

2021-2022

CYBER AUSTRALIA



Australian Cyber Conference



AUSCERT

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S
PIONEER CYBER EMERGENCY
RESPONSE TEAM



Incident
Management



Phishing
Take-Down



Security
Bulletins



Security Incident
Notifications



Sensitive
Information Alert



Early Warning
SMS



Malicious
URL Feed



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

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

BECOME A MEMBER TODAY

+61 (0)7 3365 4417

MEMBERSHIP@AUSCERT.ORG.AU

AUSCERT.ORG.AU

FOREWORD

Alex Hoffmann,
Deputy Chairperson,
Australian Information
Security Association



The cyber security industry in Australia has experienced a tumultuous six months. As an industry, as organisations and as individuals, many of us have had to adapt our work practices while simultaneously enabling others to do so safely.

The coronavirus pandemic has shone a light on the inevitability of unpredictable change, the importance of resilience, our dependence on the supply chain,

and the reality that even a global pandemic will not slow or deter threat actors – quite the opposite.

As we're all acutely aware, 14 months on and this still rings true. It is especially the case for our members and partners in Victoria and New South Wales.

The Australian Information Security Association's (AISA's) volunteers and operations team have worked hard over this period to deliver meaningful content and value to our membership base under trying circumstances. The heart and soul of our association is in bringing people together to learn, network and socialise – something not easily done with the unpredictability that the pandemic has delivered.

As we look back, the restrictions in place in Melbourne in November last year were the catalyst for the creation of our first virtual conference through Risk and Cyber Week. With many of the learnings from this event, the teams have since coordinated to significantly increase our online webinars through the state-based branches and, of course, our cloud branch.

We were thrilled to have been able to move ahead with scaled in-person events in Perth, Brisbane and Adelaide throughout 2020 and 2021, and, of course, to have held CyberCon Canberra in March 2021. These

physical events were a reminder of just what we'd been missing elsewhere in the country, and what we have to look forward to.

The future for AISA is bright, and as increased vaccination rates lead to greater freedoms, so too does our mission and focus to get our cyber community back together (in person) as soon as possible. Beyond the CyberCon 2021 Virtual Edition this November, we're deep in planning for local and national scaled events alike. Dates have been set for our largest conferences in Canberra (March 2022) and Melbourne (October 2022).

With the ambitious plans we have to increase our events, we will be scaling our operations team to match them. A key first step is the appointment of Megan Spielvogel (AISA's current Operations Manager) to the newly created role of General Manager. In this role, Spielvogel will be expanding her operations team in due course. This is not just to cater for the planned upswing in events, but also to further evolve and shape programs that will drive additional member benefits and community engagement. We offer Spielvogel our sincere congratulations.

It can be argued that cyber security has never been more relevant, or more topical, than it is right at this moment. We're at an inflection point where cyber has truly transcended technical and risk audiences, and has become as relevant to board directors as it is to end users of technology – which is everyone. By extension, the mission and purpose of AISA have never been more relevant. Our recent submission to the federal government on strengthening Australia's cyber security regulations and incentives was shaped by a far-reaching survey of our 7500-strong membership base. The learnings from this survey not only serve to reflect the sentiment of our members in the submission, but will also be used to inform how AISA will continue to evolve and support those same members who contributed to it. •

CONTENTS

- 1 FOREWORD** ALEX HOFFMANN
- 6 SECURE CONNECTIONS: PARTNERSHIPS PROMOTING DIGITAL SAFETY**
- 8 SECURING YOUR SOFTWARE SUPPLY CHAIN**
- 10 THE SHAPING OF CYBER IN THE POST-SEPTEMBER 11 WORLD** DR LESLEY SEEBECK
- 14 ADDRESSING CYBER VULNERABILITIES IN AUSTRALIA'S SUPPLY CHAINS**
- 16 WORKING TOGETHER TO FIGHT CYBERCRIME** AMANDA-JANE TURNER
- 18 DEAKIN UNIVERSITY CURBS SECURITY RISKS OF CURIOUS STUDENTS**
- 20 RANSOMWARE IS ONLY PART OF THE SECURITY CONVERSATION**
- 22 SECURITY AUTOMATION: A NUMBERS GAME** DAVID BRAUE
- 26 FROM CYBERTHREAT TO CYBERWARFARE** SIMON GALBALLY
- 30 AVOID THE FALSE PROPHETS OF CYBER**
- 32 LEGAL HACKING – WHY NOT?** PROFESSOR BRIAN MARTIN
- 34 CYBER CLOAKING**
- 36 LIFE AS AN ETHICAL HACKER** CRAIG FORD
- 42 THINK YOU'LL NEVER FALL FOR A BUSINESS EMAIL COMPROMISE SCAM?** DAVID BRAUE
- 44 ANALYSING AUSTRALIA'S RESPONSE TO MICROSOFT EXCHANGE VULNERABILITIES** EDWARD FARRELL
- 46 RANSOMWARE – REPORTING, PAYMENTS AND THE OTHER 98 PER CENT OF BUSINESSES**
- 48 CYBER SECURITY MATURITY: AUSTRALIAN BUSINESS GETS A PASS MARK, BUT CAN DO BETTER** CRAIG BATY
- 52 DEFENDING AGAINST THE RANSOMWARE EXPLOSION**
- 54 YOU'RE ONLY AS SECURE AS YOUR SOFTWARE SUPPLY CHAIN** DAVID BRAUE
- 58 TESSERENT: A HOMEGROWN SUCCESS STORY**
- 60 FROM SECURITY-ENHANCED 5G NETWORKS TO SECURITY-BY-DESIGN 6G SYSTEMS** DR DAVID SOLDANI
- 64 THE INTERNET OF THINGS – ARE WE PREPARED FOR IT?** MANDI JACOBSON AND ANGELL ZHANG
- 67 IN A DIGITAL WORLD, DISRUPTION IS ONLY A DDOS AWAY** DAVID BRAUE
- 70 EMPOWER YOUR ORGANISATION TO SAFEGUARD INFORMATION TO ENSURE INFORMATION RESILIENCE**
- 72 ARTIFICIAL INTELLIGENCE FOR CYBER SECURITY: NEW SOLUTIONS, BUT ALSO NEW RISKS** DR CHRIS EWIN
- 74 APPLYING RISK APPETITE TO YOUR CROWN JEWELS** DENNY WAN AND MICHAEL COLLINS
- 79 API ON WHEELS: A ROAD TRIP OF RISKY VULNERABILITIES** PIETER DANHIEUX
- 82 SCHOLARSHIP OPENING DOORS TO CYBER INDUSTRY**
- 84 UNIVERSITIES MUST STAND FIRM ON CYBER** DAVID BRAUE
- 90 THE NEW ERA OF CYBER SECURITY**

- 94 AUSTRALIA'S CYBER SECURITY SKILLS SHORTAGE VS LOWEST UNEMPLOYMENT RATE** MINA ZAKI
- 98 IS THERE REALLY A SKILLS CRISIS IN THE CYBER SECURITY SECTOR?** DAMIEN MANUEL
- 104 USING THREAT INTELLIGENCE IN YOUR DEFENCE STRATEGY**
- 106 MAKING TRAINING WORK IS HARD – BUT LETTING IT FAIL IS EVEN WORSE** DAVID BRAUE
- 110 DO YOUR LEGAL ADVISERS PRACTISE CYBER SECURITY THE WAY THEY SHOULD?** DAVID BRAUE
- 112 LEADING CYBER SECURITY FROM THE TOP: THE NEXT CHALLENGE FOR BOARDS**
- 114 CONSULTING GIANTS** DAVID BRAUE
- 118 SECURE YOUR FUTURE WITH CYBER SECURITY AT UQ**
- 120 RANSOMWARE GANGS HAVE BUSINESSES ON THE ROPES** DAVID BRAUE
- 126 SIX PRINCIPLES FOR BOARDS ON CYBER RISK GOVERNANCE** SHELLEY DEMPSEY
- 130 THE DIGITAL GOD PROBLEM**
- 132 PREPARING FOR 'CYBER MAYDAY AND THE DAY AFTER'** SHAMANE TAN
- 136 CONNECTED CITIES: A CYBERCRIMINAL'S PLAYGROUND** DAVID BRAUE
- 140 SOURCE CODE SECURITY** DAVID BRAUE
- 144 THE FUTURE OF CLOUD SECURITY**

PUBLISHED BY:



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

ABN 30 007 224 204

PO Box 256
North Melbourne VIC 3051

Tel: 03 9274 4200

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

PUBLISHER

David Haratsis
david.haratsis@executivemedia.com.au

MANAGING EDITOR

Giulia Heppell
giulia.heppell@executivemedia.com.au

JOURNALIST

David Braue

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

EDITORIAL AND DESIGN TEAM

Kate Hutcheson, Eden Cox, Abby Schmidt

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

© 2021 Executive Media Pty Ltd. All rights reserved. Reproduction in whole or part without written permission is strictly prohibited.

All stock images sourced from iStock.com

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

Deakin University

a partner you can trust
in a cyber-world



Today's world of e-commerce, cloud services, virtual collaboration and instant communication has transformed the way we work. COVID-19 has accelerated digital technology adoption even more – allowing businesses to pivot and adapt. But it has introduced new risks to be managed.

Businesses are turning to Deakin University for our unique cyber-ecosystem that provides the full spectrum of education, research and translation across all relevant disciplines, such as network security, artificial intelligence, transport and logistics, energy, business, law, regulation, policy and human behaviour. Deakin offers:

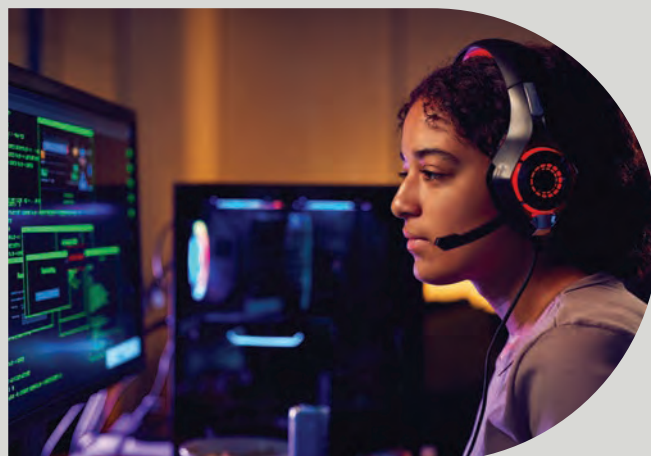
- A pool of industry-ready talent through internships and work placements.
- Partnering to develop innovative services and products.
- Data analytics and assessments to gain deeper insights into markets and information.
- Automation through AI-enabled systems to increase productivity and reliability.
- Retraining and upskilling of staff to adapt to new challenges.
- Research focused on reducing business risk, optimising business processes and developing new technologies.

Deakin has provided cyber security education and research since 2003 and is among the world's top 100 universities for Computer Science and Engineering (2021 ARWU).

Our cyber-ecosystem includes the Centre for Cyber Security Research and Innovation (CSRI); CyRise –the Southern Hemisphere's only dedicated cyber security accelerator; the Institute for Intelligent Systems Research and Innovation (IISRI); Deakin Energy; the Applied Artificial Intelligence Institute (A²I²); and the Digital Innovation for SMEs Hub (The DISH).

Our business partners include NAB, NTT, CyberCX, PwC, Deloitte and Netskope, through to global automotive companies, defence and government agencies.

The only way to tackle the cyber security challenges of today is through a holistic approach. By leveraging the capacity of a trusted research partner, together we can make a difference to protect Australians.





'Deakin is researching in the cyber security space in innovative ways, providing skills to the industry as well as building a pipeline of terrific talent for the future.'

John Karabin

Director of Cybersecurity
NTT Australia Ltd.



'Having Deakin as a partner for CyRise has been a tremendously powerful addition to our program. Deakin's depth of capability in cyber security research and its knowledge of the market has been a huge asset as we try and help our portfolio of companies grow globally. Whether as mentors, connectors, funders or co-innovators, Deakin has been there for us from day one.'

Scott Handsaker

CEO
CyRise



Find out more:
cybercentre.org.au





Secure connections: partnerships promoting digital safety

BY DAMIEN MANUEL, DIRECTOR CYBER SECURITY RESEARCH AND INNOVATION (CSRI), AND PROFESSOR ROBIN DOSS, RESEARCH DIRECTOR CSRI, DEAKIN UNIVERSITY

THE FUTURE OF digital technology and artificial intelligence (AI) is brimming with exciting potential, both for doing business and enjoying our leisure time. Streamlined ecommerce, cloud-based services, smart devices and autonomous systems are already here, and more are on the horizon.

The COVID-19 pandemic has forced businesses to transform digitally, rapidly pivoting to survive. Virtual innovation has risen to the challenge by finding new ways of connecting us while we are physically apart.

Yet, broad uptake of increasingly sophisticated technology has introduced new risks. The more connected we become, the greater our threat surface. Unfortunately, there are more nefarious actors now than ever before.

Keeping critical infrastructure safe in this connected environment requires expertise and consistent

monitoring for emerging threats. The cost of first-class cyber security is often beyond the reach of small to medium-sized enterprises (SMEs).

It makes sense, then, to engage a trusted partner for SME cyber security needs. Deakin University has been at the forefront of that model, providing cyber security education and research since 2003.

Deakin's success has involved building a cyber ecosystem encompassing many points on the value chain, with expertise from the Centre for Cyber Security Research and Innovation (CSRI); CyRise, the Southern Hemisphere's only dedicated cyber security accelerator; the Institute for Intelligent Systems Research and Innovation (IISRI); Deakin Energy; School of IT; the Applied Artificial Intelligence Institute (A2I2); and the Digital Innovation for SMEs Hub (the DISH).

ADVANCING DIGITAL INNOVATION POST COVID-19

Officially launched in August 2021, the DISH offers Victorian SMEs business health checks to improve efficiency, funding and cash flow. Conducted by Deakin's Faculty of Business and Law, CSRI, A2I2 and partner organisations, the health checks will encourage new product opportunities and potential new markets.

To facilitate this, SMEs will be able to leverage world-leading research expertise from Deakin's innovation centres, such as CSRI and A2I2. The DISH provides access to a pool of industry-ready talent to give businesses a competitive edge. Bootcamps, innovation workshops and rapid hackathons embedded in the program will help businesses to embrace digital technology, and become more cyber resilient in a post-COVID-19 world.

DRIVING CYBER SAFETY FOR HUMAN SAFETY

Our vehicles of the future will take the form of complex mobile computers, designed to be automated and connected. But this raises two key questions for community safety: how secure will the systems and electronics of these vehicles be; and can we trust decisions made by the onboard AIs?

Fully trusting AI models in safety-critical applications like driving can lead to catastrophe if the models do not know their limits. Deakin's IISRI has developed systems to gauge AI confidence when making decisions, including predictive uncertainty estimates during inference time. Uncertainties are applied when screening predictions and potentially erroneous cases are treated with extra caution; for example, reducing speed and driver notifications in autonomous vehicles, mitigating the risk of disaster.

Advanced onboard instrumentation exposes drivers to threats from hackers and malware. World-leading cyber security researchers from Deakin's CSRI are working with industry partners to ensure next-generation vehicles are cyber-safe and can network securely.

The resilience of future automotive systems relies on more than robust components. Projects at IISRI and CSRI contribute to understanding the security and privacy of connected vehicles, and advanced, state-of-the-art systems to ensure safety.



ACCELERATING CYBER STARTUPS TO FUTURE-PROOF INDUSTRY

Cyber attacks cost the world trillions of dollars annually and cause devastating damage to businesses. Hence, cyber security professionals are in high demand. The challenge is meeting this demand with a pipeline between professionals and specialist companies, building Australia's capacity and talent pool in cyber security.

This is where universities like Deakin and its partners provide cyber security excellence.

CyRise, a partnership between Deakin and global IT company NNT Ltd Australia, is leading the future of cyber security innovation by creating an ecosystem for promising startups.

This includes:

- a selective 14-week program exposing startups to international best practice, industry mentors, investors and customers

- graduating over 27 high-quality companies with global potential from the program since its inception in 2017
- raising additional capital by 63 per cent on graduation, a world-standard result.

The CyRise startups have been increasingly successful, including SecureStack, named one of 20 cyber security startups to watch by *Forbes*. Supporting developers and security teams, SecureStack analyses source code, cloud stacks and attack surface to find gaps. Its CI/CD provides ongoing insight to protect global companies.

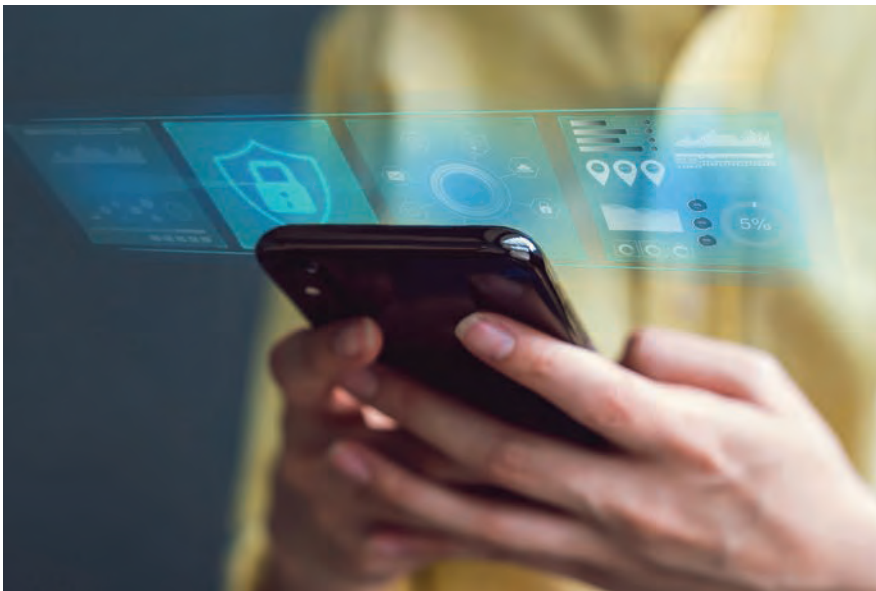
Other successful startups include badook, the first test automation solution designed to maintain data integrity; and Devicie, which raised \$1.3 million to support human-centric device management.

THE SECURITY TO PROSPER

The need for cyber security is self-evident, but it's also vital for the economy and jobs growth. Investing in Australian cyber security capacity can play a part in creating crucial, high-value jobs.

At Deakin, we're taking a holistic approach to today's cyber security challenges, with an eye on the prosperity of tomorrow. The skills and capabilities of our trusted research partners augment our world-leading multidisciplinary experts in cyber security, AI, transport and logistics, energy, and business.

From a deep capability in cyber security research and market knowledge, Deakin is supporting companies to grow globally and keep us all safe. •



Securing your software supply chain

BY KEN MIZOTA, PLATFORM STRATEGY DIRECTOR, RAPID7

How to safely leverage software to drive innovation.

WOULD YOU CONSIDER leaving your house unlocked all the time? It might save you a lot of time if your grocery delivery person can let themselves in to restock your fridge, or so your plumber can fix your boiler.

Yet, you don't know who else might walk in, or what they might take when they leave. And that's a little like the problem organisations have with software supply chains.

The demand for rapid innovation means organisations are employing open-source and third-party software more than ever. Software supply chains can be complicated. They consist of multiple elements: software vendors, service partners and providers, in-house developers, and open-source software libraries. This complexity creates vulnerabilities.

Attackers are taking advantage to launch devastating software supply chain attacks, such as Equifax, SolarWinds, Codecov and, most recently, the Microsoft Exchange breach.

Traditional supply chain exploits, such as the Apache Struts incident at Equifax, target publicly disclosed open-source vulnerabilities left unpatched in the wild. Next-generation software supply chain attacks are far more sinister. Bad actors take the initiative and inject malicious code into open-source projects feeding the global supply chain.

So, what can be done?

PREVENTION

Organisations rarely control their entire software supply chain. Instead, your cyber supply chain risk management strategy should

include steps to create an inventory and monitor your third-party tools. Document how each software licence is supported by its supplier, and learn about vulnerabilities and disclosed breaches. As a software consumer, perform integrity checks for executable code. As a software supplier, consider implementing controls such as egress filtering, IP address safelisting and automated credential rotation to reduce avoidable risk.

DETECTION

Prevention controls alone will never be 100 per cent effective. Multiple layers of detection controls are essential for catching suspicious or malicious activity. Monitor third parties with access to your systems, such as suppliers, and identify dependencies to help you create detection rules that trigger investigations. Process execution, authentication, activity and network logs are common sources to monitor. When looking for suspicious activity, keep an eye out for ingress from, and egress to, unusual IP addresses or regions.

RESPONSE

A good incident response plan is the same for supply chain attacks as it is for any other attack. Scope the extent of the breach, the affected parts of the business and what data has been lost or compromised.

Deploy containment protocols, such as disconnecting and quarantining affected devices, updating security protocols, and deploying patches. Begin your remediation reporting and recovery processes.

Supply chain vulnerabilities are a real threat for organisations of all sizes; however, a security program with sound risk management, prevention, detection and response capabilities can mitigate, reduce or even avoid the impact of supply chain incidents. ●



For more information, visit
www.rapid7.com/c/apac-supply-chain/



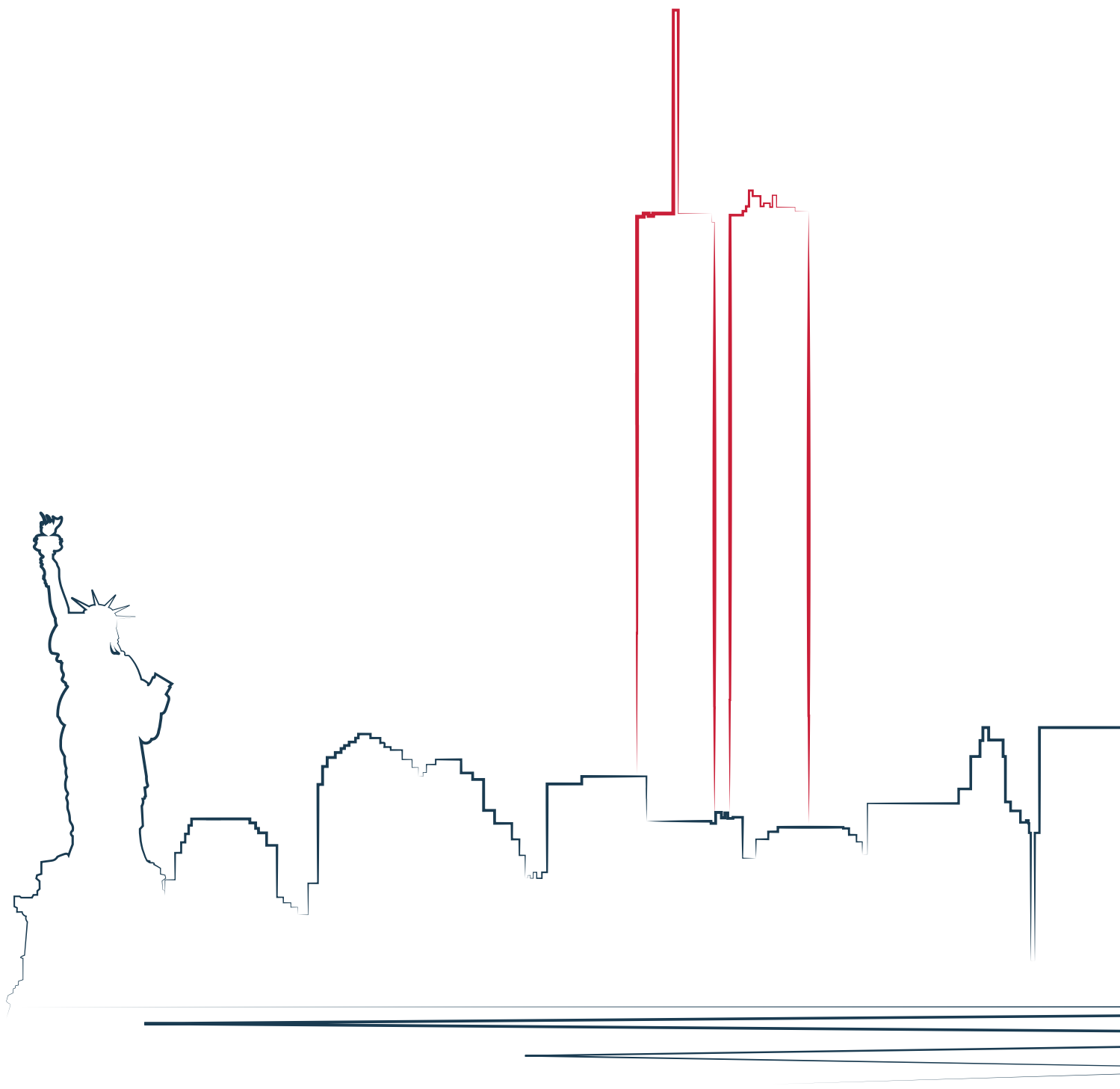
Security that advances with you

Innovate without slowing down. Get the visibility, analytics, automation, and expert guidance you need to securely advance.

Learn how we can help:

Visit us at www.rapid7.com
or email us at anzsales@rapid7.com

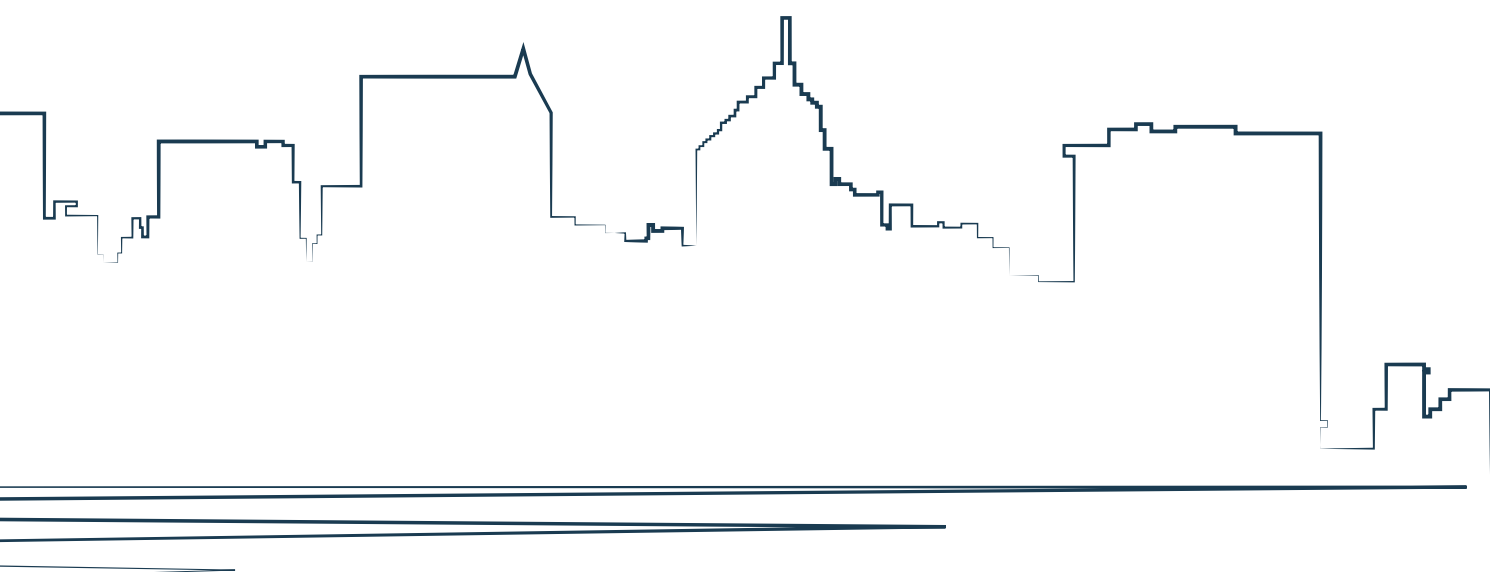
RAPID7



The shaping of cyber in the post-September 11 world

— BY DR LESLEY SEEBECK, HONORARY PROFESSOR,
AUSTRALIAN NATIONAL UNIVERSITY, AND CEO, CYBER2 —

Twenty years after the September 11 attacks, the problems posed by the cyber world seem to pale beside the death and destruction experienced that day. September 11 was proof that one did not need high levels of technological sophistication to wreak havoc and damage a nation's psyche.





Dr Lesley Seebeck

It's easy to forget that the notion of cyberwar was prevalent in the imagination of Western governments before September 11. Much of that stemmed from the assumption that technology would be involved in any threat to US and Western security during what was termed 'the unipolar moment'.

The focus on cyber built on ideas emerging from the revolution in military affairs (RMA) and the importance of information superiority during the first Gulf War. In military strategy, there is always a tendency to look for known adversaries in familiar forms, and it was easier to worry about an enemy that fought in ways that undermined Western information dominance than one that was aberrant.

