers the technical knowledge, insight, and hands-on training you need to confidently defend your network

SEC587
Advanced Open-Source Intelligence (OSINT) Gathering and Analysis

SEC587 trains professionals to use GenAI/ML for OSINT, focusing on advanced techniques to analyze and validate data from various sources.

FORENSIC & INCIDENT RESPONSE

FOR518
Mac and iOS Forensic Analysis and Incident Response

FOR518 teaches professionals AI-enhanced forensic techniques for Apple devices, improving accuracy in artifact analysis and security incident identification.

FOR577
LINUX Incident Response and Threat Hunting

FOR577 uses AI to enhance forensic investigations on Linux systems, improving validation and streamlining processes for more effective security incident detection and response.

FOR585
Smartphone Forensic Analysis In-Depth

FOR585 trains cybersecurity professionals in advanced, AI-enhanced techniques for analyzing and extracting forensic data from smartphones, enhancing mobile security incident detection and investigation.

OFFENSIVE OPERATIONS

SEC504
Hacker Tools Techniques and Incident Handling

SEC504 trains cybersecurity professionals in identifying and responding to threats, using AI to enhance detection, analysis, and automated response capabilities.

SEC598
Security Automation for Offense Defense and Cloud

SEC598 trains professionals to use advanced AI and automation to enhance offensive and defensive cybersecurity strategies in cloud environments.

CYBERSECURITY LEADERSHIP

LDR512
Security Leadership Essentials for Managers

LDR512 trains leaders to manage cybersecurity defenses strategically, using AI insights to improve decision-making and security policy development.

LDR514
Security Strategic Planning, Policy, and Leadership

LDR514 trains cybersecurity leaders in advanced strategies and policy development, using AI-driven data analysis to improve security governance and decision-making.

To find out how SANS can help your organisation build AI-ready cyber teams, contact us at **anz@sans.org** for more information | **+61 2 6174 4581**