September 11, and policy responses to it, however, have fundamentally shaped our understanding of security, including cyber security, even in countries physically distant from those events and the subsequent military campaigns in Iraq and Afghanistan.

There are similarities between the attacks on the World Trade Centre and the Pentagon and cyber security. In both cases, the attacks are comparatively low-budget; just a few perpetrators can have an extraordinary effect. The costs of failure for the defenders can be high, but is typically low for attackers. Attackers and facilitators can be used as proxies, though nation-state adversaries – such as China, North Korea, Russia and Iran – while finding deniability useful, are more intent on building their own intrinsic capability.

The policy responses by governments to September 11 echo those in cyber, particularly the breadth of perceived threat and a lessening of trust in systems and people.

The policy responses by governments to September 11 echo those in cyber, particularly the breadth of perceived threat and a lessening of trust in systems and people

During the early years post September 11, policymakers sought new conceptual frameworks for understanding and managing the real and present danger posed by terrorists. Borrowed from disaster management, the all-hazards approach held considerable appeal. It holds that regardless of the nature of disaster, there are common elements to preparedness, reaction and response: for example, people may need to be evacuated, physical assets secured, medical teams deployed and victims triaged, and communications assured.

From a practical planning perspective, it's logical to extend such an approach to human-made disasters. More problematically, however, is that the all-hazards approach was stretched to encompass policy; quite literally, policy responses had to encompass all hazards.

While that expansion fit with the broadening ambit of national security, which was supercharged after September 11, it did little to help policymakers prioritise limited resources or design sustainable systems. To paraphrase Helen and Dash from *The Incredibles*, when every hazard is special, no hazard is. But it elevated security to the primary, defining role of government. To gain traction in policy contests, advocates often looked for security rationales to help win arguments and funding.

Over time, the all-hazards approach, which focused on preparation and response, evolved to one of protection. The expectation, argued David Omand, was that the state would manage risks to the safety of the citizen, such that normal life could continue. The reality of prioritisation and expectation of action has led governments to focus more on what they can control – their own societies – than the much harder inequalities, conditions and incentives that encourage and empower threat actors, such as terrorists, dark web criminal organisations and adversarial hackers.

Those trends have been reinforced by the insider threat – notably Edward Snowden – and lone wolf attackers. To governments, people have become material threats to safety, peace and stability. In democracies, the apparent distrust of people has been mirrored by eroding public trust in institutions, often magnified by social media.

To cyber professionals, these trends are familiar. Cyber security itself evolved from a much more narrowly defined concept based on information security. While the calculus of prioritisation of resources in organisations is typically more business focused – cyber security rarely trumps other priorities except in extremis – there remains the expectation of meeting a spectrum of threats, many unanticipated.

The idea that people, particularly users, are the problem is not uncommon in IT departments – after all, if people only did as they were expected, systems would work properly and engineers would have fewer problems. Cyber professionals, however, are conscious that such a premise is short-sighted and overlooks systemic risk. Simply placing blame on users, or preventing them from getting their jobs done or meeting operational needs, is doomed to fail, and will be followed quickly by the appointment of a new chief information security officer (CISO).

Given that CISOs are often on the front lines of threats, facing constant attack by disparate adversaries with initiative and incentive, there are lessons that they could take back to policymakers. These include the importance



of culture and trust within organisations, between organisations and their stakeholders, and between governments and citizens. After all, a hard-won lesson is that cyber security is indeed a team sport, needing the support of technologists, operations, business functions, users, leadership and external stakeholders.

Cyber security – often described as an art or a practice – requires constant evolution and adaptation. It is not easily reduced to the abstractions of rigid legal code, which is often the tool most readily available to the hand of governments. As the world of cyber security is shaped by decisions made outside the organisation, by the technology choices of others, and by habit and practice, it has much to teach policymakers about resilience.

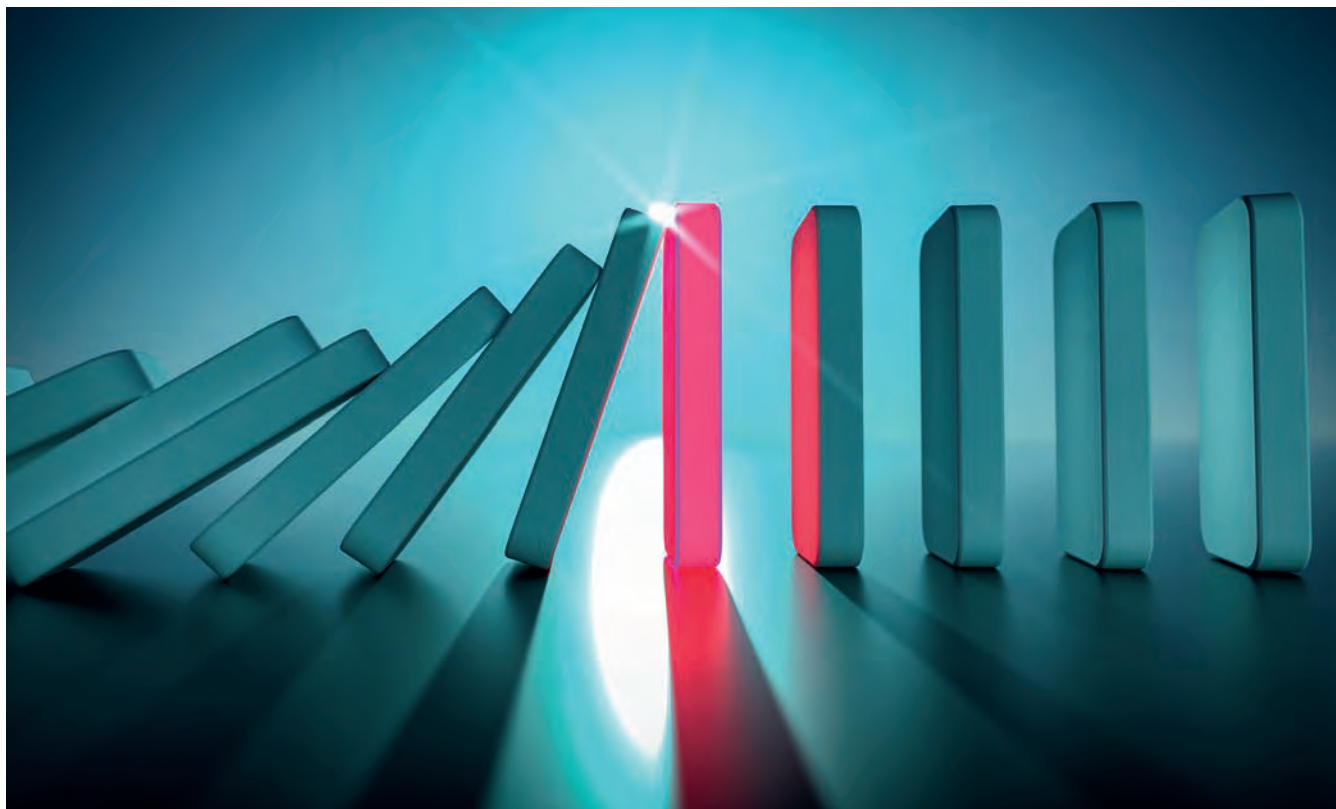
Last, cyber specialists are more aware than most of the dangers inherent in the surveillance state: data is easy to collect and difficult to secure; people are fallible; and technologies offer, at best, fleeting assurance. The tools and ammunition available to repressive regimes, organisations and partners, even simply to inhibit expression, far outweigh the defences not just of states, but especially of individuals. The future of cyber security

needs to be shaped by more than a response to threats: it must work actively to protect and uphold the freedoms intrinsic to our society. ●

.....
AISA member and former CEO of the Cyber Institute, Australian National University, Dr Lesley Seebeck has held senior executive roles in the federal government as Chief Investment Officer at the Digital Transformation Agency, as Chief Information Officer at the Bureau of Meteorology, and in the Department of Finance.

Dr Seebeck has extensive experience in strategy, policy, management, budget, information technology and research roles in the Australian public services industry and academia. She has worked in the Departments of Finance and Defence, and the Prime Minister and Cabinet, the Office of National Assessments, and as an IT and management consultant in private industry and at two universities. She served on the government's Naval Shipbuilding Advisory Board from 2019 to 2020. In March 2017, she was recognised as Federal Government CIO of the Year.

Dr Seebeck has a PhD in information technology, an MBA, a Master of Defence Studies, and a Bachelor of Applied Science (Physics).



Addressing cyber vulnerabilities in Australia's supply chains

DURING WORLD WAR II, United States Air Force bombing crews were ordered to destroy ball bearing plants in Schweinfurt, Germany. Ball bearings are a critical component in the production of war machinery. Just a few bombing runs on ball bearing plants in Schweinfurt reduced German war-machine production by 38 per cent. The attack on an enemy's supply chain had a compounding effect that was much greater than the initial impact.

The concept of a supply chain attack is simple. The first step is to figure out all the components used to manufacture a mechanical device and trace those components, skilled resources, raw materials, transport and other logistics involved all the way back to their origin. A disruption at any point in this chain of relationships and interdependencies has the potential to halt production.

Malicious cyber actors are aware that attacks against supply chains are highly effective and profitable. Ransomware of any organisation along a supply chain applies pressure

to the victim to pay, compounded by upstream and downstream partners waiting for the business to resume normal operations.

Not only do cybercriminals lock up computer networks to stop production, but they also sell confidential stolen data to competitors and profit at both ends. These attacks already extend into the Internet of Things, satellite, medical and critical infrastructure networks. Imagine the impact of locking down a mining company's production facilities, ransoming a satellite before a \$500-million pay-per-view boxing match, or locking a power company out of its own smart meters. These threats are not science fiction; many have already occurred, and more will follow.

State-based cyber actors work against Australian interests by compromising critical infrastructure, military, commercial and academic networks to further their own economic, political and military goals. Why go to this effort? To create 'cyber-shu', as the Chinese put it – building potential power that can be

unleashed on the battlefield at a time of their choosing.

In 1943, the Nazis assessed the impact of ball bearing factory destruction and reacted wisely. They distributed manufacturing to multiple domestic locations that could be better defended, sought multiple suppliers for raw resources and stockpiled components in anticipation of future disruptions.

Work by the Australian Cyber Security Centre continues to teach critical infrastructure and small businesses alike that they need to defend themselves better, collaborate on defensive measures, and plan ahead for cyber intrusions. Collaboration is also key in the security industry, amplifying these messages through education, threat intelligence dissemination and security controls that leverage collective defence efforts. These philosophies underpin Cybermerc's continued efforts as the company continues its mission to build a collective defence across Australian networks through the AUSHIELD program. •



CYBERMERC

Let's defend our digital borders together.



AUSHIELD DEFEND

Australian owned and operated

Australian-specific Cyber Threat Intelligence

Collaborative Analyst Workbench

Integrated Training and Mentoring of Analysts

Accessible to Small Business and Enterprise

Over 130 Intelligence Feeds

All data hosted in Australia

JOIN



AUSTRALIA'S NATIONAL THREAT SHARING PLATFORM

cybermerc.com

twitter.com/CybermercCom

linkedin.com/company/cybermerc

WORKING TOGETHER TO FIGHT CYBERCRIME

— BY AMANDA-JANE TURNER —

The more interconnected and advanced technology becomes, the greater the risk of cybercrime.

We live in an amazing time – one in which advances in technology and communication allow us to meet with colleagues virtually, see inside museums and art galleries in countries we may never visit, and keep in touch with friends and family from all over the world. We have smart cities, watches that can receive emails, and cars that can diagnose their own mechanical faults. There is technology to help deaf people to hear and help hearts to beat properly, and robotics to assist in surgery.

Think about your daily life outside of work: how much of it involves some type of technology? In the developed world, even those who do not own a computer or smartphone have some exposure to technology. Unfortunately, the more interconnected and advanced technology becomes, the greater the opportunities for cybercriminals.

In Australia, ‘cybercrime’ refers to both crimes directed at information communication technologies and crimes where information technology is an integral part of the offence. This means that cybercrime is as diverse as the technology used to perpetrate it. It includes malware, romance fraud, advanced fee scams, tech support or refund scams, phishing campaigns, ransomware, identity theft, online predators, grooming of underaged persons, and child abuse material. Fighting cybercrime is a massive undertaking, and cyber security professionals, law enforcement and intelligence agencies cannot do it alone.

Collaboration is key to successfully fighting cybercrime. Whether it is public and private sector agencies sharing relevant, timely, actionable intelligence; educators ensuring their students understand privacy and safe online practices; or individuals applying appropriate online safeguards, we all have a part to play in making our world more cyber safe. The more we work together to detect, deter or prevent a cybercrime, the harder we make it for criminals to succeed.

It is important that all users of technology understand the basics of how to keep themselves safer in the digital

world, understand the threats and work together to fight cybercrime. You do not have to be a computer expert to play a part in helping yourself and your community to stay safer from cybercrime. Individuals who own and use computers should consider, at the bare minimum, applying the basics of cyber security, such as using reputable, up-to-date antivirus software; applying security update patches to software; keeping important data backed up on removable offline media; having strong, unique passwords; and using multi-factor authentication where possible.

It is important that we all collaborate and do what is within our means to educate others about safe online practices, such as how to secure privacy settings on social media, the dangers of oversharing on social platforms and being cautious about unsolicited messages. Understanding how and where to report cybercrime, online bullying, and online child safety issues is also paramount in collaborating as a society to fight cybercrime. It is acknowledged that not all victims of cybercrime will have the outcome they want, as investigation, attribution and arrests are challenging in the multi-jurisdictional, easy-to-hide world of cybercrime; however, notifying appropriate authorities of cybercrime, and sharing information with other relevant bodies may also help others be forewarned of similar malicious campaigns and support cybercrime intelligence-gathering efforts.

Sharing information on cybercrime to help form intelligence or raise awareness is a way we can all work together to fight cybercrime. Public agencies such as the not-for-profit organisation AusCERT and the Australian Government’s Australian Cyber Security Centre (ACSC), for example, provide resources for businesses and individuals to help them stay safe from cybercrime. As individuals, we also have the power to support cybercrime-fighting efforts by sharing relevant information about cybercrime and cyber security on social media, at our places of work,



and with our family and friends. The messaging about cyber safety, cyber security and cybercrime needs to be ongoing, via a variety of mediums and from people of all walks of life, and to become part of everyday life. Applying cyber security practices should become as natural as locking our doors before we leave the house, or looking both ways before we cross the street. Every little bit done in a collaborative effort to enhance our cyber security posture as individuals or businesses makes it that little bit harder for criminals to succeed.

As we work together to help prevent cybercrime, let's also work together to change the stereotypes that only non-technical, older people; the desperate; or the greedy are impacted by cybercrime. Nobody is immune from cybercrime; anyone can be scammed, have their devices infected with malware, have their children harmed by online predatory behaviour, or have their credentials or identity stolen. Collaborating against cybercrime also includes changing the victim blaming narrative. Victims of cybercrime are not to blame – the criminals are. So, as a community, let's support the victims, learn from their experiences and collaborate to help prevent similar incidents in the future. Cybercrime is big business, and it's not going

away anytime soon. This is why it is crucial that we collaborate, stay vigilant, share knowledge and support others to stay safe from cybercrime.

Increased interconnectivity and constant technological development provide an increased opportunity for criminals. Fighting cybercrime is a huge job, and we all need to work together to the best of our abilities to help harden our communities, nations and the world against cybercrime. Fighting cybercrime in silos will never get us ahead of the criminals. We are all stronger together, so let's all actively work together to fight cybercrime. To achieve a world that is aware of, and resilient against, cybercrime, we all need to keep working together. •

Amanda-Jane Turner is a cybercrime specialist with an interest in the mechanisms and mitigation of cybercrime. She is a firm believer that diversity in all its forms should be encouraged to promote innovation and find solutions to challenges facing the world. She has won multiple InfoSec industry awards, and in 2019 she was in the first cohort to be named a Fellow of AISA. Turner presents on cybercrime at cyber security conferences and writes books on the subject, and is the founder of the Demystify Cyber project to help people stay safe from cybercrime.

Deakin University curbs security risks of curious students

'STUDENTS TYPICALLY USE

technology in an unusual way compared to staff, and this sometimes triggers indicators of compromise for their behaviours,' says Fadi Alja'fari, Information Security and Risk Manager at Deakin University.

'That was our big challenge and why we sought a solution with user behaviour and entity analytics (UEBA). We needed a technical solution to help normalise these events, and to differentiate between what is a malicious indicator of compromise and something that's benign or unexpected behaviour.'

The cyber security team evaluated four of the top solutions surveyed by Gartner and chose the Exabeam Fusion SIEM to meet its requirements. Top criteria included better visibility via user- and device-based analytics, easy implementation, ease of use, and a good support model.

'Out of the box, our security operations analysts can use Exabeam Fusion SIEM to respond to alerts without much customisation,' says Alja'fari. 'This allows our security engineers to focus all of their time on improving our cyber defences instead of learning how to create anomaly detection and events correlation queries – which was incredibly time consuming.'

Deakin University's security operations team values opportunities to save time and resources. The team was painfully aware of being outgunned by data: its log aggregation solution generated massive amounts of feeds and alerts on the network. Deployment of Exabeam enabled automatic analysis of all the university's security data, with notifications of anomalies as they materialised sent to security operators.

'Before Exabeam, operators had a delay of deciphering the data and attempting to understand which events might lead to an actual security incident,' says Alja'fari.

For example, students might use a VPN service in different ways from a staff member, according to



Alja'fari. 'Students will use a VPN to try jumping through proxies, using the Tor network, or use one just to try it out and experiment.' He notes that these behaviours might ordinarily trigger security alerts by legacy tools. 'With Exabeam, we can tell when a student's VPN behaviour is legitimate and not an indicator of compromise. This saves our security team an enormous amount of time.'

Some of Deakin's other use cases addressed by Exabeam include identifying legitimate network logins from multiple geolocations, leveraging email logs for data leak prevention, and implementing a more cost-efficient logging strategy. 'Exabeam's

threat hunting capability is something the security operations team looks at on a daily basis for anomaly analysis,' says Alja'fari.

Deakin University benefits from its Exabeam deployment with:

- stronger enterprise security, with behavioural analytics by discovering unusual risks from student 'experimentation'
- deeper visibility on enterprise risks, and a streamlined, proactive method of addressing security issues
- augmenting cyber security education for student interns who shadow security team use of Exabeam. •



You can
resolve attacks.
Or, you can
resolve attacks
faster.

Odds are you're overwhelmed
by alerts and manual threat
investigations.

**Exabeam has the analytics and
automation you need to streamline
and accelerate threat detection,
investigation and response to stay
ahead of attackers.**

Outsmart the Odds.



Ransomware is only part of the security conversation

BY JASON SMART, CYBER SECURITY DIRECTOR, PWC AUSTRALIA

Cybercriminals are looking at the bigger picture – so make sure you do, too.

THERE'S NO QUESTION that ransomware poses a real and significant threat to Australian businesses – but with so much talk about ransomware in the media, it's easy to get distracted from the threats posed by other vectors, including malware, business email compromise (BEC), supply chain attacks and nation-state actors.

Those threats haven't gone away just because ransomware has increased; in fact, all indications are that more creative cybercriminal attackers are continuing to test corporate security defences using many of the same techniques they have been using for years.

Many companies seek help resolving compromises caused by exploits that are well-known and well-understood. They often fail to see other attacks coming because 'selection bias' focuses attention on the highest-profile threats.

Even companies that are investing in security operations centres (SOCs) often do so without a complete vision of the defences

they need to put in place to support those capabilities.

This can leave them with SOCs that are perfectly good at monitoring their current operational state and providing a platform for incident response – but fall short in anticipating attacks because they do not implement adequate threat intelligence capabilities.

Without integrating effective threat intelligence into their security posture, even those with otherwise extensive security budgets are flying blind, lacking a complete picture of the changing threat profile.

That leaves them exposed to threats (including nation-state threats) that still represent a clear and present danger, with foreign threat actors still very interested in Australia's businesses and government bodies.

In our experience, many companies are also failing to consider threat intelligence impacts on their supply chains – even well-protected companies can be compromised through trusted partners or suppliers that lack the same level of protection or threat intelligence.



Jason Smart

Within the last year alone, the SolarWinds, Kaseya and Accellion breaches have demonstrated how effectively trusted supply chains can be used for nefarious purposes.

Threat intelligence researchers are observing similar traits across these breaches, and we know that guidelines like the Australian Signals Directorate's Essential Eight can go a long way towards preventing them from happening again.

To adequately protect your own business, make sure you focus not only on protecting your own networks, but that you also invest the time and money to secure other points of vulnerability.

Despite continuous warnings from security experts, many companies still do not test the security of their supply chains, introduce security controls to mitigate supplier risk or otherwise ensure their suppliers meet the same standards required of their own networks. That's like locking your front door while leaving your windows wide open.

To stay safe, step back and consider the bigger picture around your cyber security – particularly the threat landscape throughout your supply chain – and make sure you consider this in the context of your entire business. •





How can we
keep your business
and our economy
protected?

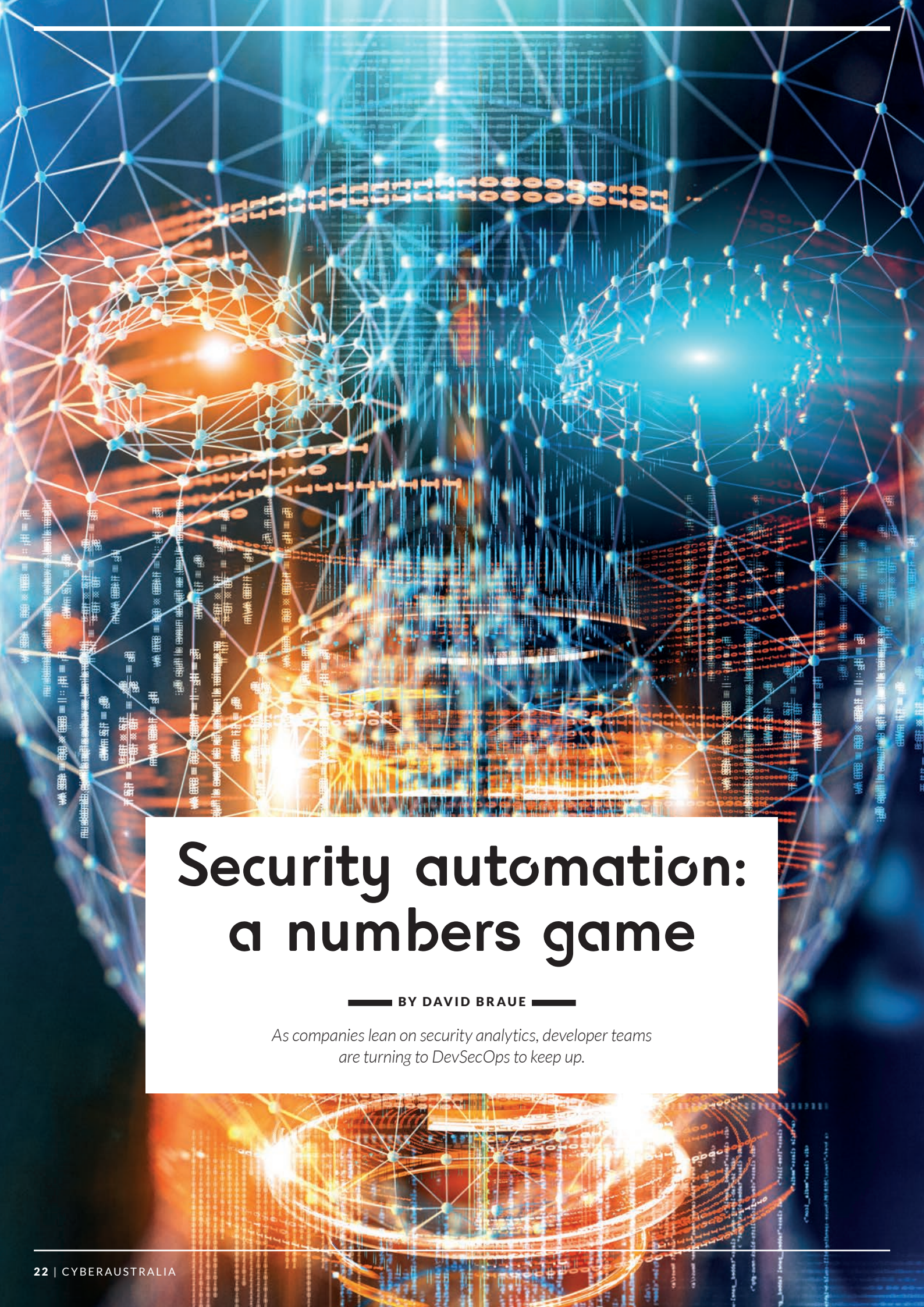
By creating
solutions together.

Every day across the globe, our community of solvers work together with business leaders, governments, regulators and our own researchers to understand and protect businesses and society from the critical cybersecurity threats we all face.

We translate our deep understanding of the threats and risks on the security frontline and within emerging technology into meaningful insights that work for your business. By creating solutions together to safeguard your organisation, you can pursue new opportunities and ensure your business isn't just protected, but thrives.

www.pwc.com.au/cybersecurity





Security automation: a numbers game

— BY DAVID BRAUE —

*As companies lean on security analytics, developer teams
are turning to DevSecOps to keep up.*

The digital transformation of the major retailer Big W began several years before the COVID-19 pandemic hit, but the company's rapid transformation to an integrated digital shopping experience proved timely as lockdowns pushed customers towards click-and-collect and home delivery options.

Supporting this change at the company's back end was a major cultural transformation that helped accelerate application development by bringing together software engineering and infrastructure teams to create a development, security and operations (DevSecOps) culture.

This integrated, accelerated development cycle has helped speed the team's software development from deploying once per month or quarter to deploying new versions of its software 10 times per day. DevOps Engineering Lead Anton Vishnyakov has also created a new imperative to ensure that this faster cycle also maintains crucial data security.

With its heightened focus on security, Big W has joined myriad companies embracing DevSecOps – an invaluable new capability that is integrating security best practice into a DevOps world where automation has quickly become an integral part of faster and more accurate delivery.

'At some point, the complexity of the systems is so high that it's just not good enough to have disconnected teams,' Vishnyakov said during a recent GitLab webinar, in which he noted that DevSecOps success 'is all about bringing teams together'.

Network, data, mobile and other engineers all have input into the application development life cycle, and security means something different to each of them. DevSecOps is causing teams to 'shift left' by pushing security into the development cycle earlier, he said, which creates its own challenges.

'We add more people, more money and more expertise to achieve the same goal,' he explained. 'It's not only diversification of expertise from the security team, but [it also] allows us to make more data-driven, precise and informed choices.'

That ability is crucial in retail, where increasing online exposure has become essential in preventing cybercriminals from harvesting sensitive personal and financial details en masse.

According to Verizon's latest Data Breach Investigations Report, system intrusion, social engineering and basic web application attacks – all key security threats that DevSecOps can mitigate – accounted for 77 per cent of the 165 confirmed breaches where sensitive data was compromised last year.

Avoiding this has become increasingly difficult given the sheer pace of transformation and the pandemic-era pressures put on teams to keep up.

'Technology-wise, we are coping with an enormous complexity of modern systems, whether in the cloud or

Kubernetes and other complex technologies,' Vishnyakov explained. 'Automation takes that complexity away and makes it a consumable product for engineering teams.'

Yet, reaching that point can be a challenge, Vishnyakov added, noting that transitioning to a DevSecOps mentality requires the 'same story that happened with DevOps – but at a much faster pace, and probably [with] much higher stakes, because it's security'.

PUTTING A PRICE TAG ON AUTOMATION

The shift towards DevSecOps is proceduralising a trend that began years ago, as the increasing complexity of enterprise systems – and their companion security monitoring tools – made it clear that contemporary security architectures would buckle under the weight of monitoring data.

Not only could humans no longer keep up with the firehose of security alerts, but the use of data analytics driven by artificial intelligence (AI) and machine learning (ML) was the clear choice for performing deep analysis on large datasets where cybercriminals actively try to minimise their footprint.

By picking out seemingly inconsequential indicators of compromise spaced across long periods of time, AI-based security analytics tools have been a shot in the arm for companies' efforts to identify compromises, including low-and-slow advanced persistent threats (APTs).

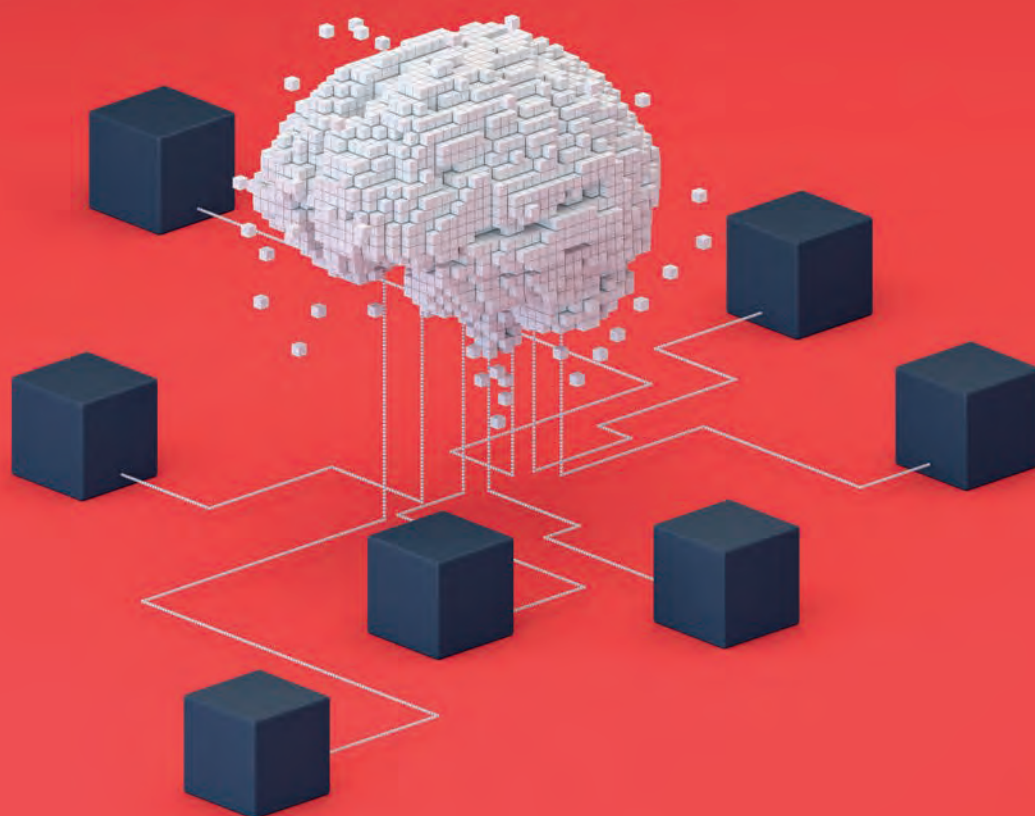
Analytics-driven security operations also tap into formal threat-intelligence feeds that monitor new threats and vulnerabilities as they emerge to give companies a heads-up as the most pressing threats wax and wane.

These factors have rapidly changed the way companies protect themselves against breaches – and, paired with DevSecOps' ability to automate the application of that insight, statistics now show just how valuable security automation has become to the corporate bottom line.

Indeed, the recent IBM and Ponemon Institute Cost of a Data Breach 2021 report found that fully deployed security AI and automation were the single most effective way to reduce the cost of a data breach.

Breaches were 80 per cent less costly, on average, in companies that reported they had fully deployed AI and automation capabilities – \$3.98 million (US\$2.9 million) on average, compared to \$9.2 million (US\$6.71 million) on average in companies without such capabilities.

Companies with mature AI/ML and automation capabilities also proved better at quickly identifying and resolving data breaches. This translates into significant benefits for industries like retail, where the average cost of data breaches surged by 63 per cent over the past year – from \$2.8 million (US\$2.01 million) last year to \$4.48 million (US\$3.27 million) – largely due to the sector's high degree of exposure in a period of rapid changes in consumer demand.



THE PATH TO AUTOMATION

Companies have warmed to the idea that security automation has become a necessary capability in today's computing environment, with Splunk's latest State of Security survey confirming that 82 per cent of organisations see security analytics, automation and ML as being more important to security decision-making than they were two years ago.

Recognising this trend, security vendors have been racing to add AI and automation capabilities to their products, with AI-driven analytics already available in some form from every major security vendor, and a slew of startups joining the party with AI-native tools.

Every company is at a different point in its adoption of the tools; however, Gartner believes the transition to AI-driven security will be a significant factor in security technology and services spending, which will grow 12.4 per cent this year alone – twice as quickly as the 6.4 per cent growth rate recorded last year.

'Organisations continue to grapple with the security and regulatory demands of public cloud and software as a service,' notes Gartner Managing Vice President Lawrence Pingree, who adds that growth in 'early market signals of growing automation and further adoption of ML technologies in support of AI security'.

'To combat attacks, organisations will extend and standardise threat detection and response activities.'

The transition to DevSecOps will be a key part of this trend. Gartner Senior Director Analyst Mark Horvath recently outlined five key steps that will speed the transition to an automation culture:

1. *Establish surface security requirements early*, doing some things that allow developers to start off in a good place.
2. *Adapt some of the security concepts to developers* so they are not learning security language so much as putting things in their own native language.
3. *Introduce security coaches*, because not every developer has expertise in everything; this is the agile DevSecOps way of bringing expertise into a team.
4. *Use harm reduction* as an iterative strategy. 'Any step you make towards a secure outcome is better than not having made that step. We want to reduce the risk and harm that the application is exposed to; over many cycles, we come out with a really good outcome,' Horvath says.
5. *Embrace threat models* offering a 'very powerful way' of getting developers started on the right foot, without them having to understand what the patterns are.

Over time, Horvath says, 'Security becomes the tenet of development; it becomes something the team can be good at and is consumed in a way that is native to what the team is doing.' ●



Provide Complete Control & Visibility Over File Transfers

MOVEit is the leading secure managed file software trusted by thousands of organizations worldwide to provide the secure and compliant transfer of your sensitive data.



**DEPLOY ON-PREM
OR IN CLOUD**



**EMAIL AND
WEB TRANSFER**



**REST API
FUNCTIONALITY**



**AUTOMATE MANUAL
PROCESSES**



**SECURE END-USER
COLLABORATION**



**MOBILE
APP**

Loved by Users



Capterra



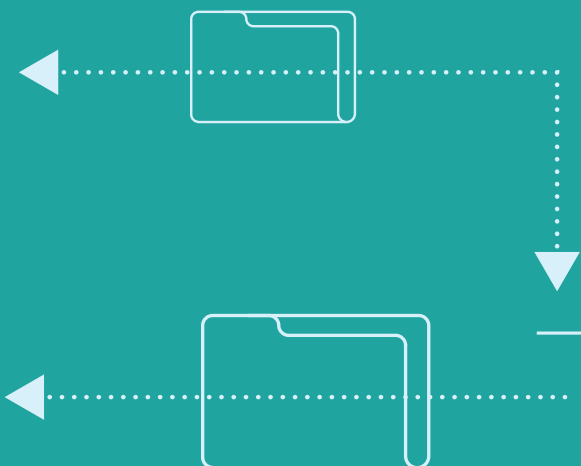
G2 CROWD



TrustRadius



spiceworks



Start your free trial today:

www.ipswitch.com/trial

Contact us:

www.ipswitch.com/contact-sales



From cyberthreat to cyberwarfare

— BY SIMON GALBALLY —

Catastrophic ransomware attacks have been a wake-up call, but the looming main event is quantum computing. Data has never been more exposed to cyber attacks due to the exponential growth in remote working and cloud computing. Similarly, cybercriminals have never been better resourced, yet many cyber security solutions are no longer fit for purpose. Today's most sensitive long-life data must be safe in a post-quantum world.

In 2020, a single cyber attack reported to be among the worst cyber espionage incidents in history – attributed to Russian state-sponsored cyber gangs – breached at least 200 major organisations around the world, including US government agencies, the North Atlantic Treaty Organization, the European parliament, Microsoft, and various other government agencies and commercial enterprises. It successfully exploited software systems including SolarWinds, Microsoft and VMware. Its long duration of nine months and successful data breaches highlighted key cyber security issues:

- › failures in 'legacy' malware detection and prevention cyber security solutions
- › failures to encrypt sensitive data when stored and moving across networks
- › the consequences of software systems' security vulnerabilities – an issue reflected in the US cyber security Executive Order.

While global cyber attack statistics highlight the need for zero-trust cyber security strategies, many 'legacy' anti-malware/anti-ransomware cyber security solutions relied upon today may no longer be fit for purpose, and enterprise business software systems are often too vulnerable.

Advanced technology, critical national infrastructure, government and health sectors are prized targets for cybercriminals, whether they are state-sponsored or other bad actors. Now, the COVID-19-driven world of remote worker collaboration and the exponential growth of cloud computing are increasing these organisations' exposure to cyberthreats. Their confidential data and the networks carrying it are exposed to increased attacks.

All organisations' IT systems are subject to multiple attack vectors, where vulnerabilities may be exploited – not just for financial gain, theft of intellectual property

and citizens' identities, but also to cause business disruption and catastrophic harm. The threats of data breaches arising from ransomware/malware attacks and network ingress hacking attacks demand a zero-trust cyber security approach. Proactive anti-malware/anti-ransomware, strong data encryption and secure encrypted remote worker collaboration require fit-for-purpose, state-of-the-art cyber security solutions.

FIT FOR PURPOSE

The continuing failures of 'legacy' cyber security solutions to effectively prevent catastrophic cyber attacks are well-documented. Many legacy anti-ransomware/anti-malware solutions are no longer fit for purpose – being detection-based and dependent upon 'disclosed' known malicious code. They are ineffective in the face of today's signatureless 'undisclosed' malware and zero-day threats.

Enterprise software systems proven to be vulnerable to cyber attacks are dependent upon customers implementing queues of frequent software security patching. Systems-critical data networks, and cloud computer and storage network solutions are increasingly exposed to eavesdropping and data ingress, leading to data breaches and hack attacks such as denial-of-service and flooding attacks. Both require state-of-the-art cyber security for maximum data protection.

The world of cyber security has changed significantly, reflecting new cybercriminals who are better resourced and more skilled than ever, including globally connected cyber gangs and state-sponsored syndicates.

The Australian Cyber Security Centre highlighted that 25 per cent of 67,000 reported cyber attacks focused on critical infrastructure, and that a cyber attack occurs every eight minutes in Australia, with criminals and spies exploiting COVID-19 remote work. Similarly, the Office of the Australian Information Commissioner reported that the healthcare sector suffered the worst data breach statistics in Australia, including stolen patient records and database hacking. It also highlighted significant breaches in the finance, legal, accounting, insurance and government sectors. The critical questions are: were the cyber security solutions effective, and what percentage of the breached data was protected by encryption?



Then there are the damaging ransomware attacks. The most notable recent attacks in Australia were on Nine Entertainment, Toll Holdings and JBS Foods. All of these attacks resulted in serious business disruption, supply chain consequences, and significant clean-up and IT systems damage costs.

THE LOOMING 'MAIN EVENT' – QUANTUM COMPUTING

In the face of these increasing cyber security threats, the 'main event' is looming – quantum computing. It is universally considered the biggest cyber security threat in history. The threat is that quantum computers' exponentially greater computing power renders today's public key encryption algorithms redundant.

Although quantum computers may be three to five years away, the reality is that today's encrypted data will be 'backward vulnerable' to future quantum computing attacks. To be safe, data requires quantum-resistant encryption protection now.

Why is quantum computing such a threat now? The most sensitive data – citizen identities, government secrets and intellectual property – have a long life of 10, 20 or even 50 years, making it backward vulnerable today to quantum computing's arrival tomorrow. It demands long-term data protection now for a quantum-safe future.

Fortunately, quantum-resistant technologies exist today that may be implemented to protect data against both quantum and conventional cyber attacks – the use of 'hybrid encryption'.

Strong encryption begins with the algorithms. While today's public key algorithms are all vulnerable to quantum computers, quantum-resistant algorithms are designed to be secure in a post-quantum world. From the short list of candidate algorithms being assessed by the National Institute of Standards and

Technology (NIST), a draft standard algorithm is expected as soon as 2022. NIST guidelines recommend adopting a 'hybrid' classic/quantum approach today in anticipation of the new standards.

Then, quantum key distribution is necessary to allow encryption keys to be distributed in a way that guarantees forward secrecy using a quantum principle known as the 'observer effect'.

Finally, a source of genuine number randomness is required where numbers used to seed the keys are not vulnerable to prediction or bias. Randomness will become more crucial because quantum computers will be able to ascertain patterns much quicker than classic computers.

A ZERO-TRUST, QUANTUM-SAFE WORLD

Like all crime, cybercrime is a reality and here to stay, making a zero-trust approach to cyber security a necessity. The issue is whether or not the cyber security solutions relied upon are fit for purpose today. While strong encryption does guarantee data protection in the event of successful data breaches, as quantum computing approaches it is vital that organisations understand that today's conventional encryption standards won't be secure in a post-quantum world. Quantum-resistant encryption is essential.

Organisations should be planning now for the impact of quantum computing today by introducing cryptographic agility and completing a quantum computing cyberthreat analysis. Today's sensitive long-life data requires quantum-resistant encryption to ensure its future security.

The world has changed, and the main event is quantum computing as we move from cyberthreat to cyberwarfare. ●

For more information, visit www.senetas.com

SENETAS CYBERSECURITY SOLUTIONS

TRUSTED GLOBALLY
MADE IN **AUSTRALIA**.



Senetas Headquarters: 312 Kings Way, South Melbourne, VIC 3205
T: +61 (0) 3 9868 4555 E: info@senetas.com W: www.senetas.com



SECURITY WITHOUT COMPROMISE

Senetas CypherNET encryptors are FIPS and CC certified. They are used to protect commercial and government data across all network topologies. Agile by design, they also offer Quantum Resistant Encryption for long term data protection.



COLLABORATE WITH CONFIDENCE

SureDrop is the secure file sharing and collaboration application with 100% data sovereignty control. It has all the usability of box-type file-sharing apps with the addition of best-in-class encryption security and seamless integration with Microsoft Office, Azure and Outlook.



PROACTIVE ANTI-MALWARE PROTECTION

Votiro Secure File Gateway leverages patented content disarm and reconstruction technology to provide proactive protection against today's most advanced and persistent malware and ransomware attacks, including signatureless, undisclosed or zero-day exploits.





Avoid the false prophets of cyber

BY CARLO MINASSIAN, FOUNDER AND CEO, LMNTRIX

LISTED AS ‘EFFECTIVE’ controls in security standards, many assume they will be judged as doing the right thing when making the costly decision to invest, despite a history of standards outdated before publication and breaches appearing as an inevitable risk in their risk registers.

Apple, with one of the best-funded security teams imaginable, lost 90 gigabytes before a breach was detected a year later. Target – one of the world’s largest retailers, with a security information and event management (SIEM) software monitored by one of Gartner’s leading managed security service providers (MSSPs) – also experienced an outrageous breach. Insurance giant CNA Financial reportedly paid \$40 million in ransom despite its Endpoint Detection and Response (EDR) vendor proclaiming ‘We Stop Breaches’.

These breaches – and many others (don’t forget Bank of America and JPMorgan Chase & Co.) – had five things in common:

1. spending millions on cyber security
2. compliant to one or more security standards

3. demonstrated threat detection capabilities as non-existent or rudimentary
4. lost reputation, business and credibility
5. experienced escalating remediation and recovery costs post breach.

HOW IS THIS POSSIBLE?

SIEMs, EDRs, security operation centres (SOCs) and MSSPs are at the centre of many security strategies, but most are considered a failed waste of company resources. If in doubt, ask a market analyst, or better still, hire a red team.

Watch how a red team sends malware into your network, takes control of your machines, and blasts through your web application firewall. Watch how they move laterally, elevate privileges and exfiltrate terabytes without the SOC or MSSP detecting a thing.

This scenario has been playing out for years, where security-savvy organisations are either breached or test their controls to prove their inefficacy.

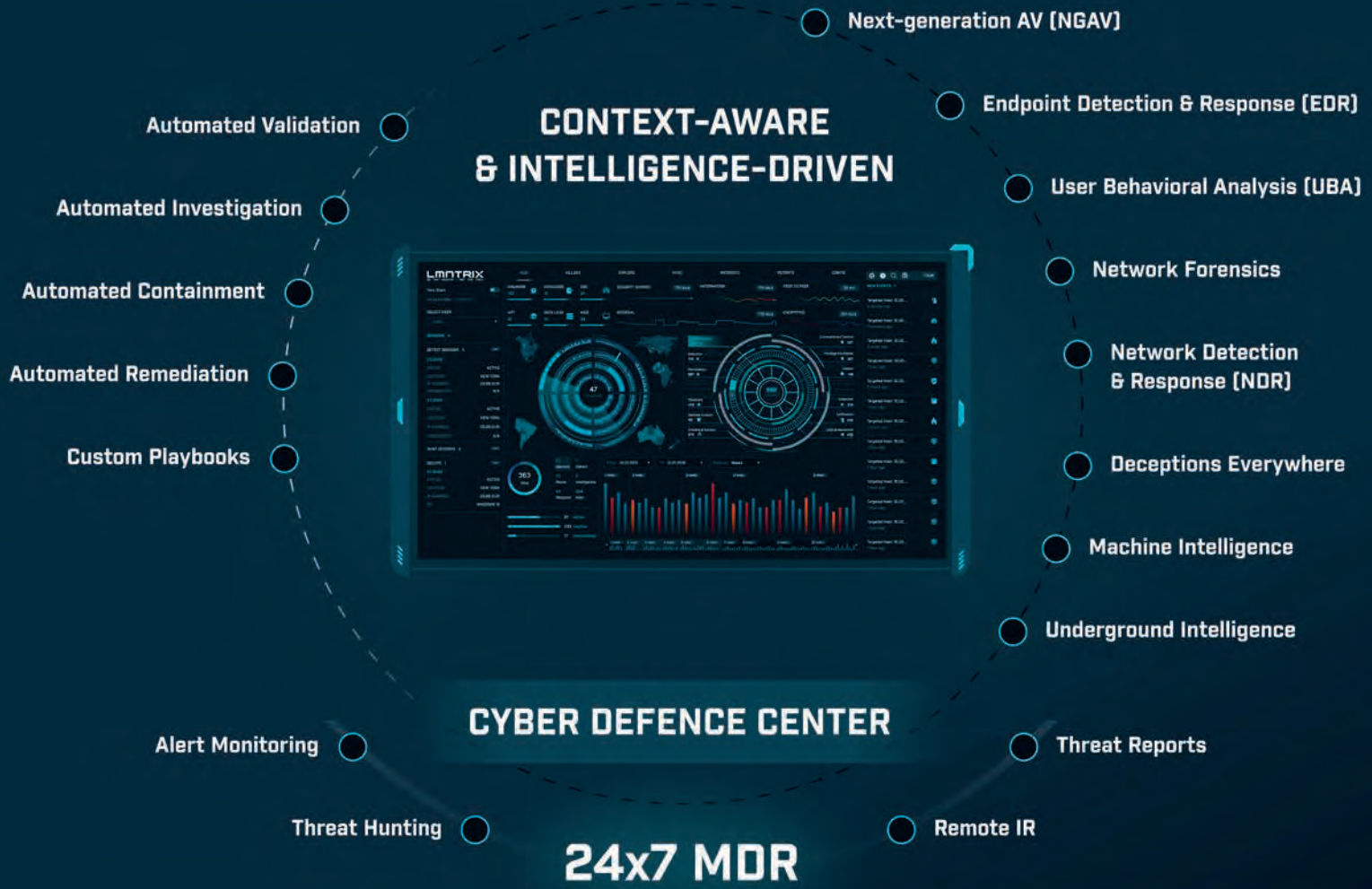
Imagine how the executives and board feel when they read the red team report.

Although clients may receive hundreds of alerts from their SIEM, EDR, MSSP or SOC, depending on the volume of logs and size of the network, almost all will be false positives.

Clients chase false positives until ‘alert fatigue’ takes over and they simply start ignoring them. A security engineer at a large client recently told me, ‘We close the incidents quickly because our chief information security officer gets upset when we have too many MSSP incidents open in the queue.’

The enlightened now seek services that suppress false positives, using advanced detection and response capability to only alert for ‘validated breaches’ with precise and timely remediation and recovery actions.

I hope this article will help you join the enlightened. Avoid the errors of the past; consider a genuine solution where breaches are validated, investigated, contained and remediated; and consider where post-breach forensics give you the full picture of scope, impact, resolution and improvement to prevent it from happening again. ●



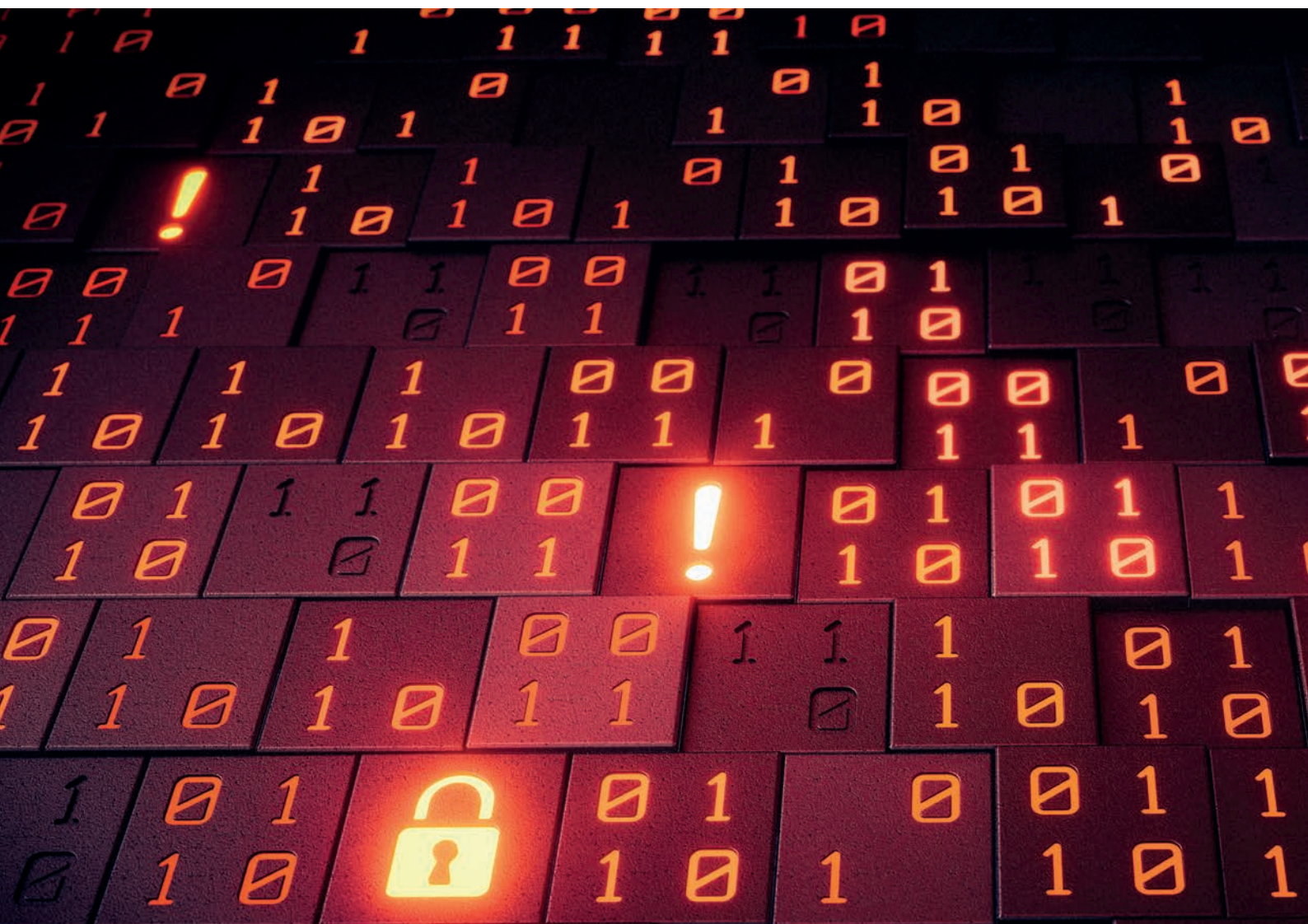
LMNTRIX unifies Machine and Underground Intelligence, NGAV, EDR, NDR, Network Forensics, UEBA and Deception Everywhere for automated attack validation, investigation, containment and remediation on a single platform and at no extra cost is backed by 24/7 Detection and Response for even the smallest security teams.



A single investigative platform for insights into threats on enterprise, cloud, hybrid, and industrial control systems (ICS) networks, LMNTRIX XDR delivers unique advantages over current network security solutions.



A holistic, multi-vector platform with unlimited retention of full-fidelity network traffic, innovative security visualizations, with ease of use and cost-savings of an on-demand deployment model.



Legal hacking – why not?

— BY PROFESSOR BRIAN MARTIN, EMERITUS PROFESSOR, UNIVERSITY OF WOLLONGONG, AND AISA MEMBER —

A new law gives police extraordinary powers for disruptive hacking, which will harm security and Australian businesses.



Brian Martin

Imagine that you are tasked with purchasing database software for your organisation. Two promising options are from Belarus and Belgium. The Belarus product is cheaper, but then you learn that Belarus is a dictatorship that spies on its citizens. You worry that the Belarus software may not be totally secure, so opt for the Belgian product.

Government repression can be bad for business. The *Defence Trade Controls Act 2012* has severe controls over Australian military-related and dual-use research, including computing research. It allows the Department of Defence to take over intellectual property. High-tech

entrepreneur Brendan Jones was one target; he ended up leaving the country.¹

Then came the law enabling Australian agencies to demand access to encrypted communications. This was opposed by the tech sector on the grounds that customers would not trust Australian products to be secure. Industry pleas were ignored.

The latest law is the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021*, which was recently passed.² It enables the Australian Federal Police and the Australian Criminal Intelligence Commission to obtain warrants to access the accounts of targets – including email and social media – and to add, change or delete data. Remarkably, this legalises what might otherwise be called malicious or black-hat hacking.



This hacking law was passed with support from both major parties. There was limited consultation, and advice from expert bodies was ignored.

The danger to the tech industry is obvious. Whatever the intent of the law, and however it is used, the perception will be that Australian products cannot be trusted. Software might have been tampered with, databases might be corrupted and back doors might have been inserted. Because accounts can be commandeered, even the authenticity of messages may be in doubt. These worries might be unwarranted, but, like the hypothetical Belarus example, perception can be just as influential as reality.

It is well-documented that police with access to databases on citizens can be bribed, often on a regular basis, by private investigators seeking information. And some police misuse their access for personal reasons – for example, to stalk an ex-partner. Imagine the attraction

that hacking powers will create for mission creep and individual abuse.

TACTICS

Around the world, powerful perpetrators of injustice – for example, illegal surveillance, sexual harassment, police beatings and massacres – try to reduce public outrage about their actions.³

A crucial technique is cover-up. The hacking law provides severe penalties for revealing any operations. When people don't know what agencies are doing, they won't be upset.

Another outrage-reduction technique is reframing: namely, describing the action in a favourable way. The rationale for the hacking law is to counter criminal activities, such as paedophile rings – surely a worthy goal. This distracts attention from the lack of specificity in the law – it can be used more widely.

A third technique is devaluation. The government's rhetoric suggests that anyone opposed to the law opposes action against criminals.

Then there is intimidation. Exposing hacking operations can lead to 10 years in prison. On top of this is a plausible fear that those who speak out might themselves become targets of surveillance.

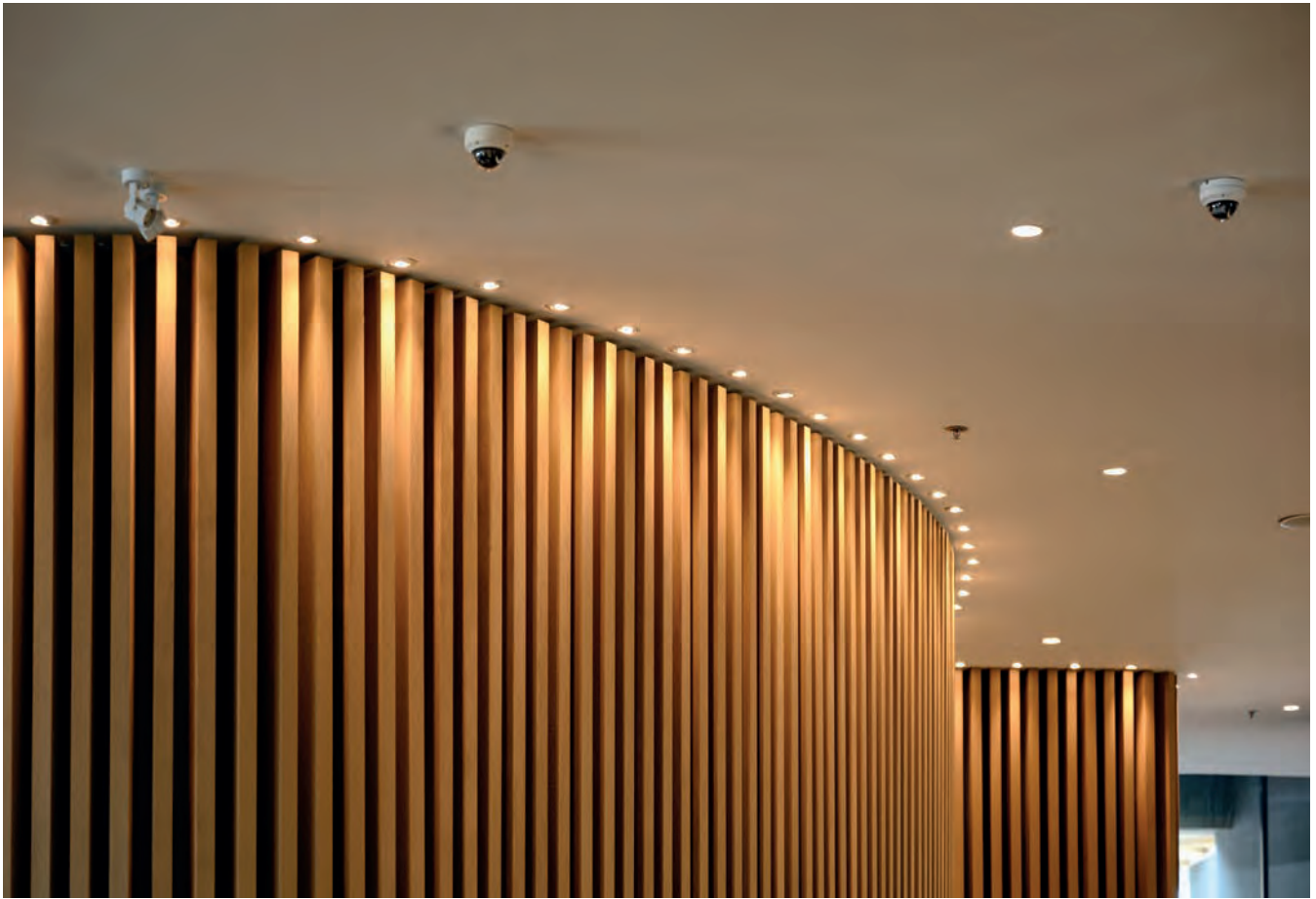
The government has followed the playbook of other powerful perpetrators, and the damage to the tech industry is an afterthought. Implicitly, industry concerns are devalued – that is, if they receive any attention at all.

Looking at these methods to reduce outrage over injustice points to counter methods: expose the adverse actions, counter rationales, frame legal hacking as an injustice, have respected individuals and groups give credibility to concerns, and stand up to intimidation. There is an alternative. Like Brendan Jones, you can give up on Australia – or you can resist. Resistance against legislation that overreaches requires voices – particularly those from industry. This is exactly the sort of legislation that the Australian Information Security Association (AISA) – in partnership with its sister associations across the business community – should speak up against in public venues. •

A theoretical physicist by training, Brian Martin is Emeritus Professor of Social Sciences at the University of Wollongong, and the author of 20 books and hundreds of articles. He has a special interest in free speech and organisational dissent.

References

- 1 Brendan Jones, 'Defence takes control over Australian research,' *Australasian Science*, April 2016
- 2 <https://bit.ly/3pDrqPQ>
- 3 'Backfire materials,' <https://www.bmartin.cc/pubs/backfire.html>



Cyber cloaking

LAST SEPTEMBER, GARTNER included cyberthreats to physical processes and assets in its 'Top 9 Security and Risk Trends for 2020'. The global research company explained how 'emerging threats, such as ransomware attacks on business processes, potential siegeware attacks on building management systems, GPS spoofing and continuing operational technology (OT)/Internet of Things (IoT) system vulnerabilities, straddle the cyber-physical world'.

Security misconfigurations or, in some cases, a total disregard for security, resulting in opportunistic attacks, are some of the most common security shortcomings today.

Ransomware has long been an IT security issue, but can also impact building management servers that may control multiple systems, like lighting, and heating, ventilation and air conditioning.

Picture the wasted stock that a butcher would have to discard if their refrigeration system was tampered with, or building occupants being unable to exit the building after access

controls were locked down. These are extreme examples, but are a wake-up call. Organisations must consider what they could be liable for in the result of an attack. More commonly, the issue revolves around money. Opportunistic robots don't care what the system is – all they want to do is lock it up and ransom it back to its owner for cryptocurrency.

Not defining clear lines of ownership is one of the biggest mistakes an organisation can make when it comes to OT security. Between facilities managers (FMs), OT managers and, sometimes, building management system contractors, there are often no clear lines of accountability for the system. There's no rule for who should own any system – as they are all different – as long as somebody does.

To even start to tackle the cyber security issue, a current understanding of a site's risk profile is required, including what assets are on site and their life cycles. Tackling the issue can be an incredibly technical task most of the time. It is

unfair to expect FMs or contractors to build this by themselves. Progress is being made in this area, though, as many buildings and real estate investment trusts are building cyber security policies that empower their FMs to communicate cyber risk and expectations with contractors. For this reason, a contractor who provides support that helps FMs to understand and meet their security requirements, regardless of their OT security literacy, is key.

Cyber cloaking is the best defence. Without it, you are exposed directly to the internet. Cyber cloaking will hide you to the point where, based on the Australian Cyber Security Centre's recommendation of security modelling, nothing should be accessed without some sort of VPN. This prevents bots and unknown people on the internet from being able to detect your equipment during their scans.

Grosvenor Engineering Group's team of cyber experts can assist you with risk modelling and getting the right solution to make you invisible to the bad guys. •

Are there gaps in your OT security?

BE INVISIBLE.

An oversight of many property managers is thinking that Cyber attacks only occur through IT systems, however, ransomware attacks are becoming increasingly common through Operational Technology (OT) systems. Think: HVAC, BMS, CCTV, Fire systems, IoT and other services critical to running your buildings.

Grosvenor Cyber Cloaking

Will ensure you're not exposed, after all, outsiders can't attack what they can't find.

Speak to our OT experts to embrace all the benefits of smarter buildings without the cyber security risk.

www.grosvenorcyber.solutions



GROSVENOR]
engineering group



A person with dark hair and glasses is seen from the side, looking at a computer monitor. The room is dimly lit with a strong blue light source, possibly from the screens or ambient lighting. In the background, another person is partially visible, also working at a computer. The overall atmosphere is focused and technical.

Life as an ethical hacker

— BY CRAIG FORD —

Have you ever wondered what it would be like to be an ethical hacker?

When I talk about ethical hacking, I am not talking about the fluffy Hollywood version of a hacker – that isn't real. Seriously, you can't think a hacker sits around in a dark basement with a hoodie pulled over their head, typing with leather gloves. Have you ever tried to type with leather gloves on? Or any gloves at all? It is unrealistic, and it's restrictive; you would click the wrong keys, and there is no way you would be able to type fast enough to hack a secret foreign government server in just a few minutes, as they do on the big screen.

What about that darkened room? I don't know about everyone else who works on computers for a living, but my eyes are not as good as they used to be – there is no way I could get away with working in a dark room. I would get the worst headaches and pretty much destroy any vision I have left in my eyes.

Oh, and don't forget the crazy matrix code running on all of the computer monitors, which means absolutely nothing to anyone at all.

Now that we have gotten that out of the way, what would life as an ethical hacker really be like? First, just to be thorough, let's explain what an ethical hacker is. An ethical hacker is essentially a hacker or security professional who looks for vulnerabilities or configuration mistakes in a client's system. They could even be a penetration tester who has been hired by a particular client to test their systems for these types of issues or vulnerabilities, to report on them and, in some instances, to recommend changes to remove the threat or risk before a malicious actor – aka the bad guys – tries to exploit them for their own gain.

They could perform a similar role through a bug bounty program, looking at companies' systems as part of an approved testing regime, being rewarded with a monetary bounty if they find something of worth and submit a report to the client. This is becoming a very common model, and there are some very successful ethical hackers making a great living via the bug bounty model.

The last type of ethical hacker is what I would say is a bit more of a grey area in the ethical hacking space. Essentially, this ethical hacker would, without anyone's permission, scour the internet for any and every vulnerability. They would exploit them, test the vulnerabilities and then, in most cases, ethically disclose these vulnerabilities to the affected organisations – allowing them to secure the threat before it is publicly disclosed. These ethical hackers would sometimes also be paid a bounty, but other times (if they don't get the response they want) they may publicly disclose the vulnerability without the company's permission or the company having any real chance of shoring up the risk.

So that, in a nutshell, is what an ethical hacker is. Many people want to know what it is really like to be a



hacker, spending your days hacking into systems and just being really awesome. Well, let's stop there.

Most of the time, being a penetration tester or ethical hacker is pretty boring. You could be reviewing code for days, using tools to try to manipulate known vulnerabilities, just dredging through every part of a system looking for one little thread to pull. It isn't as exciting as all of that Hollywood drama, I am sorry to tell you.

Once you have finished your testing – whether you find anything of merit or not – if you are penetration testing, you would need to write a 50-page report on everything you did, why you did it and what the results were. As a penetration tester, report writing is as big a part of your job as the testing is. You need to ensure that you document everything along the way and collate the information in a meaningful report at the end.

That's one big thing everyone needs to know before they go down the path of being an ethical hacker: you need to know how to write a good report. Whether you are penetration testing or doing bug bounties, that skill can mean the difference between a good payout and not very much. You need to be able to clearly define the vulnerabilities and what they mean from a business/day-to-day operations viewpoint.

Don't get me wrong, being an ethical hacker can be an awesome career, but you need to understand what it is really like and not fall in love with the Hollywood lie. It's important to understand what you will do on a day-to-day basis. It's challenging and, at times, exciting; but you need to be grounded in reality before going down this path.



You will need to look closely at yourself and figure out if you are suited to being an ethical hacker. Not everyone is, and that's okay. We are all individuals and we all have specific skills. That's what it means to be human. So, how do you know if you would be suited to ethical hacking?

Let's widen this out a little. In your day-to-day life, how do you see the world? Do you walk into a room and start to look for weak points, ways you could manipulate something, or ways to gain access to a system or network? Do you use a device or application and automatically start to think of ways you could manipulate it to do something it was never intended to do? Do you sit on the train and see things that you could use against users, and analyse everything?

When you go to a website, do you see web forms or add-ons that automatically raise alarm bells for you? Do you just 'feel' that they are a risk, and know that it should be done better? Do you want to know how things work, break them down and then put them back together?

If you've answered yes to any of these questions, you really could be a great ethical hacker; you have that natural curiosity, and that need to see more than just what is in front of you.

Security is a big industry, so if this doesn't sound like you, that's also great. You have more options than just getting into penetration testing. You could get into awareness: the human side of things. You could join the blue team in the security operations centre to help stop attackers and threats from getting through. There are also governance, risk and compliance, and even

management roles that are all important to keeping systems and data safe.

If you have an interest in security, find what makes you tick. If that's ethical hacking, great. If it's not, then we still need you; we need people to look at things differently. We have a lot of challenges that we all need to work on to make our systems safer and more resilient against malicious threats. You may not end up as an ethical hacker, but you might figure out how to make encryption better. You might even figure out how to teach security awareness, helping users to learn how to stay safer online.

What problem can you help solve in security? Find that and make it your mission. •

Craig Ford is a cyber security professional with experience working in ethical hacking, incident response, security consulting and more. Ford is the AISA Cyber Security Professional of the Year 2020, and a nominee for the AWSN Women in Security awards – Male Champion of Change 2021. He is a Senior Security Architect with Baidam Solutions, and is currently doing a full-time placement with the Australian Taxation Office in Brisbane. He is a freelance cyber security journalist with previous works on CSO Online, and has a regular column in *Women in Security* magazine. He is a published author of two books (*A Hacker I Am* and *A Hacker I Am Vol 2*), and has a new book series starting with *Foresight*, a hacker/cyberpunk fantasy novel, currently in the works and set for publishing in the second half of 2022, with more to follow soon after. Ford has been a member of the AISA Brisbane executive team since early 2020, and was recently been appointed the Branch Chair for Brisbane.



QBE Strengthens Zero Trust Posture with Illumio

Gaining micro-segmentation that reduces complexity and risk across a globally distributed infrastructure

As operations span Australia, Asia Pacific, Europe, and North America, the scope and scale of the company's compute estate continues to expand. The move to hybrid multi-cloud data centers and an increasingly complex application environment required QBE to think differently about how to protect the organization and its customers.

Further compounded by the rising threat of ransomware in the industry, a Zero Trust approach to security became front of mind for CISO Andrew Dell. "We have partners inside our network, service providers that are in the cloud, and other networks connected to us," he explained. "So, we need to think differently about controlling access to our data and our applications, how we reduce risk, and what technologies will help get us to a Zero Trust model."

A focus on Zero Trust meant re-evaluating the company's segmentation strategy. QBE relied on physical firewalls and virtual firewall appliances for segmentation, which proved to be "labor intensive and complex," according to Andrew. Firewall rulesets would become almost unmanageable for the team, potentially putting the very applications they were trying to protect at risk.

QBE needed micro-segmentation for more efficient, granular control over dynamic environments. Futureproofing the business with a solution that would empower the organization to "go faster, safely" was critical. "We are always looking for simple solutions to complex problems," said Andrew. He found exactly that in Illumio Core: a software-based micro-segmentation solution that eliminates network segmentation headaches and provides the foundation for Zero Trust security – starting with visibility capabilities.

Illumio's real-time application dependency map showing traffic flows between workloads wherever they run delivered quick value. "The initial attraction was really the simplicity," recalled Andrew. "Having the ability to span the physical and the virtual and present insights in a highly resolved fashion is a game-changer. It enabled us to be more efficient with our resources and planning right away."

Equipped with the understanding needed to segment confidently, the team set out to tackle "crown jewel" applications first. According to Nick Venn, global collaboration and cyber infrastructure manager at QBE, "Since Illumio policies are independent of underlying infrastructure, we get greater and granular security and performance. And the best thing is the policy can now follow the workload, so we don't have to worry about recreating policies or re-architecting the network. That flexibility is absolutely essential."

These efficiencies translate into years saved for QBE. "For an organization of our size and scale and complexity, traditionally rolling out an equivalent solution was a multi-year proposition," said Andrew. "But with Illumio, we had production assets enforced and under control in months, fulfilling our need to move faster and further our Zero Trust posture..."

Learn more about QBE's Zero Trust journey at www.illumio.com/resource-center





Segment in minutes on your path to Zero Trust

Stop ransomware, contain cyberattacks, and reduce risk with automated security enforcement.

[START YOUR JOURNEY AT ILLUMIO.COM](https://illumio.com)



THINK YOU'LL NEVER FALL FOR A BUSINESS EMAIL COMPROMISE SCAM?

Despite awareness, Australian companies are still losing millions to business email compromise every year.

David Braue reports.

With all of the security industry's focus on ransomware, it can be easy to forget that the old favourites are still out there, too. Business email compromise (BEC) remains a major threat for companies that still haven't implemented the changes needed to defend their core business processes against manipulation.

BEC scams took more than \$79 million from victims in over 3300 incidents reported to the Australian Cyber Security Centre (ACSC) over the past 12 months, according to a recent update from the Australian Federal Police (AFP).

Construction firms have become a favourite target, with the ACSC recently releasing a formal alert warning of a 'growing trend' of BEC attacks on Australian construction companies.

Many characteristics of the construction industry make it ripe for picking by BEC criminals – including the large sums of money and regular milestone payments involved in

construction contracts; the complex labour arrangements that provide many opportunities to pose as a subcontractor; the large number of relatively unsophisticated small businesses and sole proprietors; and the large number of invoices circulating around any given project.

Scammers typically go to great lengths to support their ruse, using techniques like registering look-alike domain names; hacking the email accounts of legitimate suppliers, then sending invoices with new account details; or playing confidence games by impersonating executives on the phone or in person.

Across construction and other industries, the Office of the Australian Information Commissioner (OAIC) received 35 reports of impersonation-related data breaches during the first half of 2021 alone.

Each of those victims likely believed that they would never fall for such a ruse, but ongoing reports of breaches confirm that cybercriminals remain as adept as ever at circumventing victims' precautions.

In late 2020, one Australian business engaged the AFP after cybercriminals hacked its email system and sent emails to internal staff requesting payment of invoices that had been doctored to include the scammers' Singapore bank details.

Two payments were processed – totalling \$519,545 and \$2,148,938 – before the company realised that it had been hit by BEC scammers.

Rapid engagement with authorities – the AFP liaised with Singaporean authorities via Interpol – saw the second funds transfer blocked in Singapore, limiting the company's losses to just the first transfer.

THE ENTERPRISE STRIKES BEC

For most companies, however, the loss of half a million dollars can pose an existential threat – and not everybody is so lucky.

The key to protection against BEC fraud, the ACSC says, is to remain ever-vigilant for telltale signs of fraud. Ensure that any requests for large transfers or changes to bank details are vetted and confirmed with calls or face-to-face visits. Consider implementing a layered approvals process to ensure that no one person's oversight will contribute to material losses.

Effective BEC defences also require a concerted focus on staff training, with employees requiring a healthy degree of scepticism to ensure that they take adequate time to evaluate the veracity of any requests for action. This includes emails that may purport to be from suppliers requesting that the accounts payable or other staff members log into a key system to confirm their details; such requests are common phishing attacks that continue to deceive too many victims, far too effectively.

The lingering threat of BEC has persisted throughout the pandemic; even as ransomware grew to account for around 30 per cent of US data breaches during 2020, BEC was not far behind, accounting for 27 per cent of breaches analysed in the recent F5 Application Protection Report.

Yet, while BEC is often discussed as a separate type of attack, F5 Threat Research Evangelist Sander Vinberg warns it's important to remember that BEC 'is not really a tactic or a technique, [but] an outcome of an attack'.

Where BEC scammers use hijacked email accounts, he says, those accounts were made vulnerable due to a completely different compromise – often the publication of an authorised executive or finance employee's passwords due to a prior data breach on a completely different site.

Scammers regularly use massive, freely available databases of stolen passwords to fuel 'credential stuffing' attacks whose ongoing and significant success stems from the fact that many users still re-use the same password across many business and personal sites.

Successfully finding a CEO's email password is an open licence for a BEC criminal, who now doesn't even need to spoof the CEO's identity to execute their fraud.

In this case, the lack of obvious deception can be a major problem for companies whose employees aren't conditioned to question the instructions of their superiors.

With many reported BEC compromises but a relatively low number of reported credential-stuffing attacks, Vinberg believes that companies keen to tighten their BEC defences face a dual-pronged challenge. 'It tells us, firstly, that credential stuffing is a problem, but it also tells us that detecting credential stuffing is a significant problem,' he explains.

Companies must stick to 'defence in depth' strategies that layer defences and processes in order to maintain BEC protection despite ongoing change, says Vinberg.

'It can be very easy to not take the time to blend new controls into a holistic security architecture,' he adds, 'and so we can accidentally undo our defence-in-depth principles' with limited visibility of credential stuffing and other BEC enablers.

A range of companies have taken different approaches to improving detection of BEC fraud, with email filtering providers like Mimecast and Proofpoint leaning on artificial intelligence to train their platforms to identify possible BEC messages.

Payment security providers like eftsure insert a gateway at a different point in the process, interfacing with payment systems to check that the account details of any submitted payment matches the details of the business registered to that account.

Other companies have pushed the importance of Domain-based Message Authentication, Reporting, and Conformance (DMARC), a DNS-based tool that identifies and blocks messages from spoofed domains before they even get to the company.

DMARC struggled to gain traction in its early years, but one recent PowerDMARC analysis found that 54 per cent of 140 company domains had DMARC records, and 18 per cent had their DMARC policy level set to the highest 'enforcement' level – meaning that noncompliant messages would be flat-out rejected or quarantined for further analysis.

Education, healthcare and banking providers were the most advanced in implementing DMARC – but as the ACSC's concerns about construction-industry BECs demonstrate, if one target proves too hard, thwarted cybercriminals will simply go elsewhere until they succeed.

'Don't be embarrassed if you fall victim,' says AFP Commander of Cybercrime Operations Chris Goldsmid, who advises companies to report suspected fraud to their bank and the police 'to give us the best chance of recovering your money'.

'It is reasonable to ask questions to protect yourself or your company.' •

Analysing Australia's response to Microsoft Exchange vulnerabilities

— BY EDWARD FARRELL, DIRECTOR, MERCURY INFORMATION SECURITY SERVICES —

As part of research activities, Mercury conducts regular digital reconnaissance and exploration to understand Australia's risk exposure to a number of threats. We use this information for our own professional understanding, as well as to shape and inform an appreciation among our customers.

Since March, our team has been analysing the responsiveness of Australian Internet Protocol version 4 (IPv4) addresses exposure of Microsoft's Outlook Web Access (OWA) instances. Mercury held the hypothesis that by capturing version numbers, we could gauge how rapidly Australian firms were updating systems. This has been occurring via our Open Source Intelligence infrastructure in Amazon Web Services, where we've been gathering the OWA version of individual hosts with a simple HTTP request to affected IP addresses. We'd performed similar hunts for MS17-010 in 2017 and again for Remote Desktop Protocol-related vulnerabilities in 2019. This is an awesome experience for my team and me in terms of engineering: thinking through how we are going to conduct our process, as well as take the temperature of vulnerability management in Australia.

VULNERABILITIES AND THE CONCEPT OF PATCHING

The most important thing to remember in cyber security is not that people are evil and want to destroy the world (as most unscrupulous cyber security vendors will tell us), but that people make mistakes. This is most clear in applications and software development; vendors are under pressure to get new releases out in a timely manner, and combined with common software flaws or even systemic issues in software development, vulnerabilities are going to be ever-present. This idea of making mistakes can be extended to patch management, either through forgetting to apply patches or through the fact that we don't resource patch management effectively.

Since the Australia Defence Signals Directorate – now the Australian Signals Directorate – released the top 35 strategies to mitigate targeted cyber intrusions in the early 2010s, patching applications and operating systems

has been critical to preventing intrusions. With exploit code typically being identified or openly available within 48 hours of a vulnerability being released, speed is now a critical factor in applying these patches. Any instance of exploitation of a vulnerability that leads to remote code execution can result in any number of outcomes, from cryptominers to ransomware, all the way through to targeted data collection by a threat actor.

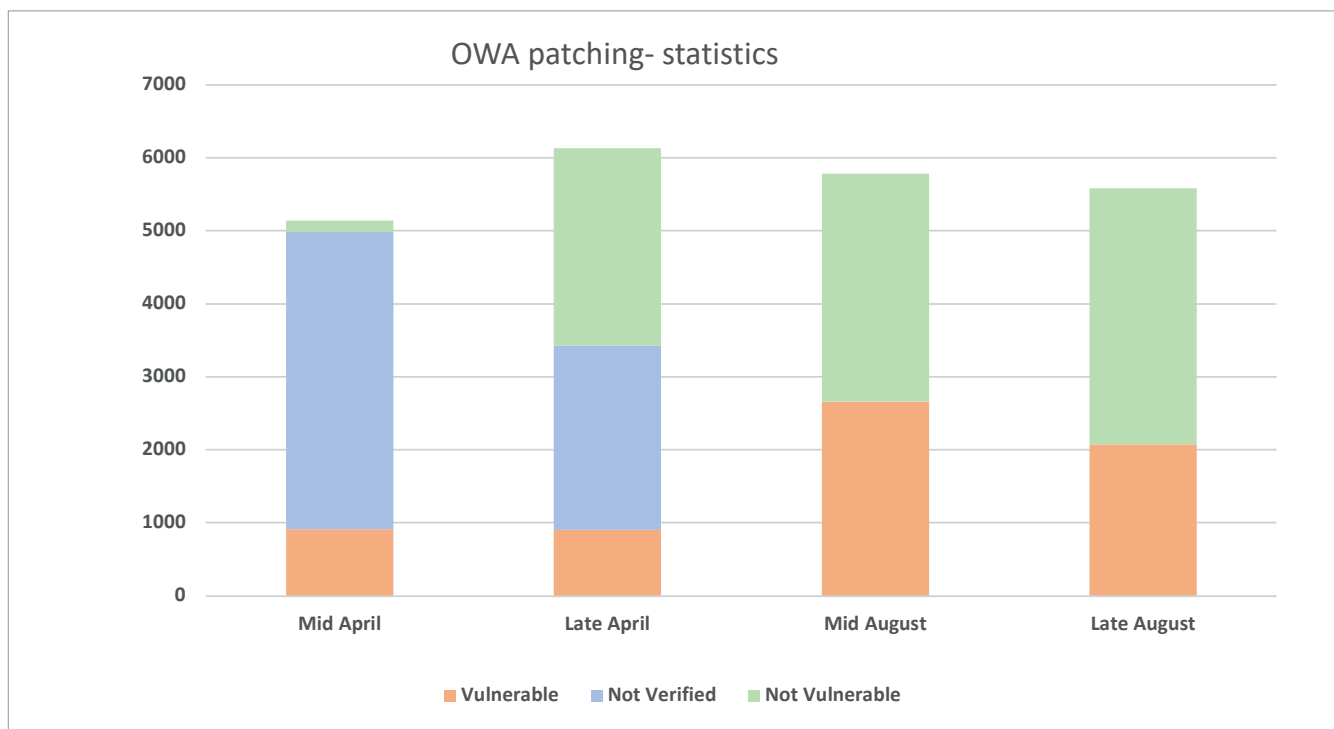
Our target vulnerabilities in this instance are a handful of issues disclosed in Microsoft Exchange throughout 2021.

The most important thing to remember in cyber security is not that people are evil and want to destroy the world (as most unscrupulous cyber security vendors will tell us), but that people make mistakes

HOW WE'VE BEEN PERFORMING AS A COUNTRY (BY THE NUMBERS)

Our analysis identified that in mid April (around 48 hours after the publication of CVE-2021-28482), there were approximately 8100 identifiable OWA instances based on a number of data points, including our own identification and several other resources. Of these, 158 were patched within the 48-hour time frame (around three per cent of the 5139 accessible instances).

An additional 911 were definitely vulnerable, and the remainder could not be accurately determined (based on



minor version numbers, where patches were released in March or at other times).

By late April, 2699 could be verified as patched. By August, and with the release of CVE-2021-34473 the month prior, the gap had evidently widened. By the time of our final analysis in late August, 63 per cent (3505) of accessible systems were patched. Another 17 per cent are definitely not applying patches; however, 25 per cent could very well be maintained. While system owners in Australia are patching, as a nation we're not patching at a high enough speed to outpace threat actors, and a number of systems are just not being maintained.

SOME OVERALL OBSERVATIONS AND ANALYSIS (QUALITATIVE)

Exploring most of these domains, very few government organisations, or even larger entities, are affected. Empirical analysis suggests that most of the affected hosts belong to smaller organisations that cannot afford cyber security services and, in the current STEM boom, are probably struggling to maintain human resources to sustain their existing technological environments.

Some interesting observations we've made in our dataset include the following:

- › *The good:* Micro and small enterprises are less likely to be affected, largely due to their use of Office365 or Google to host their email infrastructure.
- › *The bad:* One particular issue we did note was that a politically sensitive system was on the internet and exploitable; however, when we'd raised it via an intermediary, the issue was brushed off.
- › *The ugly:* A cyber security organisation of some note – resplendent with online talks, thought leadership, wonderful Gartner products and even 'attack threat surface mapping' expertise – had failed to identify their own system as vulnerable

for three months. While we will not name and shame, notwithstanding some sensitive clients highlighted on their website as organisations they support, we encourage anyone acquiring cyber security services (or any technology services) to evaluate service providers before entering multi-million-dollar contracts with them.

AS AN END NOTE

During our latest iteration, and inspired by our work with the CTI League (<https://cti-league.com/>), Mercury sought to identify healthcare infrastructure affected by this issue. We conducted outreach with the Australian Cyber Security Centre (ACSC) to engage and disclose to affected healthcare organisations, given their role in helping Australia during the COVID-19 pandemic. In our August sweep, we'd also collected Transport Layer Security certificates and some Domain Name System data to correlate affected systems, with a priority placed on health care.

We encourage anyone who is performing this sort of research to contribute to the effort and tie in with ACSC with reporting and information sharing. Our experience over the past seven years of research, and even in receiving information, is that the ACSC has been incredibly responsive to what we put forward, and is an effective coordinator. •

Edward Farrell is a security consultant with over 12 years' experience in information security and 17 years' experience in the IT industry. As Director of Mercury ISS – one of Australia's few remaining independent security firms – he has conducted or overseen the delivery of 500 security assessment activities and incident responses in the past five years. His professional highlights include lecturing at the Australian Defence Force Academy, being rated in the top 200 bug bounty hunters in 2015, and running an awesome team of security professionals.



Ransomware – reporting, payments and the other 98 per cent of businesses

BY GARRETT O'HARA, CHIEF TECHNOLOGY OFFICER, APAC, MIMICAST

'Time's up for the organised criminals who prey on our schools, hospitals, businesses and private citizens with this despicable technology.'

THAT WAS WHAT Minister for Home Affairs Karen Andrews said in July 2021 upon announcing Operation Orcus, a new government task force to counter ransomware – one that spans multiple government agencies.

This was followed up recently by the Australian Government's announcement of a Ransomware Action Plan which – among other measures – will compel organisations with annual turnover of more than \$10 million to report ransomware attacks.

While any government initiative to counter this growing, damaging and extremely costly form of criminality is to be welcomed, this is just one piece of an increasingly complex puzzle. Another huge piece of the puzzle is how to address the dilemma that faces every organisation hit with ransomware: to pay or not to pay?

Operation Orcus is one of several government initiatives targeting ransomware. In March, the government released a report, 'Locked Out: Tackling Australia's ransomware threat', putting the onus on businesses to protect themselves from ransomware and offering guidance on how to do so.

On the question of paying ransoms, the report says, 'Australian Cyber Security Centre's (ACSC's) advice regarding ransomware payment is clear – do not pay. Payment may be illegal under certain circumstances.'

When announcing the Ransomware Action Plan the Australian Government reiterated this by saying that it 'does not condone ransom payments being made to cybercriminals. Any ransom payment, small or large, fuels the ransomware business model, putting other Australians at risk. Paying ransoms does not guarantee access to locked systems or sensitive data, and may open the victim up to repeat attacks.'

Such warnings can be tough to heed for an organisation facing a very real prospect of extinction if it fails to pay. Further complicating the issue – as the Colonial Pipeline attack demonstrated – is the responsibility that a critical infrastructure organisation has to society as a whole.

Fuel supplies to much of the eastern United States were disrupted when Colonial was hit by ransomware. In an interview with *The Wall Street Journal*,

CEO Joseph Blount said that the decision to pay the ransom was 'the right thing to do for the country.'

Earlier this year the Australian Labor Party (ALP) released a report, 'Beyond The Blame Game Time for A National Ransomware Strategy', that called for a number of government initiatives to counter ransomware, including regulating the payment of ransoms by Australian organisations. The ALP followed this up in June when shadow assistant minister for cyber security, Tim Watts, introduced a private members' bill that would require organisations to notify the Australian Cyber Security Centre (ACSC) of any payments made in response to a ransomware attack.

The Federal Government Ransomware Action plan followed soon after, showing a recognition from both sides of politics that ransomware is only increasing in prominence and consequence.

Mandatory ransomware notification will be good for society. The lack of transparency is bad for everybody. Without regulations, organisations tend to do what is good for them in the moment, which may be

bad for society as a whole. That is what we have been seeing.

Without regulation, there's no reason for an organisation not to pay. It's cost-effective and it keeps the doors open. It can feel like the right sort of fiduciary decision. The only way to get away from that is regulation.

Mandatory reporting will enable us to really understand the size of the problem, and get a better insight into who ransomware actors are and where the ransoms are going. That should enable the government and everybody else to better tackle the problem.

Support for mandatory reporting and stronger government action against ransomware were two of the key themes to emerge from Mimecast's Cyber Resilience Executive Society Roundtable: To Pay or Not to Pay.

Increased Australian Government involvement in corporate ransomware response was identified as a key focus point, with one panel member saying the government 'needs to make a big leap in terms of communications' about ransomware risks and viable remediation strategies.

Spelling out that organisations also need to pull their weight, the panel agreed that better transparency around ransomware attacks, payments and remediation would help every Australian organisation better prepare for an attack.

In these respects, the Ransomware Action Plan is welcome, with the private sector keenly awaiting consultation on how it will be put into practice. The plan will need to ensure reporting of attacks and payments is constructed in such a way that it does not push instances of payment into the shadows for fear of punishment. Doing so will only maintain the status quo of payments going unreported and government – and industry – not being able to fully measure and tackle the problem.

The onus can't sit solely with government, as recent sluggish and potentially costly responses to ransomware attacks have shown. A properly implemented set of legislation will help right the balance in this respect.

TWO PER CENT – A GOOD START BUT DOES IT GO FAR ENOUGH?

Diving into the details of the Ransomware Action plan, mandating

that companies with turnover exceeding \$10 million must report attacks is at least a move in the right direction. But this accounts for less than two per cent of Australian businesses.

Ransomware is indeed a pandemic, so such a move can be likened to vaccinating only two per cent of the population against COVID-19. This would hardly be seen as a satisfactory result.

The larger organisations who are mandated to report ransomware will also logically have larger cyber security budgets and resources, which perhaps paints an even less clear picture of the true extent of the impact.

AWARENESS, UNDERSTANDING AND SMB SUPPORT – 'CYBERCARE'

Awareness and understanding are huge first steps in combatting ransomware. Governments have shown success with such mass awareness initiatives in the past – who doesn't remember the Cancer Council's 'Slip, Slop, Slap' campaign of the 1980s?

Such a cyber security campaign would lift awareness considerably and needs to be coupled with a cyber health program that encapsulates businesses of all sizes.

One approach that needs strong consideration is a small to medium-sized business (SMB) cyber health program. There is a huge opportunity for the private, public and tertiary sectors to build a service that is free for the first period of engagement. This would allow SMBs to have their cyber health diagnosed, gaps identified and measures put in place for them to achieve a certain standard of SMB cyber health without having to make an upfront investment.

Following this first engagement, ongoing support and health checks would be provided at a subsidised cost, much like essential health care is available to all Australians.

Think of it as 'cybercare'. There are economic benefits to focusing more on prevention, because – like health care – it provides cyber protection across the community and the economy, including in industries and sectors where SMBs, through lack of resources, can unwittingly be weak links in a supply chain's cyber security posture.

Awareness, training and the right regulation helps organisations and individuals – who we know are the easiest firewalls to get past – understand the enemy we are all up against.

TAKING ACTION AGAINST RANSOMWARE: KEY STEPS **Make sure cyber security is on the board's agenda**

A once-a-year check-in doesn't cut it. Frequent, regular deep dives will drive accountability, awareness and action. The chief information security officer (CISO) needs to be a member of the risk subcommittee. This will enable the board to get a better handle on the challenges and issues that directly affect their security risks, and gain more visibility into actions and investments needed to mitigate them.

Security awareness training needs to be driven from the top

Directors and senior executives shape culture through the policies and practices they follow, and by setting the right example through their own behaviour. Cyber-savvy leadership combined with relevant training can go a long way towards changing behaviours.

Regular internal communications

Give the CISO a regular internal voice to share security challenges that other organisations face to build an environment of awareness and vigilance.

Foster a cyber-aware company culture

This is key to building cyber resilience, and a strong culture isn't built overnight. It requires sustained effort and repetition, and a hard look at current practices. Most importantly, it needs to be inclusive and tailored to each organisation.

Cyber resilience

Layered protection and integrated security solutions are absolutely critical to minimise the chances of and fallout from a cyber attack. The right solutions to recover from an attack and continue business as usual are just as important as protective measures. With resilience, organisations can stack the ransomware odds in their favour. ●

Cyber security maturity: Australian business gets a pass mark, but can do better

— BY CRAIG BATY, PRINCIPAL, DATADRVN —

In February and March 2021, AISA collaborated with research and advisory firm DataDriven to conduct a major study of 120 Australian ICT decision-makers.



Craig Baty

The State of the Digital Nation: Cyber Security in Australia 2021 study looked at a range of information and communications technology (ICT) issues in the sector through the eyes of the people who manage and deliver these technologies – the ICT decision-makers. This is the second year that the Australian Information Security Association (AISA) and DataDriven

have conducted this study, and there are some interesting differences this year compared to 2020.

SECURITY IS A PRIORITY BUSINESS OBJECTIVE FOR BUSINESS LEADERS

A key finding of the survey is the centrality of security and related issues to Australian businesses.

Managing risk and cyber security ranks the third most important business objective in 2021, similar to its second-place ranking in 2020. Two-thirds (66 per cent) of respondents rate it an 'extremely high' or 'high' priority, compared to 63 per cent in 2020.

Improving all aspects of security also ranks in the top six business objectives, with 66 per cent of respondents rating it a high or extremely high priority. Security continues to become more of an issue across the whole business, rather than just for the ICT team.

Business leaders say they're also juggling a range of other objectives, including their number one priority of increasing productivity and collaboration (72 per cent of respondents). This was also the top business objective in 2020. Further priorities include increasing competitive advantage (66 per cent) and increasing the pace of innovation (65 per cent).

EIGHT OF THE TOP 10 ICT STRATEGIC CHALLENGES ARE TO DO WITH SECURITY

Cyber security is clearly the biggest issue facing Australia's ICT professionals (Figure 1). While 74 per cent of respondents say applications development is the top ICT strategic challenge, eight of the other top 10 challenges are directly concerned with cyber security or closely related to it (e.g., regulatory compliance, business continuity and privacy regulations).

Application security has jumped up the list of ICT strategic challenges, becoming the second-ranked challenge this year. This is connected to accelerating digital transformation across all industries as businesses rush to provide improved customer experience through better web and mobile apps. Businesses are hyper-aware that applications directly used by their customers must offer robust security and protect their data and privacy.

Network security is ranked the third-biggest challenge this year. Network security is rated a high or major challenge by more respondents (70 per cent) in 2021 than in 2020 (58 per cent). The scale of the network security challenge has grown due to the burgeoning extended networks businesses deployed to support working from home during the COVID-19 pandemic. Such networks were often hastily deployed and relied, in many cases, on employees' own end-user devices and routers. Businesses know they must harden these networks as the 'new normal' of work from home continues.

Data centre security fell in rank, from second in 2020 to 20th this year (even though it only fell by one percentage point in terms of being a major or high challenge). That's because other challenges increased more, relative to data centre security. This is underlined

by how cloud security has gone in the opposite direction (growing from 52 per cent to 64 per cent) as businesses continue with major cloud migration initiatives.

DEPLOYMENT AND INVESTMENT IN SECURITY PRODUCTS HAS RAMPED UP

Three-quarters of all respondents have implemented all 12 of the cyber security technologies we asked about – either as mature implementations, or ones that are underway or at pilot/ POC stage (Figure 2).

Nothing could be more a sign of the times than ransomware protection being the most widely implemented technology (84 per cent of organisations), and also the technology that will attract the heaviest investment over the next 12 months (84 per cent of respondents are investing).

Similarly, incident detection response and recovery is widely deployed (80 per cent) and is the second investment priority (84 per cent will make some investment), followed by zero-trust architecture (ZTA), which is used at 82 per cent of organisations, and which 79 per cent will invest in further during the next 12 months.

The other most widely deployed technologies include data encryption (83 per cent), antivirus/spyware/malware (82 per cent), blockchain for verification and identity management/authentication purposes, anti-money laundering and fraud prevention (both 80 per cent).

These deployments have generally gone up significantly compared to 2020. In 2020, data encryption was deployed by 76 per cent of respondents compared to 83 per cent in 2021, blockchain by 58 per cent of respondents compared to 80 per cent in 2021, and authentication/identity management by 71 per cent of respondents compared to 84 per cent in 2021. This growth trend is apparent across almost all cyber security technologies we researched, including the use of artificial intelligence in cyber security (63 per cent in 2020, 79 per cent now), fraud prevention (76 per cent in 2020, 80 per cent now) and biometrics (60 per cent in 2020, 77 per cent now).



Figure 1



Figure 2

YEAR-ON-YEAR (YOY) COMPARISON

In Figure 1, the table to the left of the chart compares the prominence of items this year and last year. The column headed '2021' shows the percentage of respondents who rated each topic a 'major' or 'high' challenge this year. The '2020' column shows the comparable result from last year's study. If the item wasn't included in 2020 that's denoted by 'x'. The 'Change' column shows how the result changed since 2020: a blue up-arrow denotes an increase in 2021, a red down-arrow indicates a decrease in 2021, '=' means no change.

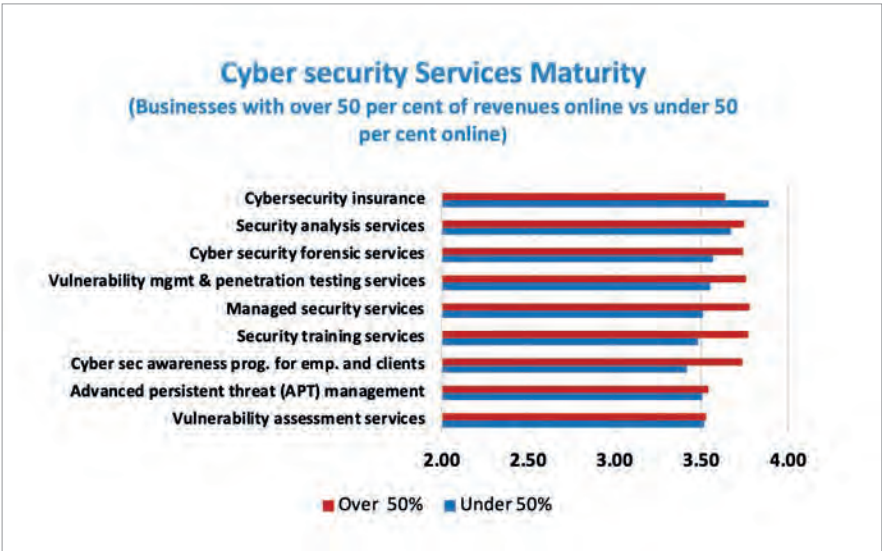


Figure 3



Figure 4

INVESTMENT TO IMPLEMENTATION (I²M) COMPARISON

Figure 2 shows the level of planned investment in the next 12 months for each technology (on the horizontal axis) and the current degree of implementation (vertical axis). The scale for both axes is 60 to 100 per cent (more than 60 per cent both plan investment in all technologies and have implemented all technologies). The cross-point of the axes is 80 per cent. The more a technology lies to the right, the higher the planned investment (e.g., 84 per cent plan to invest in ransomware); and the higher it is on the vertical axis, the more widespread the implementation (e.g., 84 per cent have already deployed ransomware). The important message of this chart is the relativity of the plots.

Despite widespread current deployment, it's clear that businesses understand they still need to invest more in cyber security to continue to address the growing magnitude of the risk. As a result, planned investments in cyber security technologies are also higher across the board in 2021 than in 2020. Of the seven cyber security technology items we researched in both 2020 and 2021, the planned investment in 2021

is higher by a margin of at least 22 percentage points, and extends up to 36 percentage points.

CYBER SECURITY SERVICES ARE ALSO SURGING

It's a similar picture with cyber security services. Figure 3 shows maturity based on the extent of deployment of these services.

The scale is a weighted scale from zero to five that reflects how extensive the deployment is for each service. Zero represents no deployment and five represents ubiquitous deployment. The chart also depicts maturity separately for businesses that do a majority of business online compared to those that generate a minority of revenues online. The red bars show the maturity level for organisations that generate 50 per cent and above of their revenues online (for shorthand, we'll call these 'ecommerce businesses'), and the blue bar depicts service maturity for businesses that derive less than 50 per cent of their revenues online (we'll call them 'offline businesses').

Ecommerce businesses are more mature in their use of cyber security services than offline businesses. This is true across all the services we researched except for cyber security insurance.

The results for related questions about cyber security technologies maturity, and backup and recovery technologies maturity are very similar; ecommerce businesses are more advanced in 10 out of 12 cyber security technologies we researched, and in all seven of the backup and recovery technologies.

The fact that offline businesses are more advanced in their use of cyber security insurance is congruent with the likelihood that they feel more at risk due to their generally lower cyber security technologies' maturity compared to ecommerce businesses.

The breakdown between ecommerce and offline businesses has changed markedly in a year (Figure 4). Respondents to this year's study are more advanced in generating online revenues. More than half (54.8 per cent) of 2021 respondents work for ecommerce organisations, while 45.2 per cent work for offline organisations. This is a significant growth compared to the 2020 survey, where only 31.7 per cent of respondents were ecommerce businesses, and is consistent with the move to online business during lengthy lockdowns and restrictions.



A CANARY IN THE COALMINE MOMENT?

Despite the positive findings that Australian businesses consider cyber security one of the top business priorities, have ramped up deployment of cyber security technologies and services, and plan to increase investment in the next 12 months, we do have one finding that is slightly concerning. A sizeable proportion of respondents perceive cyber security to be over-hyped, and also say it is unimportant. By contrast, respondents to the 2020 study were almost unanimous that cyber security was important, and did not believe it was over-hyped.

This is a potentially worrying finding, and is in contrast to cyber security's prominent ranking as a key business objective in this same survey. It's quite possible that some respondents have developed some 'security fatigue' given the repeated media and industry reporting on security threats.

This is perhaps a warning that cyber security, and ICT professionals and writers must communicate clearly and candidly about security threats. It's important to balance the message between honestly warning of the gravity of the threat while not using overly alarming language.

Despite the hint of security fatigue, the study shows that Australian ICT leaders grasp the magnitude of the current threats and take security

very seriously. They are treating cyber security as a priority for the whole business, not just for ICT. They have significantly increased deployment of security technologies, services and backup capabilities over the past 12 months, and they are ramping up their security investments heavily over the next 12 months to further protect and secure their infrastructure and assets. This is encouraging news given the continued rise in security incidents over the past year. •

.....
Craig Baty has extensive research and thought-leadership experience in the Asia-Pacific and Japan ICT markets. Baty is Principal and Founder of DataDriven, an Australia-based research and advisory firm specialising in research-based data-driven thought leadership, ICT strategy consulting for technology users and providers, outsourcing, vendor management, competitive intelligence, and technology go-to-market enablement projects. Baty has over 30 years of executive and board-level experience in the ICT industry, including as a Group VP and Head of Gartner Research APJ, CEO of Gartner Japan, Global VP of Frost & Sullivan, EGM Marketing and CTO of Fujitsu ANZ, GM Marketing Strategy and Alliances at BT Syntegra Australia, and more recently as VP Global Strategy and VP Digital Services in Fujitsu, Tokyo.

Defending against the ransomware explosion

BY MOREY HABER, CHIEF SECURITY OFFICER, BEYONDTRUST

RANSOMWARE SURGED

150 PER CENT in 2020, with 35 per cent of all breaches ransomware-related. In 2021, ransomware shows no signs of relenting, and Australian organisations remain prime targets for threat actors.

BeyondTrust's Malware Threat Report 2021 identified three significant ransomware trends:

1. proliferation of ransomware-as-a-service (RaaS) and ransomware kits on the dark web
2. a shift towards human-operated ransomware, which involves a mix of direct human intervention and tools
3. increasing use of native tools to perform fileless attacks in the initial stages.

THE ECONOMICS OF RANSOMWARE

Ransomware is highly successful from a return-on-investment perspective, because victims are paying up, often via their cyber insurers; however, the spate of ransomware payouts is prompting many cyber insurers to either steeply raise premiums or exit the market altogether. Insurers are also becoming much more stringent, requiring organisations to indicate, and even prove, that they have removed local admin rights for users and enforced least privilege across

their environment, to name just a few core requirements.

Of course, paying the ransom is no guarantee that an organisation will regain access to their data, and ransomware operators are also increasingly turning around and selling stolen data on the dark web.

THE RANSOMWARE BATTLEFIELD

The attack surface is ballooning with the acceleration of digital transformation and all things cloud. These technologies mean new planes of privileges that must be discovered, robustly managed and audited. Privilege, after all, is exploited in almost all cyber attacks, either to execute a piece of malware or to move laterally.

In addition, the explosion of remote working has multiplied the number of insecure remote access pathways. In 2020, 52 per cent of all ransomware attacks leveraged publicly accessible remote desktop protocol (RDP) servers to gain initial access. Today, RDP and virtual private networks (VPNs) are being stretched far beyond their legitimate use cases.

BOOSTING ENTERPRISE RANSOMWARE IMMUNITY

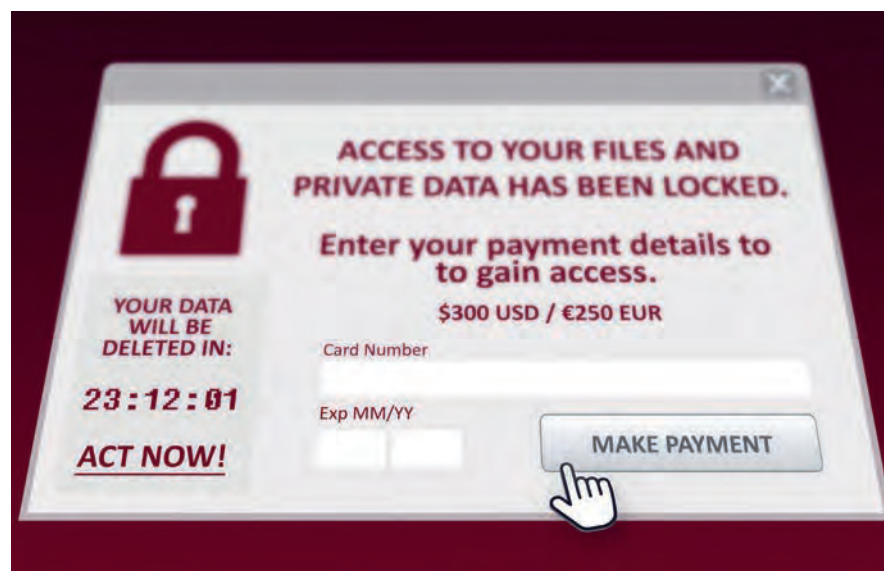
The following are some security steps every organisation should implement to protect against not



Morey Haber

only ransomware, but also a vast array of threats:

1. **Vulnerability management:** Assess risk, patch vulnerabilities in a timely manner, and/or implement other mitigations. Ransomware will frequently target known vulnerabilities to establish an initial foothold, or to propagate an attack.
2. **Privileged access management (PAM):** Secure remote access pathways, enforce least privilege (including removing admin rights), manage all privileged credentials and secrets, control applications, and monitor and manage every privileged session – whether involving a human, machine, employee or vendor. A strong PAM defence can not only prevent most ransomware outright, but can also mitigate an attack by impeding lateral movement and escalation of privileges.
3. **Backup and recovery:** Should an attacker ransom your systems, a robust backup program can condense downtime and eliminate the need to pay the ransom. Implementing these three security programs will not only minimise your exposure to ransomware and other threats, but will also enhance your ability to quickly recover from an attack. Finally, if all three are done correctly, you may potentially qualify for better cyber insurance coverage and rates. •





UNIVERSAL PRIVILEGE MANAGEMENT



Secure and protect privileges across
passwords, access, and endpoints to stop
data breaches and achieve compliance



Privileged Password
Management



Endpoint Privilege
Management



Secure Remote
Access



Cloud Privilege
Protection

beyondtrust.com

YOU'RE ONLY AS SECURE AS YOUR SOFTWARE SUPPLY CHAIN

— BY DAVID BRAUE —

Points of failure abound in the distributed cloud era.



In the pantheon of game-changing cyber security breaches, last year's hack of enterprise software vendor SolarWinds looms particularly large – not only because of the direct compromise of an estimated 18,000 of the company's customers, but also because the attack's stealth and persistence provided a stark reminder that fast-changing software supply chains are extremely vulnerable to compromise.

That hack saw suspected Russia-backed hackers insert malicious code into SolarWinds' software update engine, which dutifully distributed the malware to customers, installing what they believed were routine security patches and software updates to its Orion software.

The back-door approach was profoundly successful, sending US government agencies and large businesses like Microsoft, Cisco, Intel and Deloitte scrambling to assess what data may have been compromised during almost a year of active compromise.

Suggestions that software might be impacted by the implantation of malicious components are nothing new, but the SolarWinds attack's method – planting a Trojan horse inside a trusted system process – pointed to more systemic issues.

Contemporary computing environments introduce security issues when software is built not as a coherent whole, but as a constantly changing assemblage of interconnected software components.

Many of those components may be outside of the direct control of enterprise customers that often can't verify the integrity and security of components hosted on other companies' systems; enterprises trust that the services are secure, but only find out later that they inherited the exposure of vulnerabilities they could never have anticipated.

Such attacks often have a massive blast radius if they can infect a widely used service provider, with the July ransomware attack on a remote-management tool from network-management firm Kaseya hitting up to 1500 of its customers. The impact sent cybercriminals racing to find similar exploits, and sparked stern words between US President Joe Biden and Russian President Vladimir Putin.

SECURING THE COMPONENTISED ARCHITECTURE

In July, the European Union Agency for Cybersecurity predicted that supply chain attacks will quadruple this year compared with last year, 'posing an increasing risk for organisations'.

Those organisations have inherited supply chain vulnerabilities due to highly connected methods of modern software development, with 64 per cent of respondents to the recent Anchore 2021 Software Supply Chain Security Report stating that their



organisation was impacted by a software supply chain attack last year.

Sixty per cent said they have made securing the software supply chain a significant area of focus, particularly as they expand their use of application containers – modular application components that have found particular favour as foundation stones of scalable cloud services.

As if the tightly integrated, bespoke applications of yesteryear weren't exposed enough to malicious actors, today's distributed, loosely connected application components are a potential playground for hackers since each component can easily exist within hackable repositories on different systems, with different degrees of security.

Widely used open-source software (OSS) components have long been a particular concern since their code has been well-studied by cybercriminals, and these components can also often be modified in insecure ways when integrated into a third-party product.

In July, for example, SolarWinds was again patching a critical security vulnerability after Microsoft found a vulnerability in its Serv-U file transfer service tied to the way Serv-U implemented the open-source secure shell (SSH) protocol.

Even small mistakes in implementations can have major security implications, which is why 23 per cent of the Anchore respondents named OSS as their top container security challenge.

More worrying is the finding that many companies underestimate their use of OSS. Average estimates in this survey were that OSS components were 26 per cent of their total, around a third of the benchmark in previous studies.

'Open source doesn't mean more secure,' information security expert Bruce Schneier told this year's AISA CyberCon conference. 'Evaluated means more secure; you can hire a bunch of people to stare at your code, or you can have an open-source product where you throw it out there and hope that people take a look at it.'



‘But hope is a mediocre strategy,’ he added. ‘While high-profile pieces of code might get looked at, most open-source software is not looked at. It is not a magical way of making your things more secure; its security benefits can be just as risky as a closed-source offering.’

With fewer than half of companies following container security best practices – including scanning OSS containers and using private repositories to control dependencies – the finding that 84 per cent of respondents plan to increase

their container use is a red flag for companies seeking to minimise their supply chain exposure.

So, too, are reports that 86 per cent of companies have challenges in identifying vulnerabilities, 77 per cent report too many false positives, and 77 per cent report problems getting developers to spend the time needed to remediate security issues.

At a minimum, reducing supply chain risks requires a more coherent approach to container security, as well as awareness of the diversity of container platforms in use and each one’s security idiosyncrasies.

Anchore found that the more mature a company’s use of containers, the more likely it was to perceive that the architecture has a higher risk than conventional applications (38 per cent) compared to just 16 per cent of beginner users who felt the same way.

‘This likely arises from the fact that advanced users have a deeper understanding of the complex dependency chains that are common with containerised applications,’

the report notes. ‘They also better understand the need to adapt security processes and tools to adapt to unique container challenges.’

SECURITY WITHIN COMES FROM SECURITY THROUGHOUT

Supply chain vulnerabilities come in many forms, and as cybercriminals improve their circumvention of conventional controls, more attacks are likely to be discovered – with long-lasting and far-reaching consequences.

Authorities are, for example, still tracking the fallout from the compromise of Accellion file-transfer appliances late last year, in which the secure file-storage vendor repeatedly patched vulnerabilities that had led to data theft from organisations including ASIC, Transport for NSW, the Reserve Bank of New Zealand, airplane maker Bombardier, and Singtel.

By exploiting the fact that Accellion’s customers had moved large quantities of data into the company’s secure file-sharing servers, cybercriminals managed to completely circumvent the companies’ individual protections – highlighting a growing trend that, according to security firm F5, exploded during 2020.

Around 20 per cent of data breaches last year occurred due to third-party compromises, according to that firm’s 2021 Application Protection Report. Nearly all of these breaches were linked to ransomware attacks made possible when cybercriminals injected malware into the software ecosystem wherever they could.

Once inside, the malware spreads across connected nodes, giving cybercriminals a secure outpost from which they can steal company data and, eventually, launch a ransomware attack on the victim company that can easily spread to that company’s customers, as well. This was seen in the recent ransomware attack on cloud services provider Blackbaud.

Widespread use of common components has blurred the once conceptual boundaries between industry sectors, leading F5 to avoid suggesting that particular sectors are more vulnerable than others.

Given that players in every industry are now storing data in common third-party services and sourcing application components that are also used by very different businesses, F5 advises, ‘Sectors are no longer a good predictor of information risk... What attackers care about is target parameters – the kind of system running and the kind of data stored on that system.’

The report warns, ‘As digital transformation drives enterprise environments to look similar, and more manufacturers or wholesale merchants look to implement ecommerce platforms and sell direct to consumers, this is no longer the case. If you act like retail, you’ll get attacked like retail.’ ●



Tesseract: a homegrown success story

TESSERENT (ASX: TNT) is an extraordinary homegrown cyber security success story. Founded in Melbourne, originally focusing on managed security services and funded almost entirely by local investors, Tesseract has since grown to become Australia's number one ASX-listed cyber security provider. Now with offices across Australia and New Zealand, Tesseract partners with clients to provide not just managed security services, but also a full suite of cyber security services.

Listed on the ASX All Tech and All Ordinaries indexes, Tesseract is a truly local stock. Growing to almost 400 cyber security professionals, Tesseract has been transformed through the bringing together of carefully chosen local companies – all success stories in their own right: Rivium, Pure Security, North Security, Seer Security, Airloom, Ludus Security, iQ3, Lateral Security, Secure Logic and Loop Secure.

Partnering with more than 1000 clients – from mid-sized to enterprise, government and critical infrastructure companies – Tesseract delivers comprehensive, tailored solutions to prevent, detect and

mitigate potential cyber attacks. Tesseract provides deep expertise in security advisory (GRC) and consulting, technical assurance and testing, cloud services, 24x7 managed services and monitoring, incident response and forensics, and converged/physical security.

'Our success has largely been through the collaborative, partnership approach we take with our clients. Through our end-to-end cyber security offerings, we can become a vital extension of their teams and assist from the basement to the boardroom,' enthuses Kurt Hansen, Co-CEO, Tesseract.

The company recently launched two new divisions. The Tesseract Academy will tackle the industry-wide problem of talent shortages, improve the cyber ecosystem, and develop talent for both Tesseract and its customers. The new Tesseract Innovation division is already making strategic investments in proprietary Australian and New Zealand-based companies and products, including blockchain and biometric solutions, further boosting its sovereign cyber security capability.

Critical to Tesseract's success are its people: a team of highly skilled, multicultural, diverse, industry-recognised and leading cyber security practitioners. Tesseract is rated by its staff as equal to some of the most desirable tech companies in the world to work for¹, with a high Employee Net Promoter Score (eNPS). Employees consistently recommend Tesseract as a great place to work.

Tesseract is uniquely positioned to provide: an opportunity for local investors looking to capitalise on the growth in the cyber security industry, a dynamic and successful work environment for cyber security practitioners to build their careers, and a true partner for those organisations looking for assistance with the protection of their digital assets. ●

For more information, visit www.tesseract.com.

1. Benchmarked against 'New Tech 2020' – a group of more than 650 global tech companies who also work with Culture Amp as their survey partner.



Securing
our digital future,
together.

Comprehensive Cybersecurity Solutions

We start by listening.
Talk with one of our security consultants today:

www.tesseract.com
info@tesseract.com
1300 031 337

The region's largest ASX-listed cybersecurity company (ASX:TNT)

Melbourne | Sydney | Canberra | Brisbane | Wellington | Auckland | Christchurch





FROM SECURITY-ENHANCED 5G NETWORKS TO SECURITY-BY-DESIGN 6G SYSTEMS

— BY DR DAVID SOLDANI, CISO, RAKUTEN SYMPHONY —

The fifth generation of mobile communication systems is expanding across the world, adding new possibilities and interest beyond core.

As of June 2021, GSMA Intelligence reported that more than 170 operators have already launched commercial 5G services and more than 60 carriers have announced plans to launch them, having received spectrum across low (≤ 1 GHz), mid (≈ 1 –6 GHz) and high bands (≥ 6 GHz), most of them in the Asia Pacific and Europe.

Dell'Oro Group believes Open Radio Access Network (Open RAN) revenues will account for more than 10 per cent of the overall RAN market by 2025. In its Mobile RAN 5-Year Forecast Report, Dell'Oro highlights that the unexpected RAN surge is primarily driven by 5G New Radio (NR). By 2025, 5G NR RAN revenues are forecast to approach \$150–200 billion, cumulative 2020–2025 base station shipments will surpass 30 million, and RAN revenues are on track to reach a quarter of a trillion US dollars.

According to the Global Mobile Suppliers Association (GSA), the number of announced 5G devices continues to grow and has now risen to 991, of which 608 are commercially available. By the end of August 2021, GSA had identified more than 470 smartphones, 170 fixed wireless access customer premise equipment devices (indoor and outdoor), 130 modules, 60 modems, 40 hotspots, 20 notebooks and tablets, and 30 other devices (including drones, TVs, vehicle on-board units, etc.).

5G SECURITY CONTROLS AND ASSURANCE

In 5G, the Extensible Authentication Protocol – Authentication and Key Agreement and the 5G Authentication and Key Agreement are used for non-3GPP and 3GPP-authorized access, respectively. Those

procedures allow the mutual authentication between the UE and the network, based on a secret (shared) master key stored in the Universal Subscriber Identity Module and in the 5G core network. The user's privacy is preserved by concealing the globally unique 5G Subscription Permanent Identifier, which can be either in the format of International Mobile Subscriber Identity or presented as a Network Access Identifier.

Moreover, 5G supports security controls for non-public networks; security features for service-based interfaces, transport layer security and token-based authorisation; authentication and key management for applications, such as Internet of Things (IoT) over 5G; and network slice-specific authentication and authorisation.

5G will further evolve the user plane integrity; authentication functions; security controls for rogue base stations, slice enhancement, private networks, multi-access edge computing, and terrestrial and aerial manned and unmanned vehicles; and broadcast channels.

Moreover, 5G supports security assurance requirements and test cases for radio access and core network, data analytics, interworking, and service communication proxy functions, among other functionalities.

SECURITY IN OPEN RAN

The security architecture is further fortified for disaggregated and virtualised RAN (Open RAN). The Open RAN network is cloud native, typically with network functions implemented as containerised microservices.

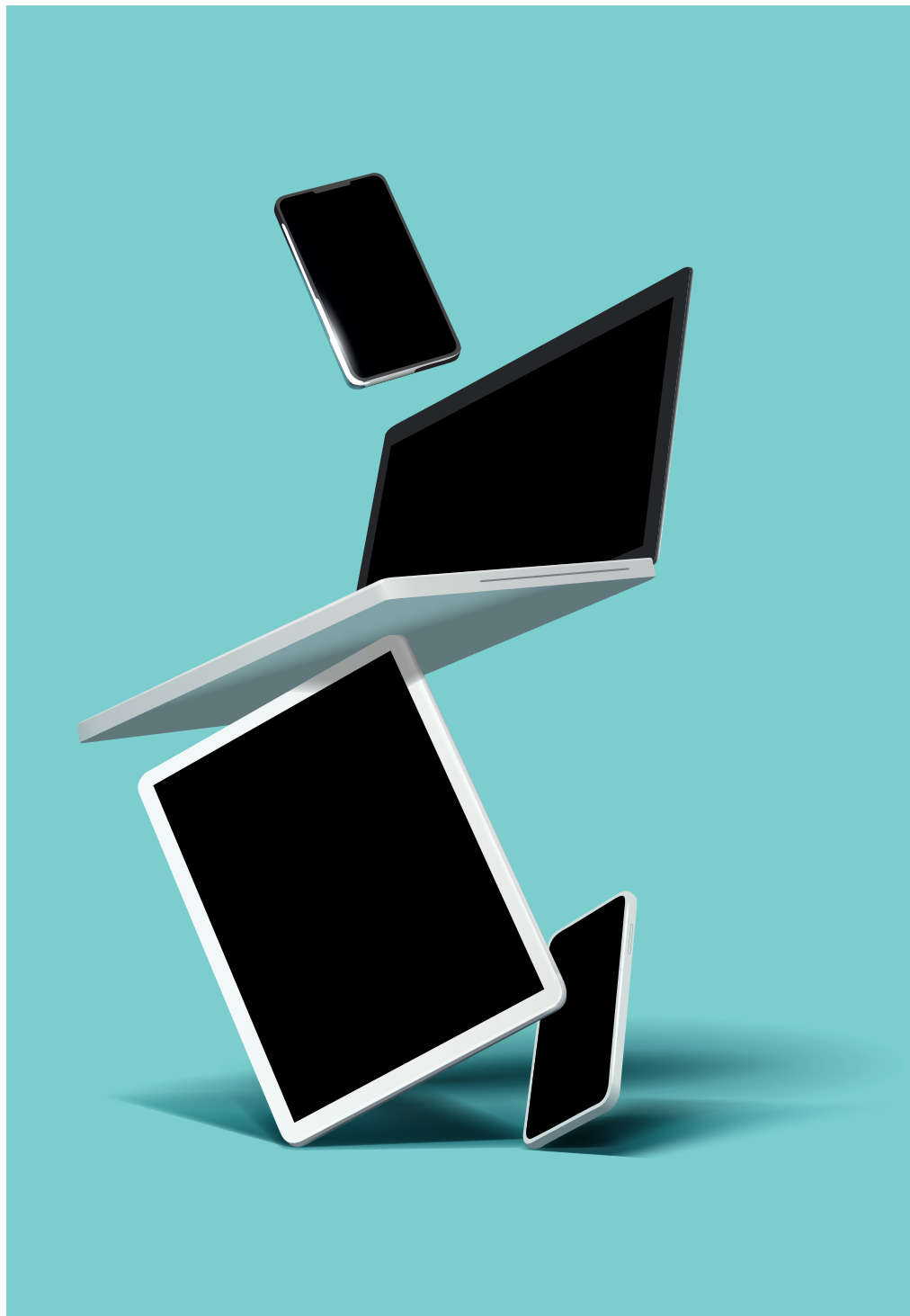
Open RAN security is built on the following tenets: secured communication between network functions, secure framework for the radio intelligent controller, and secured platform for hosting the network functions.

To support a zero-trust model, O-RAN ALLIANCE has identified several guiding principles for its ongoing work, including supporting integration with an external identity, credential and access management system using industry standard protocols; requiring authentication and authorisation on all access; supporting role-based access control; implementing

confidentiality on connections between Open RAN and external components; implementing integrity checking on connections between Open RAN and external components; supporting encryption of data at rest; supporting replay prevention; implementing security log generation and collection to an external security information; and event management.

6G GAINING MOMENTUM

Although 6G is likely to go live around 2030, the number of 6G initiatives underway globally and corresponding investments offer an intriguing prospect for the future. The requirements likely demanded by 6G include as yet unfulfilled 5G use cases and more advanced scenarios emerging for next-generation/6G networks. Examples of



such emerging scenarios include terahertz frequencies, holoportation, tactile/haptic communications, ubiquitous services (land, air, space and sea), imaging and sensing.

In Europe, the European Commission, within the Smart Network and Services framework program, has proposed a €900 million budget to invest in 6G research, with particular attention to standardisation leadership. Beyond that, Japan, Australia, the United States, the United Kingdom, Finland, South Korea and China have each allocated a huge budget to conduct their own research, and there is pressure on other nations to join.

6G wireless aims to bridge the ‘physical’ and ‘cyber’ worlds, shifting from connected people and things to connected intelligence. In short, 6G wireless is the technology to realise the fundamental paradigm shift from IoT to the internet of intelligence, the latter being defined as functions with the ability to represent knowledge, process knowledge and make decisions.

PRIVACY PRESERVATION, SECURITY CONTROLS AND ASSURANCE

In general, 6G wireless is projected to be secure by design. To shift from a security-enhanced network to a security-by-design system, 6G needs to integrate security at the heart of the infrastructure and instil the whole network, end to end, with a defence-in-depth strategy. Also, the standardisation process for 6G must provide new mechanisms for security control, security assurance and privacy preservation.

As communication networks evolve, it is expected that there will be increased reliance on artificial intelligence-enabled smart applications requiring situational, context-aware and customised privacy solutions. Hence, the 5G privacy-preserving approach may not be well-suited for future wireless applications due to a diverse and complex set of novel privacy challenges.

One potential solution is the use of pairs of deep neural networks, which can be trained with differential privacy, a formal privacy framework that limits the likelihood that queries of personal identifiable information – sensitive data that can include, for example, the full name of a person, their social security number, driver’s licence, financial information, medical records, etc. – could identify a real data subject.

The concepts related to federated learning (FL) are also active topics in the research community for ensuring privacy protection. FL is a distributed machine learning technique that allows model training for large amounts of data generated locally; the required modelling is done by each individual learner in the federation. Instead of sending a raw training dataset, each individual learner transmits their local model to an ‘aggregator’ to build a global model.

The 5G security architecture, features and protocols simply enhance the mechanisms that constitute the 4G

security posture, and 6G is expected to go well beyond that. For example, 6G wireless is expected to support, but not be limited to, the following security controls and assurance mechanisms:

- › *Zero-trust architectures*: no asset is trusted implicitly, and continuous access control, authentication and identification are used.
- › *Distributed ledger technologies*: immutable, transparent and autonomous ledgers using distributed consensus and cryptography provide an authoritative record of secure transactions.
- › *Post-quantum cryptography*: creating quantum-resistant ciphers that future quantum computers cannot crack.
- › *Adversarial machine learning*: better evaluate machine learning algorithm’s robustness and the development of defences against attacks.
- › *Cyber resiliency*: continuous detection and appropriate response to adverse events, and the ability to withstand attacks, and autonomously evolve and adapt to threats.

The GSMA Network Equipment Security Assurance Scheme (NESAS) should include O-RAN security assurance specifications, and industry players, governments, security agencies and regulators are encouraged to adopt the GSMA NESAS for testing and evaluating telecommunications equipment. The NESAS is an authoritative, unified and constantly evolving security assurance scheme for the mobile industry, and could be a part of certification and accreditation processes for current 5G and future 6G network security authorisation in any country. •

For more information on 6G fundamentals, visit <https://jtde.telsoc.org/index.php/jtde/article/view/418>

David Soldani received a Master of Science degree in engineering with full marks and a magna cum laude approbatur from the University of Florence, Italy, in 1994. He also holds a Doctor of Science in technology, with distinction, from Helsinki University of Technology, Finland, which he attained in 2006.

In 2014, 2016 and 2018, he was appointed Visiting Professor, Industry Professor and Adjunct Professor at the University of Surrey, the University of Technology Sydney and the University of New South Wales, respectively.

Dr Soldani is currently at Rakuten Symphony serving as Chief Information and Security Officer, e2e, Global. Prior to that, he was Chief Technology and Cyber Security Officer within the Asia-Pacific region at Huawei; Head of 5G Technology, e2e, Global, at Nokia; and Head of Central Research Institute and VP Strategic Research and Innovation in Europe at Huawei European Research Centre.

Dr Soldani can be reached online at www.linkedin.com/in/dr-david-soldani/





THE INTERNET OF THINGS – ARE WE PREPARED FOR IT?

— BY MANDI JACOBSON, PARTNER, AND ANGELL ZHANG, SENIOR ASSOCIATE, HOGAN LOVELLS AUSTRALIA —

‘Unfortunately, no-one can be told what IoT really is. You have to see it for yourself.’

Picture this: a dystopian future where humans are controlled by a system created by intelligent machines and are used for their energy. We’ve just described the film *The Matrix*; but in modern terms, that artificial intelligence would be regulated as, among others, an Internet of Things (IoT) technology.

Just as no-one can be told what *The Matrix* really is, the same can almost be said about IoT. There is presently no definition of IoT. Generally speaking, IoT essentially uses software to connect physical devices to the internet or to one another, and has a vast range of applications. The Australian Competition and Consumer Commission’s Digital Platforms Inquiry: Final Report (26 July 2019)¹ noted that the Organisation for Economic Co-operation and Development generally classifies IoT products into three broad categories:

1. wearables, health monitors and implantable devices
2. smart home applications
3. connected vehicles.



Mandi Jacobson



Angell Zhang

¹ <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>

It is estimated that by 2030, there will be more than 21 billion IoT devices connected to the internet globally, with the highest estimations predicting over 64 billion devices.² The expansion of IoT devices creates a more complex ecosystem, particularly when dealing with cyber security threats.

In fact, earlier this year the Australian Government opened consultation on the options for regulatory reforms and voluntary incentives to strengthen the cyber security of Australia's digital economy. As part of that consultation, many stakeholders noted that the more new internet-connected technologies come online, the harder the digital economy will become to defend.³

In September 2020, the Australian Government released the voluntary Code of Practice: Securing the Internet of Things for Consumers (the Code). In March 2021, six months after the Code's introduction, it was revealed that very few businesses had implemented the principles-based guidance introduced by the Code.⁴

It appears that Australia is falling behind its international counterparts that have moved from voluntary to mandatory measures in the requirement for manufacturers of IoT devices to have basic cyber security features.

Until IoT security is given adequate attention, many IoT devices risk falling short of adequate security measures. In turn, this compromises the privacy and security of Australian consumers. Many Australian regulators have faced the same issue. The Australian Information Commissioner previously identified that across the board, Australian users are not being adequately informed about how their personal information is being collected, used and disclosed.

Other Australian regulators have taken active steps to embed user safety into the design and functionality of IoT products and services. For example, the eSafety Commissioner, Australia's national independent regulator for online safety, has published an overview of its Safety by Design initiative, including information about the Safety by Design Framework (SbD Framework) and Safety by Design Principles (SbD Principles). The SbD Framework aims to assist organisations as they embed the rights of users and user safety into the design and functionality of products and services. The SbD Principles incorporate user safety as a fundamental design principle that needs to be embedded in the development of technological innovations from the start.

We will have to see for ourselves how the evolving landscape of IoT will develop in the coming years.

² *Code of Practice, Securing the Internet of Things for Consumers (Code)*

³ *A Call for Views: Strengthening Australia's Cyber Security Regulations and Incentives*, page 6

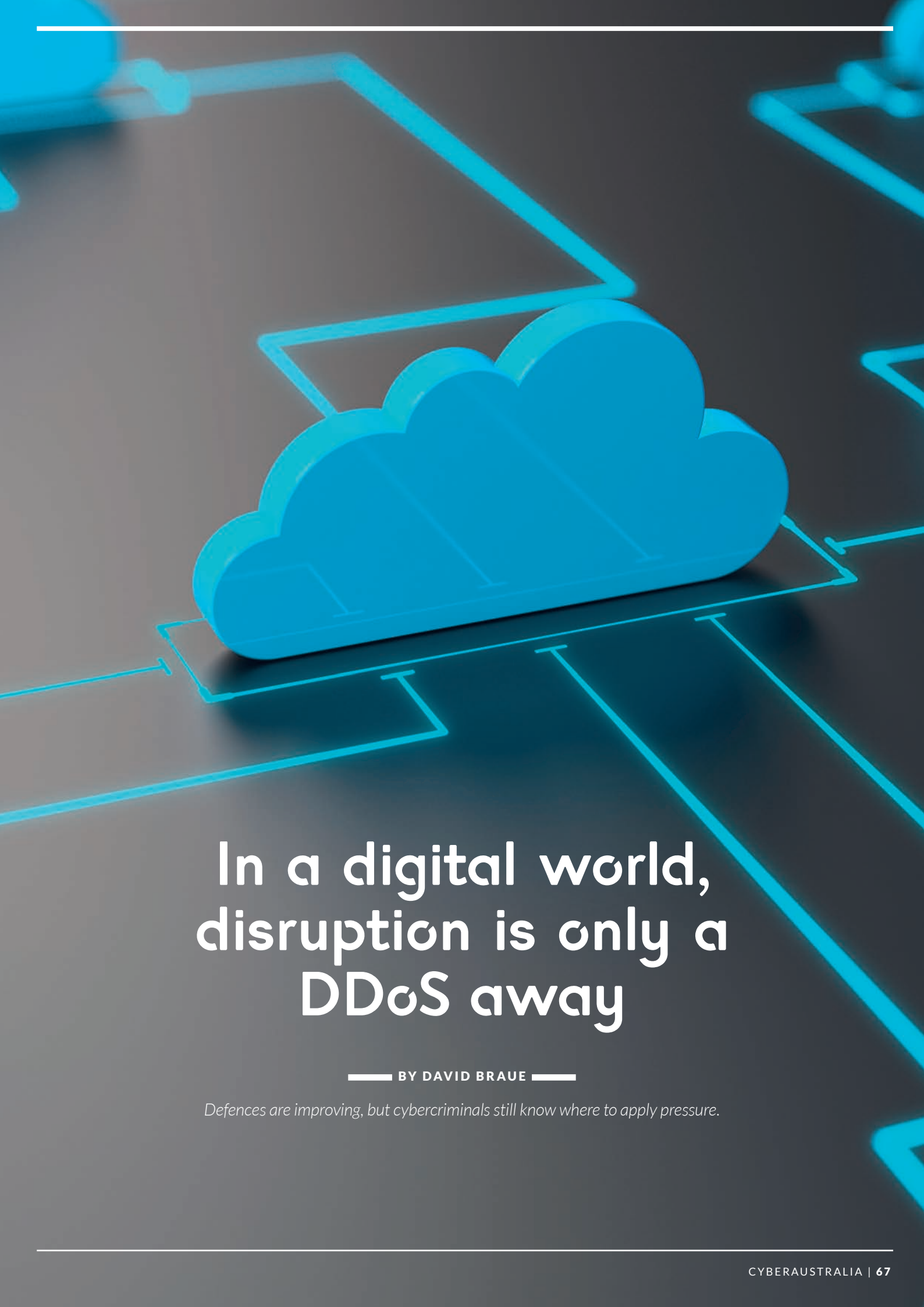
⁴ *Code*, page 31



Until that time, trust in the cyber security and privacy protection measures of IoT devices will likely remain a significant obstacle in the advancement of IoT devices. ●

Mandi Jacobson is a Partner at Hogan Lovells in Australia, and provides both advisory and litigation support to her clients. She advises on data, privacy and cyber security issues for a range of companies, in sectors such as life sciences (pharmaceuticals and medical devices), food and beverage, cosmetics, industrial chemicals and automotive. Jacobson also advises on compliance with therapeutic goods legislation; Therapeutic Goods Administration audits, registrations and listings; regulatory investigations; product liability; import and export requirements; and quarantine laws.

Angell Zhang is a Senior Associate at Hogan Lovells in Australia. She advises clients across a variety of sectors, including health, technology and ecommerce. Zhang develops global privacy and cyber security strategies, as well as international transfer strategies, for a range of major international and domestic companies, and advises on a range of privacy and cyber security issues.



In a digital world, disruption is only a DDoS away

— BY DAVID BRAUE —

Defences are improving, but cybercriminals still know where to apply pressure.

There were more than a few crossed fingers in August as application architects at the Australian Bureau of Statistics (ABS), with memories of its disastrous 2016 Census still fresh, flipped the switch on the completely rewritten online interface for the 2021 Census.

Unlike last time – when a series of distributed denial-of-service (DDoS) attacks took down the Census website during its night-time peak – the 2021 event went off smoothly, suggesting both that the ABS had learnt a hard lesson that it was determined not to repeat and that application design has matured substantially during the intervening five years.

Months of careful scrutiny of the application's design, engagement of ethical hackers to stress-test the infrastructure through its various iterations and construction of careful anti-DDoS defences proved that the risk of business interruption from such attacks can be effectively mitigated.

Such caution has become par for the course, particularly in a pandemic-era climate of digital transformation in which companies' very livelihoods depend on keeping their digital storefronts and customer-service systems continuously available.

Those systems were being built and deployed against the background noise of near-continuous DDoS campaigns, with a recent ISACA survey showing that 41 per cent of Australian and New Zealand (ANZ) organisations had seen an increase in cyberattacks on their organisation over the last year – and that 11 per cent had been hit by a DDoS attack.

The intensity of DDoS attacks has particularly increased against ANZ companies, with a recent Imperva analysis finding that the two countries comprised seven per cent of application DDoS attacks during the first half of 2021 – with Australia ranking the third most targeted country globally, and New Zealand the sixth.

Cyber criminals clearly sense new opportunities to disrupt ANZ digital services, punching the two countries

well above their weight and creating an immediate threat of business interruption that requires a careful and robust response.

Australia's high ranking as a DDoS target stems in part from local companies' strong embrace of DevOps tools and practices to meet accelerated digital-transformation timeframes that have pushed them into 'building and deploying more applications at a faster rate than ever before', says Imperva Asia-Pacific CTO Reinhart Hansen.

'The cybercriminal groups that use more advanced application layer DDoS attacks usually have a more sophisticated mindset and skill set,' he explains, noting that the groups' members 'typically have strong software development skills and the know-how to build highly targeted attack tooling' tailor-made for the 'vast increase in application surface' that the DevOps investment had created.

JOINING THE ARSENAL

For many years, DDoS architects seemed caught in a sort of arms race, competing to set ever-bigger records for DDoS attacks coordinated through the takeover of ever-increasing numbers of connected computers – and, in the case of the Mirai malware, connected Internet of Things (IoT) devices.

Defending against DDoS attacks has gotten harder not only because of the creativity of attackers, but also because widespread digital transformation has expanded the number of attack surfaces that must be defended, writes Google Threat Analysis Group (TAG) Security Reliability Engineer Damian Menscher. 'Multiplying the dozens of attack types by the diversity of infrastructure that must be defended leads to endless possibilities,' he adds.

The largest DDoS attack ever recorded, which was targeted at Google's online services and occurred in September 2017, was only revealed in late 2020, as TAG shared details of how it successfully blocked an attack that it attributed to China-sponsored nation-state actors.

Those attackers spent six months harvesting a range of attack vectors, ultimately pretending they were Google and using several different networks to pump 167 million packets per second of data to 180,000 exposed internet servers. These servers dutifully sent massive volumes of confirmation messages back to Google Cloud servers.

It was similar to the approach that took down the 2016 Census, but subsequent global efforts on the anti-DDoS front prevented the attacks from compromising Google Cloud's availability.

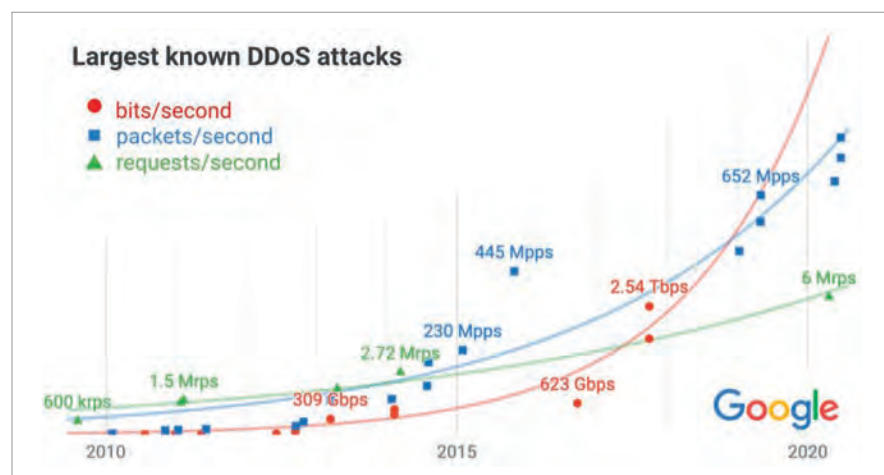
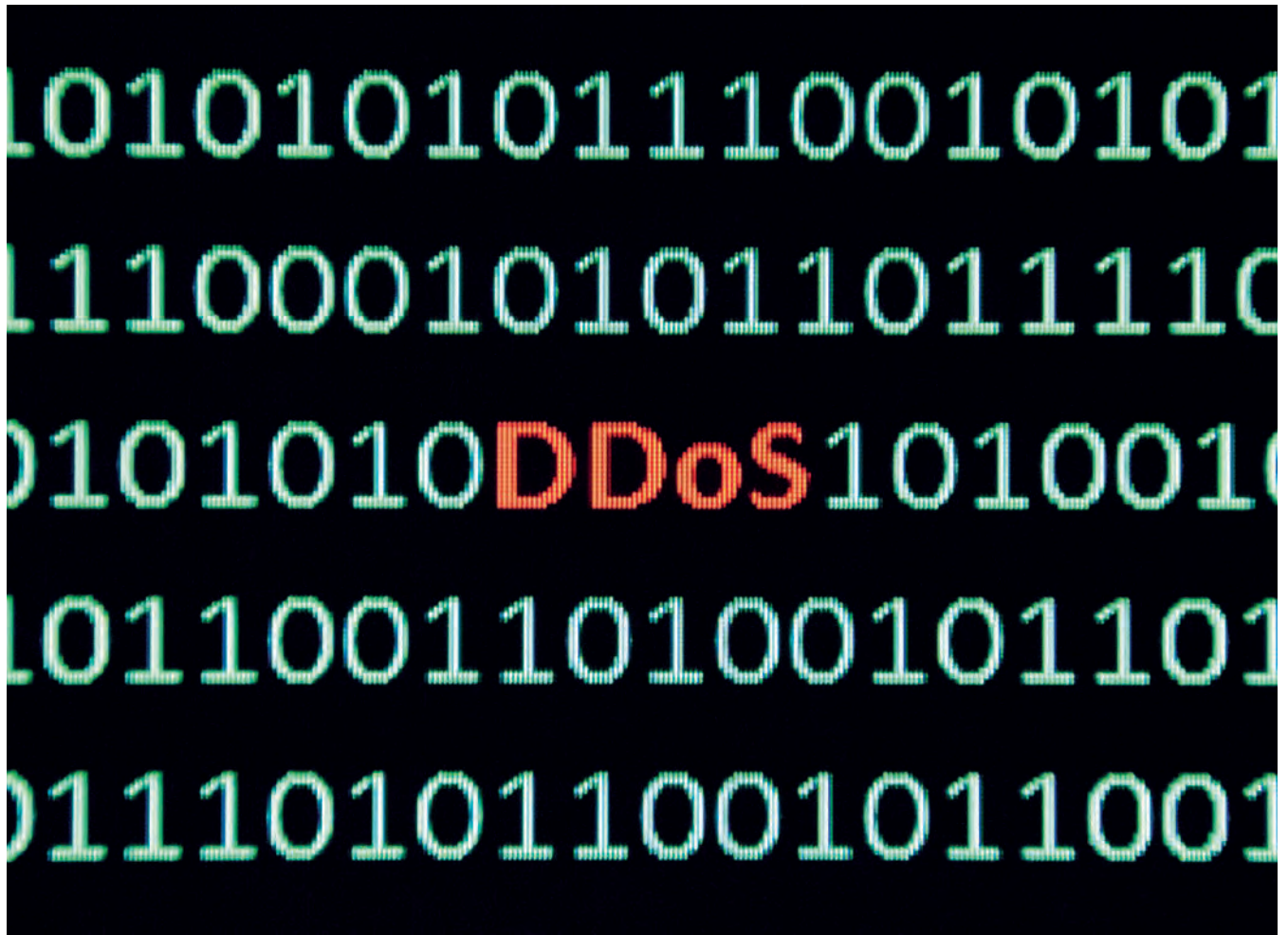


Figure 1. Credit: Google Cloud



The TAG team groups attacks based on three key metrics: network bits per second targeting network links, network packets per second targeting network equipment or DNS servers, and HTTP(s) requests per second targeting application servers.

Each group can be addressed using different families of tools, with new services such as Google's Cloud Armor Managed Protection and Cloud Load Balancing supporting a layered defence that has proven effective in blocking even large-scale DDoS attacks.

Other operators of large-scale cloud and interconnection services have added additional layers to the anti-DDoS arsenal, providing a range of options for businesses and government bodies eager to protect themselves from this time-honoured attack.

'Addressing state-sponsored DDoS attacks requires a coordinated response from the internet community,' writes Google's Director of Software Engineering, Shane Huntley. 'We work with others to identify and dismantle infrastructure used to conduct attacks.'

HOLDING COMPANIES TO RANSOM

Widespread cooperation by infrastructure operators has helped to blunt the immediate force of DDoS attacks, with anti-DDoS services blocking many attacks before they get anywhere near a network.

Yet, targeted DDoS attacks are still out there, with another Imperva analysis finding that the number of requests per second levelled at financial services providers tripled between April and June of this year.

Worryingly, DDoS actors are joining forces with ransomware artists for a new type of threat called a ransom denial of service (RDoS) attack, in which companies infected by ransomware are threatened with a massive DDoS attack if they don't meet the ransom demands.

RDoS attacks, combined with equally problematic threats to publish or sell sensitive stolen data on dark web sites – and with threats to slander the victim's reputation by informing partners, suppliers and customers that the company has been breached – have become the core elements of 'quadruple extortion' attacks that are taking ransomware to a whole new level.

These disturbing attacks popped up with increasing frequency as consultants within Palo Alto Networks' Unit 42 security arm worked with ransomware victims in the first half of this year, noting that the four-layer attack represents a significant escalation from the double extortion attacks that became widespread during 2020.

'As they've adopted these new extortion approaches, ransomware gangs have gotten greedier,' the specialists said, noting that average ransom demands have increased 518 per cent compared with last year.

Weaponised in this way, DDoS attacks have become a problematic part of an even bigger problem, making it more important than ever that companies work with their security providers to finalise and test DDoS defence tactics well before they're needed. ●



Empower your organisation to safeguard information to ensure information resilience

INFORMATION SECURITY AND the protection of privacy is of utmost importance for every organisation regardless of the size or scope. We all have an obligation to protect our information, as well as the information of our clients.

BSI's global expertise and services enable organisations to better respond to cyberthreats, and build more resilience around critical information and IT infrastructure, protecting their information, people, and reputation.

We enable a state of enhanced and sustainable information resilience through our services in the areas of information security management and training.

For organisations to protect themselves from cyber risks, it's essential to really understand what's to be protected, and make sure that those aspects are configured securely, and that people understand their roles and responsibilities in

order to protect the reputation of the organisation.

Untrained or 'unrefreshed' employees are the weakest link in your cyber security defence. According to research, 91 per cent of cyber attacks start with a phishing email.¹ BSI provides a flexible range of information and cyber security training modules and courses that help to ensure your weakest link becomes your strongest asset in remaining vigilant and resilient to the omnipresent threats. Available online, on demand, in house or as classroom-based sessions, BSI's training portfolio can help to embed information security best practice into your organisation.

Global best practice and training needs can be embedded across the entire organisation – from the leadership team and system owners, to end users – as everyone plays a role in information security. You must be aware of the needs and knowledge of

your staff, your people, your supply chain and your stakeholders to be able to mitigate risks to data. Your organisation can prepare by ensuring you have the right training programs in place.

We are committed to inspiring trust for a resilient world in everything that we do, and a part of that is facilitating training and tools to do that in an efficient matter so that organisations make protecting people and information a priority.

Ready to commit to information resilience and educating your people? Contact our experts to talk about our training programs. •

For more information, call 1300 730 134, email info.aus@bsigroup.com, or visit bsigroup.com/en-au

1. <https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email>



Protect your business, people and your reputation.

Empower your organization to safeguard its information – physical, digital and intellectual property – throughout its lifecycle from source to destruction by adopting information security-minded practices so you can protect your business and your people.

BSI can support your organization's information resilience by addressing these key areas:

- Cybersecurity
- Information management and privacy
- Security awareness and training
- Compliance to requirements

**Contact our experts to
find out how.**

call 1300 730 134

email info.aus@bsigroup.com

visit bsigroup.com/en-au

bsi.

Inspiring trust for a
more resilient world

A glowing blue brain is positioned at the bottom of the page, surrounded by a circular light effect. Above the brain, a series of light rays and data points descend from a glowing circular interface at the top, creating a sense of digital flow and connectivity. The background is a deep blue with subtle patterns of light and data points.

Artificial intelligence for cyber security: new solutions, but also new risks

— BY DR CHRIS EWIN, LECTURER, SCHOOL OF COMPUTING AND
INFORMATION SYSTEMS, UNIVERSITY OF MELBOURNE —

This year marks the 50th anniversary of the Creeper computer program, which first spread through the Advanced Research Projects Agency Network displaying the simple message, 'I'm the Creeper: catch me if you can.' The following year saw the release of Reaper, a program designed to detect and delete Creeper. In doing so, it arguably became the first antivirus.



Dr Chris Ewin

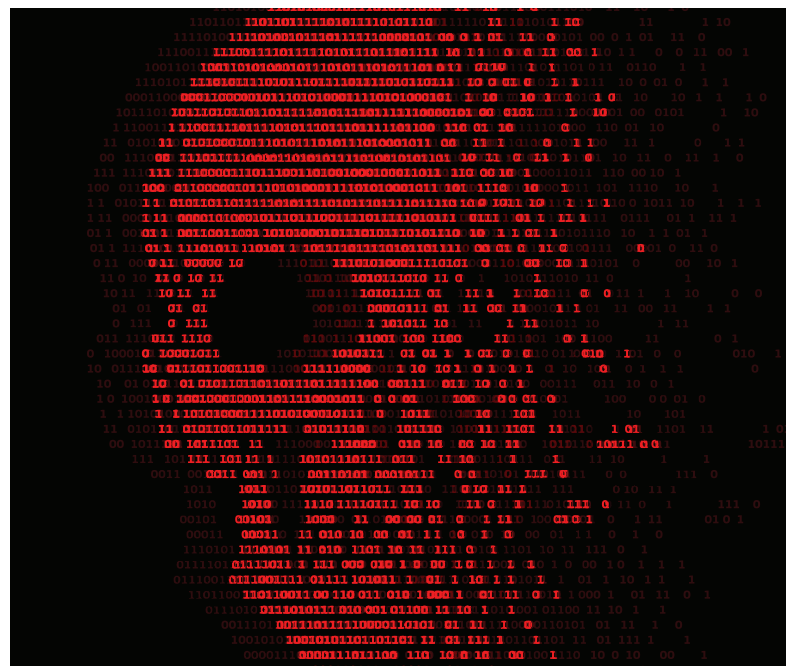
Fifty years later, the threat landscape has become unrecognisable. Cybercrime now costs the global economy an estimated \$6 trillion in damages each year, and the rapid changes to business operations necessitated by the COVID-19 pandemic have led to the emergence of new threats.

Artificial intelligence and machine learning are increasingly becoming the first line of defence against cyber attacks. Intrusion detection, spam filtering and malware classification systems are now leveraging deep learning to produce effective and accurate systems that can respond quickly to new threats. Threat detection that once required many hours of painstaking work by a security analyst can now be automated to a large degree, and the market for machine learning tools in cyber security is projected to reach \$46 billion by 2027.

Yet, while these tools show enormous promise, we must be conscious of the new security risks caused by an over-reliance on them. Machine learning systems must be trained on a large amount of real-world data and remain vulnerable to so-called adversarial attacks; for example, an attacker can make small but carefully chosen changes to a spam email or malware file that will trick the system into believing it is safe.

Alternatively, an attacker can poison the training data by introducing new samples designed to disrupt the system. To compound this problem, machine learning systems are typically designed as black boxes, without any facility for explaining why a machine learning system made a particular decision. This lack of transparency makes it difficult to verify the system's behaviour in different situations.

Machine learning systems also require the collection of vast amounts of data in order to train the models. Training data must be updated frequently to ensure protection against newly developed threats. This data isn't always curated carefully, which can result in personally identifiable information becoming part of the training data. So-called inversion attacks have been demonstrated, which allow an attacker to determine parts of the training data from the machine learning system after it has been trained. These sorts of attacks can cause the system to leak personally identifiable



information, and also pose challenges for compliance with the European Union's (EU's) General Data Protection Regulation legislation.

Compounding these challenges is the fact that most of the personnel involved in developing and deploying security systems don't have a background in data science or machine learning. Popular open-source libraries have made it very easy to produce models for both shallow and deep learning, but creating models that are both accurate and robust requires careful selection of the model parameters, as well as an understanding of the model inputs.

Being able to claim that a security system incorporates artificial intelligence or machine learning can greatly improve the marketability of a system, and the temptation to incorporate these techniques without fully understanding them or appreciating the risks involved is high.

For the time being, most of these threats remain within the realm of academia, but the chance of them being exploited in the wild over the coming years is high. The EU's recently unveiled Artificial Intelligence Act represents a first step towards establishing a framework for governing the use of machine learning systems, and should be a reminder of the risks of using these technologies without appropriate safeguards. •

Australian Information Security Association (AISA) member Dr Chris Ewin is a Lecturer in Computer Science at the University of Melbourne, with research interests in artificial intelligence and cyber security. His industry experience includes providing IT and cyber security consultancy to small businesses. He holds a PhD in computer science from the University of Melbourne.

APPLYING RISK APPETITE TO YOUR CROWN JEWELS

— BY DENNY WAN AND MICHAEL COLLINS —

Identification of information crown jewels provides a clear target for the prioritisation and focus of the cyber security management program.



The NSW Cyber Security Policy defines ‘crown jewels’ as an entity’s most valuable or operationally vital systems or information. Australia’s financial services regulator, the Australian Prudential Regulation Authority (APRA), states in the CPS 234 standard that boards are to ensure the entity maintains information security in a manner commensurate with the size and extent of threats to its information assets. While the standard states that all information assets must be classified based on criticality and sensitivity, there is no explicit methodology from the regulators for determining information crown jewels.

This paper explores a methodology for determining probable losses as a result of a cyber security threat impacting information crown jewels using the Open Group FAIR (Factor Analysis of Information Risk) cyber risk quantification framework, which can then be assessed against the entity’s risk appetite statements (RASs). This paper builds on, and learnt from, applying the methodology presented in the authors’ previous paper ‘Building an APRA CPS 234 compliance template’.¹

WHAT IS RISK APPETITE?

ISO Standard 73² (definition 3.7.1.2) defines risk appetite as the types and amount of risk, on a broad level, an entity is willing to accept in its pursuit of value. Risk appetite is established by the organisation’s most senior-level leadership (at the enterprise level), and serves as the guidepost for decisions such as setting strategy and selecting objectives. NISTIR 8286³ (Integrating cyber security and enterprise risk management (ERM)) instructs organisations to manage their risk to strategy and business objectives in relation to their risk appetite. It encourages organisations to take advantage of positive or ‘good’ risk to maximise the opportunities and benefits from delivering their mission.

According to Roderick Brown (Manager, Cyber Security Policy Development and Coordination, Cyber Security NSW), the NSW Cyber Security Policy is the foundation for improving the organisational cyber security resilience of New South Wales government agencies by making these entities aware of their risks, and helps them to make informed decisions in managing those risks. An important step is in identifying an entity’s most valuable or operationally vital systems or information (‘crown jewels’). The Open Group FAIR standard is one of several useful tools that can be used to assess the sufficiency of protection of these crown jewels, and, in particular, as a means of expressing the cyber security risk of an attack against these crown jewels in dollar value.

The Reserve Bank of Australia’s (RBA’s) RAS⁴, published online, is a good case study for applying this analysis. The RAS covers five risk categories – strategic, financial, fraud and corruption, people and culture, and operational. Cyber risk management is described in Section 4.5: Operational risks.

The RBA has a very low appetite for damage to bank assets from threats arising from malicious attacks. To address this risk, the bank aims to create strong internal processes, with development and continuous improvement of robust technology controls.

The RAS is implemented through three functions:

1. *Communications*: the RAS is published on the RBA’s intranet and website.
2. *Risk assessments*: each department maintains a risk register of the business risks it faces in its day-to-day operations and the control framework that is in place to mitigate risks.
3. *Reporting and monitoring*: a number of specific risk metrics assist management in assessing whether outcomes are consistent with the RBA’s risk appetite.



Denny Wan



Michael Collins

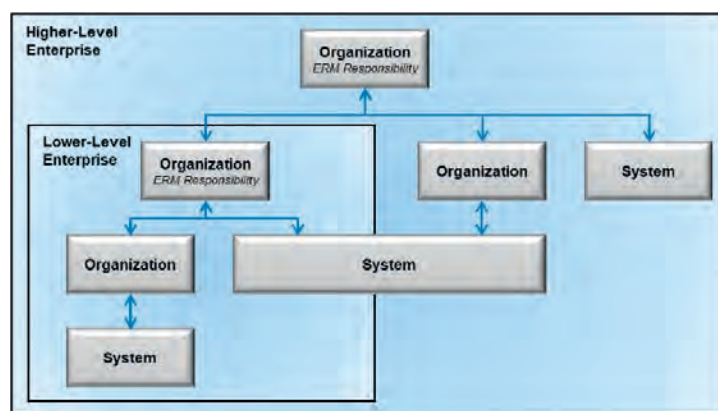


Figure 1. Enterprise hierarchy for cyber security risk management. Source: NISTIR 8286

RISK TOLERANCE

NISTIR 8286 also recommends using risk registers to manage cyber security risk cascading down the enterprise hierarchy, as depicted in Figure 1.

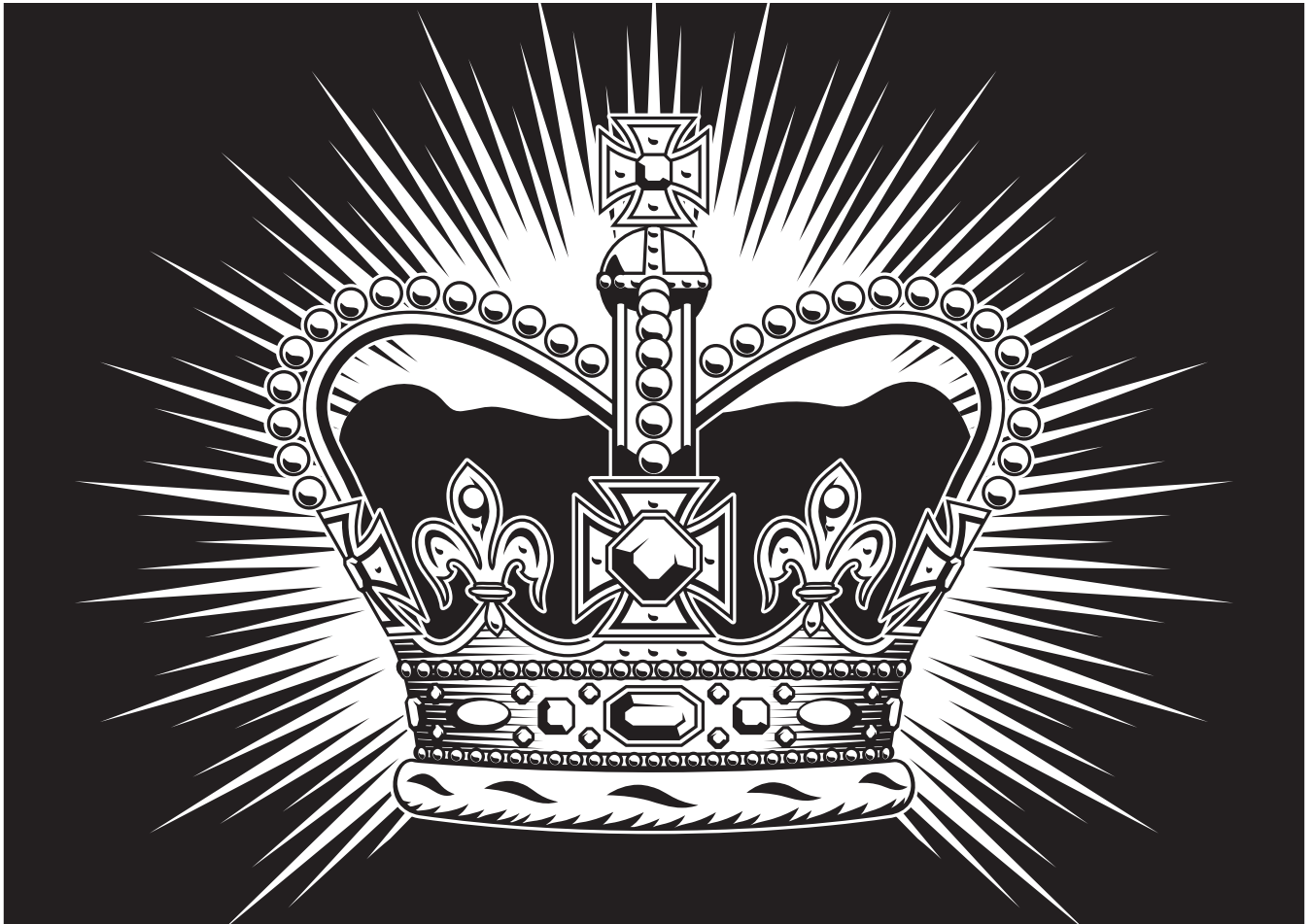
To operationalise RSA, NISTIR 8286 draws attention to the ERM concept of risk tolerance. Risk tolerance represents the organisation’s or stakeholders’ readiness to bear the remaining risk after responding to or

1 www.linkedin.com/pulse/building-apra-cps-234-compliance-template-denny-wan/

2 www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

3 <https://csrc.nist.gov/publications/detail/nistir/8286/final>

4 www.rba.gov.au/about-rba/our-policies/risk-appetite-statement.html



considering the risk, in order to achieve its objectives. The Committee of Sponsoring Organizations of the Treadway Commission defines risk tolerance as ‘the acceptable level of variance in performance relative to the achievement of objectives.’⁵

Risk tolerance can be defined at the enterprise level, but is generally established at the organisational or system level, as depicted in Figure 1. Risk tolerance is always interpreted and applied by the receiving custodians of the risk management discipline (e.g., cyber security, legal and privacy), and is usually interpreted at the organisational or system level. NISTIR 8286 includes an example where a statement of risk appetite might be: ‘Email service shall be available during the large majority of a 24-hour period.’ An associated risk tolerance statement for this defined appetite is narrower: ‘Email services shall not be interrupted for more than five minutes during core hours.’

David Tattam⁶, an Australian researcher and thought leader in enterprise risk management, put forward a multi-tiered risk threshold model, as depicted in Figure 2. The risk tolerance threshold should be used to inform operational decisions within the risk appetite. Continual tuning of the risk threshold is the operational responsibility of frontline risk managers.

DETERMINING INFORMATION CROWN JEWELS

As examined in the opening of this paper, the crown jewels of an entity are its most valuable or operationally vital systems or information. This determination is best developed at the organisational or system level, according to NISTIR 8286. This instruction is clearly communicated in the RBA RAS. The Open Group FAIR cyber risk quantification framework is a powerful tool to empower executives at the organisational or system level to identify the most valuable or operationally vital systems or information by calculating the potential financial loss exposure when these information assets are impacted by a cyber attack. The focus of the analysis is not determining the intrinsic value of the information asset (such as revenue opportunity or brand value), but the potential financial loss against the asset. The Open Group FAIR standard loss estimation covers six forms of loss, including reputational damage, fines and judgement, and loss in competitive advantage, as depicted in Figure 3.

To demonstrate how you might use FAIR to assess the financial impact of a cyber attack on your crown jewels, and how this compares to your risk appetite, let’s look at one of the more common issues facing organisations today: cloud misconfiguration. While more businesses are leveraging cloud services to accelerate their digital strategies, many are failing to understand that the balance of responsibility for security configuration falls to them as part of the shared responsibility model.

A common reason given for data breaches related to cloud services is misconfiguration of storage services,

⁵ Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017), ‘Enterprise Risk Management — Integrating with Strategy and Performance: Executive Summary’ (www.coso.org/Documents/2017-COSO-ERM)

⁶ www.linkedin.com/in/david-tattam-protectht/

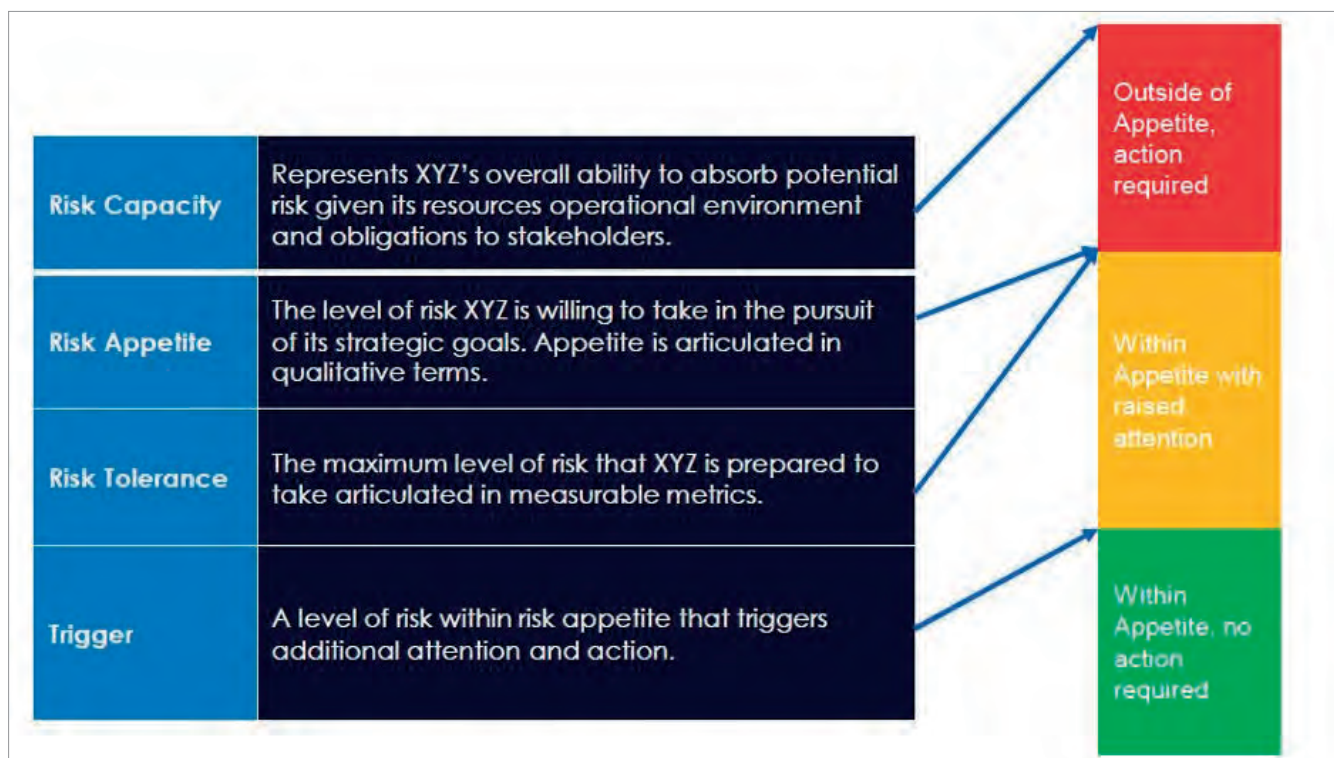


Figure 2. A multi-tiered risk threshold model. Source: David Tattam @ Protecht – ‘Integrating risk appetite into your ERM framework’ (<https://info.protechtgroup.com/risk-appetite-assessment-webinar>)

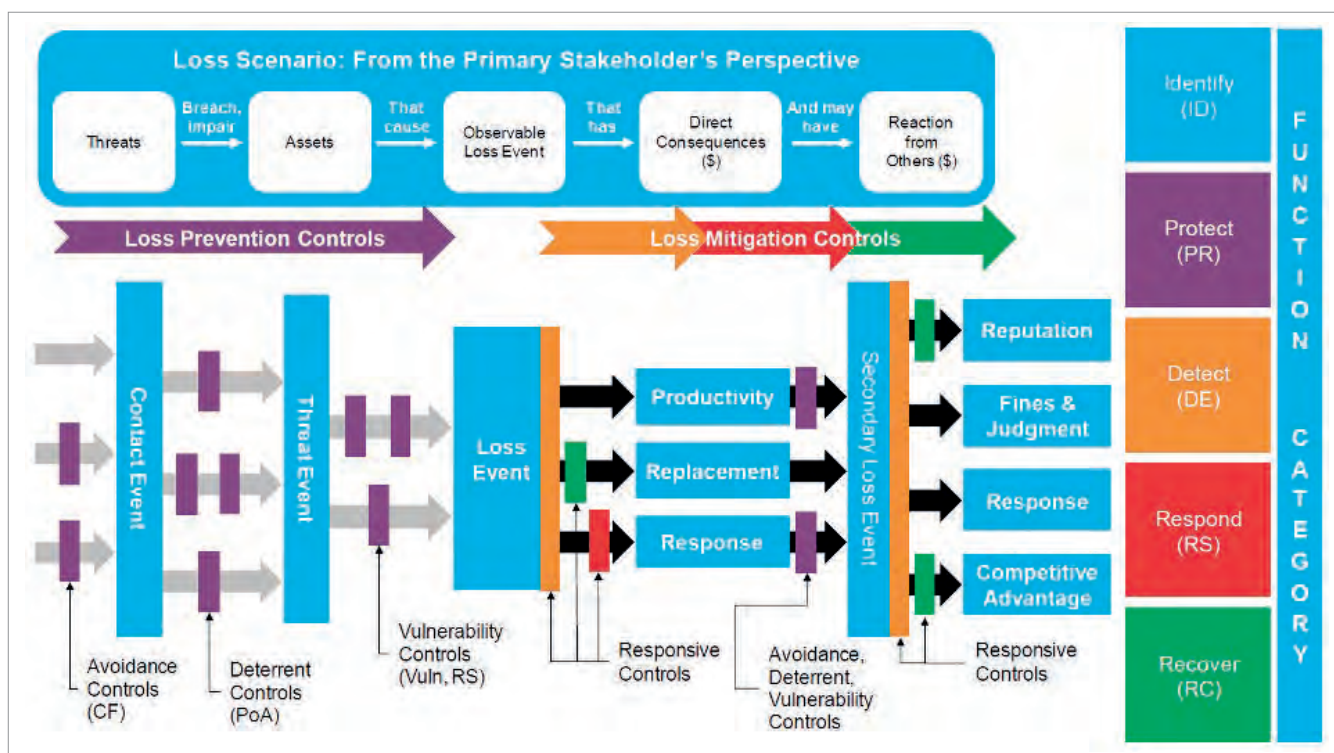


Figure 3. Decomposing an open FAIR loss scenario. Source: FAIR risk analysis (O-RA) Version 2.0 (<http://www.opengroup.org/library/c20a>)

which leaves sensitive data open to the internet and unauthorised access by malicious actors. In fact, in AquaSecurity's recently released cloud security report, it notes that users take, on average, nearly 70 days to remediate cloud storage being open to the public.⁷

So let's say that, in our hypothetical company, a near miss was recently detected during a routine check by your security team, which found a large

amount of sensitive customer information (aka crown jewels) that was to be shared with several external trusted partners had been stored in a misconfigured cloud-based storage location.

Fortunately, the misconfiguration was detected relatively early, therefore limiting public exposure to a short window. Access logs confirmed that no data was breached on this occasion. But, despite assurances from the team that it won't happen again, you're not entirely comfortable that this type of event is within your enterprise's risk appetite. In their book *Managing the*

⁷ AquaSecurity (5 September 2021), *Cloud security report H1-2021*, <https://blog.aquasec.com/cloud-configuration-threat-report>

Unexpected: Sustained Performance in a Complex World⁸, Karl Weick and Kathleen Sutcliffe call these types of events ‘cues of evolving failure’, suggesting that they provide emerging evidence that the anomaly is meaningful and potentially significant.

While organisations often dismiss these seemingly one-off events, they are at risk of normalising the behaviour. Highly reliable organisations are drawn to continually assessing anomalies as weak signals of an impending disaster. Further investigation by your team reveals a trend of these misconfigurations over a period of time, which further piques your interest in understanding more about how bad the outcomes could be.

Information security leaders can often find themselves in situations where the team responsible for the misconfiguration has essentially cried ‘no harm, no foul’, and despite you raising this with the management team, people don’t seem to think it was such a big issue. Your main challenge here is that you don’t have sufficient data to get management’s attention; you’re attempting to appeal to people based on emotions, and people are possibly seeing you as Dr No, instead of Dr Know.⁹

Using the FAIR model, you can provide context and clarity to the business about whether the potential financial loss resulting from disclosure of sensitive records is acceptable given the current control conditions and threat landscape.

Consider the differences in asking business executives whether they are comfortable with the ‘risk of misconfigured cloud storage’ versus the more powerful question, **‘Does a 10 per cent likelihood of incurring a financial loss of \$5 million or greater in the next 12 months due to a data breach resulting from misconfigured cloud storage sit within your risk appetite?’** Maybe it does, and maybe it doesn’t; but in the event it’s the latter, you are now in a better position to provide realistic and actionable solutions to contain the frequency and/or magnitude of the loss to something that is within the risk appetite for this scenario.

It is in these types of business situations that FAIR can provide you with the weight of evidence needed to allow key stakeholders to make a fully informed decision

Financial Risk Profile						
	Current Period			Previous Period		
	Net Revenue	Capital	Free Cash Flow	Net Revenue	Capital	Free Cash Flow
Enterprise						
Dept A						
Dept B						
...						
Dept N						
Reputation Risk Profile						
	Current Period			Previous Period		
	Public	Regulators	Partners	Public	Regulators	Partners
Enterprise						
Dept A						
Dept B						
...						
Dept N						
Mission Risk Profile				Previous Period		
Enterprise						
Dept A						
Dept B						
...						
Dept N						

Figure 4. Notional enterprise risk portfolio view for a private corporation

on whether they are comfortable accepting the risks associated with their crown jewels.

NISTIR 8286 includes a notional enterprise risk portfolio view for a private corporation, depicted in Figure 4.

FAIR-based modelling is useful to populate the estimate for the financial and reputational impacts from the materialisation of cyber risk scenarios.

NEXT STEP

Please join our global community of more than 11,000 FAIR practitioners through the FAIR Institute. General membership is free. For more information, visit www.fairinstitute.org/get-involved-apply-today. ●

Denny Wan is a thought leader in applying cyber risk quantification and the NIST-endorsed Open Group FAIR framework. He is a strong communicator and community builder who founded the FAIR Institute Sydney Chapter, which has a rapidly growing membership. His recent article, ‘Targeting cyber security investment – the FAIR approach,’ is a practical guide for prioritising cyber security investments. His latest article, ‘Building an APRA CPS 234 compliance template,’ explains how to quantify risk appetite and risk tolerance to identify the boundaries for good risks, and to improve competitiveness and profitability.

Michael Collins is an experienced information security professional bringing expert oversight to digital business and risk matters at executive and board levels in the financial services industry. Collins is Co-Chair of the FAIR Institute Melbourne Chapter, and combines critical thinking skills with subject matter expertise to more effectively bridge the cyber to business divide.

8 Weick, K. E., & Sutcliffe, K. M. (2015), Managing the Unexpected: Sustained Performance in a Complex World. Wiley

9 www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf

API on wheels: A road trip of risky vulnerabilities

— BY PIETER DANHIEUX —

When was the last time you took a road trip? Depending on where you are in the world, it may only be a recent return to the agenda; but nothing is better than the open road and getting a change of scenery. Unless you're a software vulnerability, of course.





Pieter Danhieux

Many have spoken at length about the dangers posed by lax cyber security measures in the automotive industry, with the likes of Tesla and Jeep already working with security researchers to find exploitable bugs that could have led to serious safety issues if not discovered early and fixed promptly.

Many have also spoken about how, in general, software security is still in the Wild West. Software is everywhere we turn, and for many connected devices, vehicles and their peripherals, the security measures need to go well beyond end-user education and vigilance.

Application programming interface (API) vulnerabilities are becoming especially insidious, with malicious API traffic growing more than 300 per cent in the past six months alone. This is rather concerning, given that modern vehicles are essentially APIs on wheels. They're connected, very chatty with other applications, and could be caught up in targeted attacks as one of many vulnerable endpoints.

WHEN YOUR EV CHARGER SAYS TOO MUCH

Connected vehicles have come under scrutiny for their software safety, but what about their accessories? The genius crew at Pen Test Partners uncovered several code-level vulnerabilities in six home electric vehicle (EV) charging brands, as well as a widespread public EV charging network.

Who cares about a charger? What could an attacker gain? Unfortunately, one of the downsides of powerful, deep tech working overtime for us is that generally, these devices have a bad case of TMI. EV chargers communicate with companion mobile apps via API, in a cloud-based environment, and all of that can be vulnerable to exploitation if not coded and configured securely. APIs, by design, open the floodgates for communication between apps, and if these endpoints are not carefully configured, too much could be shared or – worse – accessed via a vulnerable app back door.

Pen Test Partners discovered extremely dangerous vulnerabilities that could have led to millions of EV chargers being hijacked, several instances of API authorisation issues that allowed account takeover and remote control/access to an account, and even the possibility of disrupting the power grid through synchronised control of multiple EV devices. These issues were all patched, but the fact that a few lines of code were all that stood between attackers and complete disruption of core functionality and service infrastructure is deeply concerning.

It's not like it's mastermind stuff, either. Wallbox, for example, had two insecure direct object references (IDORs) in their API, which would have allowed



account takeover if exploited. IDOR falls under broken authentication, which sits at number two in the Open Web Application Security Project® Top 10 API vulnerabilities. It's as common as dirt, which points to a failing in the learning and implementation of quality code. We can't persist with connecting sensitive devices and apps through myriad buggy communication pathways, and poorly configured APIs are just that.

WORKING SECURELY WITH AUTOMOTIVE APIS TAKES EDUCATION AND PATIENCE

The frustrating thing with API security is that it is touted as a new wave of cyber security disaster to try and mitigate, when really it's just a new setting for the same old problems we have seen for decades in web development. Cross-site scripting (XSS), injection, misconfiguration – sound familiar?

Recent indicators from organisations like the National Institute of Standards and Technology are promising, and show that software security is becoming more regulated and standardised; however, we still fall short of the required experts to even put a dent in the deluge of code that is written every day. Developers need to be elevated in their security knowledge and responsibilities, and it's not on them to take the initiative. If you've got a team working on embedded systems in appliances, or APIs that could turn a car into someone's remote control toy, then you must make sure



they are equipped with what they need in order to stop introducing common vulnerabilities.

The differences between a secure API and one vulnerable due to XSS are minimal, for example, but developers need to be shown the nuances that differentiate a poor coding pattern from a good one. In addition, lazy development processes are often business as usual in API configurations, with many given vast permissions over and above the minimum requirements for them to perform their set tasks, thus opening so much extra threat surface and potential for data theft. These factors need to be considered during the build, but if they are not ingrained into acceptable development practices, the process will continue to be a risk factor.

AVOIDING THE NEW THREAT ACTOR PLAYGROUND

The dramatic increase in APIs as a target of threat actors shows that attention is moving to a perceived low-hanging fruit – and in this instance, it is one that could be a pipeline to significant paydirt, in addition to potential threats to life in the form of potential vehicle takeover.

Leaving API security up to chance is a sure-fire way to introduce problems later on, with potentially devastating consequences at worst, and frustrating rework and low performance at best. It should be a critical consideration as part of the communication ecosystem of software and high on the list of a best-in-class security program. The key to this is treating each API as though it's a human, and

assessing what access it should have. Should 'Jim from Accounting' have access to all sensitive legal documents for the entire company? Probably not, and access control is generally correctly determined in the case of real-world personnel. The same cannot be said for APIs, and it's important to remember that they are powerful chatterboxes that will let everyone know your secrets if they're not configured with the same zero-trust methods as everything else.

The organisation must be on high alert, and developers are the eyes needed on the ground to create quality code that is free from these vulnerable portals to despair. It's time to give them the opportunity to grow and thrive as security-aware engineers, with the right mindset for this goal and the hands-on skills to make the right decisions in critical stages of creation. •

.....
Pieter Danhieux is a globally recognised security expert with over 12 years' experience as a security consultant and eight years' experience as a Principal Instructor for the SANS Institute, teaching offensive techniques on how to target and assess organisations, systems, and individuals for security weaknesses. In 2016, he was recognised as one of the 'Coolest Tech People in Australia' (*Business Insider*) and awarded AISA's Cyber Security Professional of the Year. He holds GSE, CISSP, GCIH, GCFA, GSEC, GPEN, GWAPT and GCIA certifications.

You can follow Danhieux on twitter @PieterDanhieux, or on LinkedIn: <https://www.linkedin.com/in/pieterdanhieux/>



Scholarship opening doors to cyber industry

FROM WORKING ON the floor of a hardware store, to rubbing shoulders with Australia's elite cyber corps, Hannah Rice's career change has been as rapid as it is impressive.

The Edith Cowan University (ECU) student will receive \$10,000 per year during her studies, and will have the opportunity to undertake professional placements within the Department of Defence and the Australian Signals Directorate after being awarded the Leisa Condie Defence Women in STEM Undergraduate Scholarship.

The scholarship promotes diversity in the STEM workforce by increasing participation in, and building a career path for women in the sector.

She says the scholarship was an outstanding recognition of her success in her studies and would help cover costs associated with her degree.

'I'm a single mum, so the financial aspect is definitely really helpful, but obviously being recognised for this scholarship and the opportunities it provides are also really important,' she says.

She started her degree in cyber security almost by accident after spending the first part of her working life at Bunnings. But she says she was happy to be a model that other women pursuing a career in STEM could follow.

'I didn't know about everything I could learn studying cyber security, and it just seemed like a fluke that I ended up here,' she says.

'It's surprising to me that it's an industry that's hidden away. There are massive opportunities for women, but they aren't necessarily told that.'

ECU JOINS SELECT INTERNATIONAL CYBER GROUP

The University has recently become the first and only one from Australia to join the International Cyber Security Centre of Excellence as an Affiliate Member.

The centre was initiated in 2019 by universities across the United Kingdom, Europe, the United States and Japan, and acts as a hub for cyber security research, education, and advocacy.

ECU School of Science Executive Dean Professor Andrew Woodward says cyber security students were

already seeing the benefit of the partnership, with several teams competing in the global Capture the Flag competition in 2020.

'Last year, ECU students were among the top performers in the Centre of Excellence's Country-to-Country Capture the Flag, and the winning team's leader was an ECU student,' he says.

INVESTMENT IN INFRASTRUCTURE

Already considered a leader in cyber education, ECU is responding to the growing demand for cyber security graduates with industry standard training facilities.

ECU's world-class Security Operations Centre is the first of its kind in Australia and one of only a handful worldwide.

Located on the University's Joondalup Campus in the northern suburbs of Perth, the facility also provides students with the opportunity to gain experience in monitoring, detecting and responding to cyber security incidents. ●

For more information, visit ecuworldready.com.au/cyber-security

CYBER SECURITY AT ECU



AUSTRALIA'S ONLY INTERNATIONAL CYBER SECURITY CENTRE OF EXCELLENCE

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

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

ECU's Security Research Institute (ECUSRI) offers world-class teaching and research in Cyber Security, Critical Infrastructure Security, Digital Forensics and Human Security, and has a history of delivering successful research projects for Federal and Defence agencies. Two of our cyber team are members of the Interpol Global Cybercrime Expert Group.

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

**TO FIND OUT MORE, VISIT
[ECUWORLDREADY.COM.AU/CYBER-SECURITY](https://www.ecuworldready.com.au/cyber-security)** —



UNIVERSITIES MUST STAND FIRM ON CYBER

— BY DAVID BRAUE —

Supporting large, distributed user bodies leaves increasingly virtual institutions exposed.



As the vanguard in training the next generation of computer science engineers and cyber security experts, Australia's universities play a pivotal role in shaping and populating the national response to cyber security.

Yet, for precisely the same reasons, Australian universities have also come into the firing line on the global stage – to the point where recent Check Point Research analysis found that the education sector in Australia was the fourth most targeted in the world.

Australian schools and universities were hit by an average of 3934 cyber attacks per week in July alone, Check Point's analysis found, behind only Israel, Italy and India – which had 5196 weekly attacks, despite having 50 times Australia's population.

Yet, the climate of cyber security attacks on educational institutions is hardly an Australian phenomenon; the education sector was the most attacked sector in more than half of the countries that Check Point studied, and was in the top three in 94 per cent of countries.

'Schools, universities and research centres make for attractive targets to cybercriminals because they are often under-resourced from a security perspective,' says cyber security evangelist Ashwin Ram.

Remote learning exacerbated the trend during the COVID-19 pandemic, Ram adds, noting that, 'The short notice, on-and-off shift to remote learning... presents a range of new security threats that many aren't prepared to address.'

The implications of that deficiency were painted in stark relief in July, when the New South Wales Department of Education was forced to pull a range of systems offline after a cyber security attack launched just hours after the state government announced New South Wales students would return to remote learning.

'The timing of this creates considerable challenges for staff as we prepare for the start of term three,' New South Wales Department of Education Secretary Georgina Harrison said at the time.



The ability for a single ransomware or malware attack to compromise services for tens or hundreds of thousands of students makes educational institutions uniquely exposed to the depredations of cybercriminals.

This point was not lost on the Federal Bureau of Investigation in the United States, which recently warned educational institutions about a surge in PYSA/ Mespinoza ransomware targeting higher education with phishing emails or compromised remote desktop protocol credentials, then exfiltrating large volumes of data directly to a cloud storage service.

Educational institutions are also more exposed than most to potential compromise through human error, since they harbour large and diverse numbers of people with varying cyber security awareness levels and practices.

Throw in the surge in demand for large-scale, cloud-based services over the past 18 months, and the changing attack surface has become a large-scale liability as 74 per cent of education respondents said their cyber security workload had increased during 2020.

This was second only to government organisations and correlated with a slowdown in cyber security incident response – with educational institutions more likely than any other industry to report that their response times had increased over the past year.

Educational organisations were reported as the most frequently hit by ransomware in a recent Sophos analysis, which placed education alongside retail as the sectors most hit by ransomware. Sophos revealed that 44 per cent of sector respondents reported being hit by ransomware in the past year, and 35 per cent reported that they had paid a ransom to get their data back.

Significantly, recovering from a ransomware attack had proven to be more expensive in education than in any other industry sector – costing \$3.74 million (US\$2.73 million) on average, well ahead of the \$2.54 million (US\$1.85 million) average.

PUTTING THE 'IT' INTO IDENTITY

Given the particular challenges of security within the university and education sector, many institutions have, in the first instance, turned to overhauls of their identity and access management (IAM) frameworks to apply a single management framework to the surging population of desktop, cloud and mobile applications.

The University of Newcastle made that exact decision several years ago, after the security implications of its previous infrastructure were becoming clear.

The decision to overhaul its infrastructure included a 'massive move to the cloud,' including extensive use of Zoom over the nationwide AARNet backbone, University of Newcastle Manager for Solution Architecture Jimi Reilly explains.

'Little of the university had developed mobile apps for different reasons, and we recognised that from a user experience perspective, it was going to be much easier in that mobile ecosystem if we had a really robust and reliable single sign-on (SSO) technology,' he says.

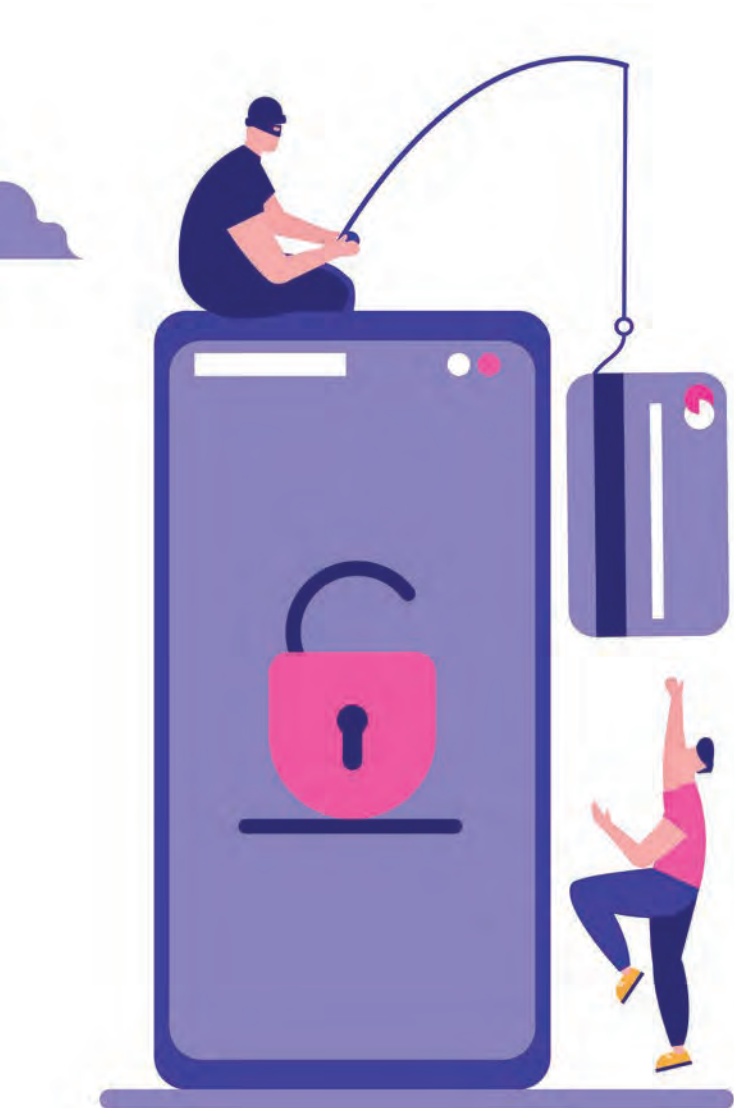
'It was an opportunity to bring all of that together and solve a few problems at the same time.'

Implementation of an Okta IAM framework – including adaptive multi-factor authentication (MFA) that ties access decisions to environmental factors, such as the location of the user and whether they are logging on from inside the network or from home – proved fruitful in improving control over access to the university's applications.

Over the course of just two months this year, the new framework isolated over 200,000 extraordinary login attempts, including university researchers logging on from Antarctica and questionable logins from Russia.

Backed by mechanisms including SMS verification and verified push – in which a registered mobile app is queried for approval each time the user wants to access a sensitive resource – the security team was able to





build appropriate SSO policies to suit its complex and distributed environment.

‘We were comfortable with the fact that in the zero-trust world, we were covered,’ Reilly says. ‘It gave us the flexibility of being able to cater to whatever discrete user requirements we had for each individual.’

The university’s transformation ‘really paid off during COVID, and allowed us to respond really quickly and in a secure way,’ Reilly continues. ‘We were serving the business, but also didn’t compromise our security during the process.’

With 51 per cent of education data breaches involving credential theft, and with social engineering by far the most common attack vector, according to Verizon’s Data Breaches Investigation Report 2021, moves to shore up identity defences are particularly valuable in the education context.

Significantly, pretexting – in which attackers make up scenarios to manipulate users into clicking on malware-laden sites – was by far the most common social-engineering vector, with nearly 90 per cent of attacks created by cybercriminals.

These attackers, Verizon notes, ‘seem to be harkening back to their creative writing courses and are putting forth the effort to invent a convincing scenario to get their victim to respond’.

GIVE A MAN A PHISH

Despite their prominence as cyber security targets, educational institutions also enjoy one significant advantage: their entire purpose is built around teaching, so they are uniquely positioned to drive a cyber security culture among both their staff and the students they serve.

The key, notes PwC Australia Partner for Cyber Pip Wyrdeman, is to push cultural change using whatever capabilities are available.

‘I would love to see the universities and training colleges start to incorporate cyber security in all of the courses they offer,’ says Wyrdeman. ‘Even in the fine arts, I think there’s a space for people to be taught the basics of cyber – even if it is simply by way of, “Here’s how you protect your non-fungible tokens”.

‘There’s a space for understanding where cyber fits any time you’re going to start playing in any sort of digital anything.’

With university courses in a sort of limbo as campuses wait to welcome back students in person, now may be the best time to drive security awareness deep into that transformation.

Gartner advises that this year, higher education institutions should seize opportunities in areas such as improving student experience and cross-life-cycle CRM; scaling virtual experiences, cloud and chatbots based on lessons learnt during the pandemic; and refining remote-learning tools, such as remote proctoring and faculty information systems.

Chief information officers (CIOs), the analyst firm advises, should balance the maintenance of key systems with the enablement of ‘emerging and innovative technologies’ using a bimodal approach and creating a ‘special unit that can explore innovation’.

Security poses particular challenges, Gartner analysts Bart Willemsen and Bob Yancello warn, noting that, ‘Threats are varied, and an adequate response is required where the institution faces most risk... Although targeted attacks are common, many organisations still fall victim to opportunistic attacks.’

The solution, they recommend, lies in closer collaboration between CIOs and security leaders ‘to confront the threat landscape on a risk-based approach, including continually evaluating how existing defences adapt to microtrends; engaging stakeholders to understand new business and technology practices; and developing organisational resiliency with strong backup and incident response plans to prepare against attacks that can’t be prevented or detected.

‘Responding proactively to cyberthreats,’ the analysis notes, ‘will be critical for higher education institutions to continue to exist and thrive.’ ●



Curtin University



MASTER OF CYBER SECURITY

Curtin University offers two Master level courses in Cyber Security that are aimed at addressing the need for cyber security professionals. The courses have been developed in collaboration with the industry and cover critical knowledge from both the defensive and offensive perspectives of cyber security.

The 1-year accelerated course is aimed at graduates from an IT degree that would like to specialise in cyber security. The course provides in depth coverage of enterprise network defence, cloud operations and security, incident handling, governance and penetration testing.

The 2-year degree Master of Computing (Cyber Security Major) is aimed at graduates that lack a solid IT background and thus covers fundamental IT skills in addition to the specialised cyber security content. The course provides bridging content on programming, software design, data analytics and project management in the first year of the course with the advanced content following in the second year of the program.

Graduates from the Master courses will be well-versed to apply their knowledge and critical thinking to information protection, fraud, policies, compliance requirements, digital forensics, system analytics and infrastructure defence.

Make tomorrow better

bit.ly/curtinmastercs for more information.



Maha Afaneh

The new era of cyber security

FROM DELIVERY SERVICES and data collection, to television shows and banking – almost everything is connected to the internet. In a post-COVID-19 society, even medical care and higher education is often conducted online.

As our reliance on technology increases, so too does the need for advanced cyber security protocols, as La Trobe University cyber security expert Dr Javed Chowdhury explains. ‘The COVID-19 pandemic has made working from home the “new normal”. This has increased the demand for people who understand cyber security and keep us safe.

‘Cyber security is no longer limited to technical degrees. We need people with business knowledge or legal expertise, or who are from a psychology background, to keep our business safe, make new laws and better understand the mindset of the hackers to help protect our society.’

NO LONGER THE PRIMARY DOMAIN OF IT DEPARTMENTS

To find the root cause of issues, the cyber security industry needs people from all walks of life – from coders to psychologists.

That’s because many cyber attacks – such as phishing – are aimed squarely at people. To stay one step ahead of hackers, we need psychologists and criminology experts who understand motivations, as well as system weaknesses.

People trained in business and finance can integrate cyber security into companies of all sizes. They’ll be at the forefront of blockchain and cryptocurrency, working for banks, food suppliers, technology innovators and even small businesses.

New technologies open the door to unexpected possibilities. We need people who can create legal and ethical frameworks for dealing with the new challenges posed by cyber security: lawyers, judges and lawmakers.

YOU DON’T NEED TO BE A TECH WIZARD

Many of La Trobe’s cyber security students come to these degrees from diverse backgrounds. La Trobe Master of Cybersecurity graduate Maha Afaneh discovered her love of cyber security while studying her criminology degree.

‘I’ve always had an interest in technical areas, so I didn’t let having a non-technical degree stop me.’

During her degree, she was head of the La Trobe Cybersecurity Society and won the 2019 Australian Information Security Association’s Cyber Security Tertiary Student of the Year Award.

HELP BRIDGE THE CYBER SKILLS GAP

Through the Australian Government’s Cyber Security Skills Partnership Innovation Fund, La Trobe has been awarded \$2.35 million to partner with industry to help bridge Australia’s cyber security skills gap.

Industry needs multidisciplinary solutions to combat ever-evolving cyberthreats. That insight is at the heart of La Trobe’s cyber security degrees.

Employers also need career-ready graduates. That’s why La Trobe has partnered with industry leaders, such as CISCO and EC-Council, to provide students with better opportunities for cyber security internships and certifications.

Be at the forefront of an exciting and in-demand career, and discover La Trobe’s undergraduate and postgraduate cyber security degrees today. ●

Cybersecurity at La Trobe

**Develop multidisciplinary solutions
to ever-evolving cyber threats.**

With digital technology penetrating almost every facet of our lives, cybercrime is no longer just a computer problem – solutions require insights from multiple perspectives. That insight is at the heart of La Trobe's cybersecurity degrees.

Step confidently into your future:
latrobe.edu.au/cybersecurity



**LA TROBE
UNIVERSITY**

All kinds of clever



NIST CYBERSECURITY FRAMEWORK PRACTITIONER

ALC has recently introduced a new certification to its flagship line-up of courses, addressing the growing trend and need of practitioners in the region who either wish to use, or have been requested to use, the NIST Cybersecurity Framework. Emanating from Executive Order 13636 **Improving Critical Infrastructure Cybersecurity** signed by former President Barack Obama in February 2013, version 1 of the Framework was released one year later on 12 February 2014. Version 1.1, released in April 2018, added the supply chain or what we refer to as the Extended Enterprise.

The benefit of using the Framework is that it provides guardrails and structure when assessing the activities and assets associated with the most critical parts of a business.

As delegates discover, the Framework is not a standard, such as PCI DSS or ISO 27001, nor is it set in stone – it is extensible, allowing users to modify and adapt the Framework to the unique needs of their organisation, including the use of multiple protection profiles; adding, deleting, or customising categories and sub-categories; and adding in new informative references.

ALC's new course, **NIST Cybersecurity Framework Practitioner**, guides participants through the generic Framework, giving extensive in-depth examples of the theory. Even though NIST emanates from the US, the course does not have a US-centric orientation. Special effort has been made to ensure both a practical and a regional flavour by use of an extended case study throughout.

The case study and corresponding exams allow participants to better reflect on the virtues of the Framework, in that an organisation is part of what is referred to as critical infrastructure. Participants discover what sector the case study is set in, the reliance on other critical sectors, and where they are placed within their own sector.

This allows a better understanding and a dialogue to be established for the cyber resilience functions used during and after an attack.

The first course ran 2-6 August 2021 using virtual, instructor-led training, and was enthusiastically received by delegates from Australia and Malaysia who were not only challenged with the theory and concepts, but performed well in the case study, mock exam and final exam.

Well done to all of you! ALC looks forward to continuing on its journey from having successfully launched a new course to embedding it as part of the ongoing curriculum for meeting the needs of cyber security professionals. I look forward to the next course scheduled for November, 2021.

Peter Nikitser
Director, ALC Cyber



**Celebrating 27 years
of training excellence!**

alctraining.com.au



LEADING IT FOR

27
YEARS

TAKE YOUR CAREER TO THE NEXT LEVEL

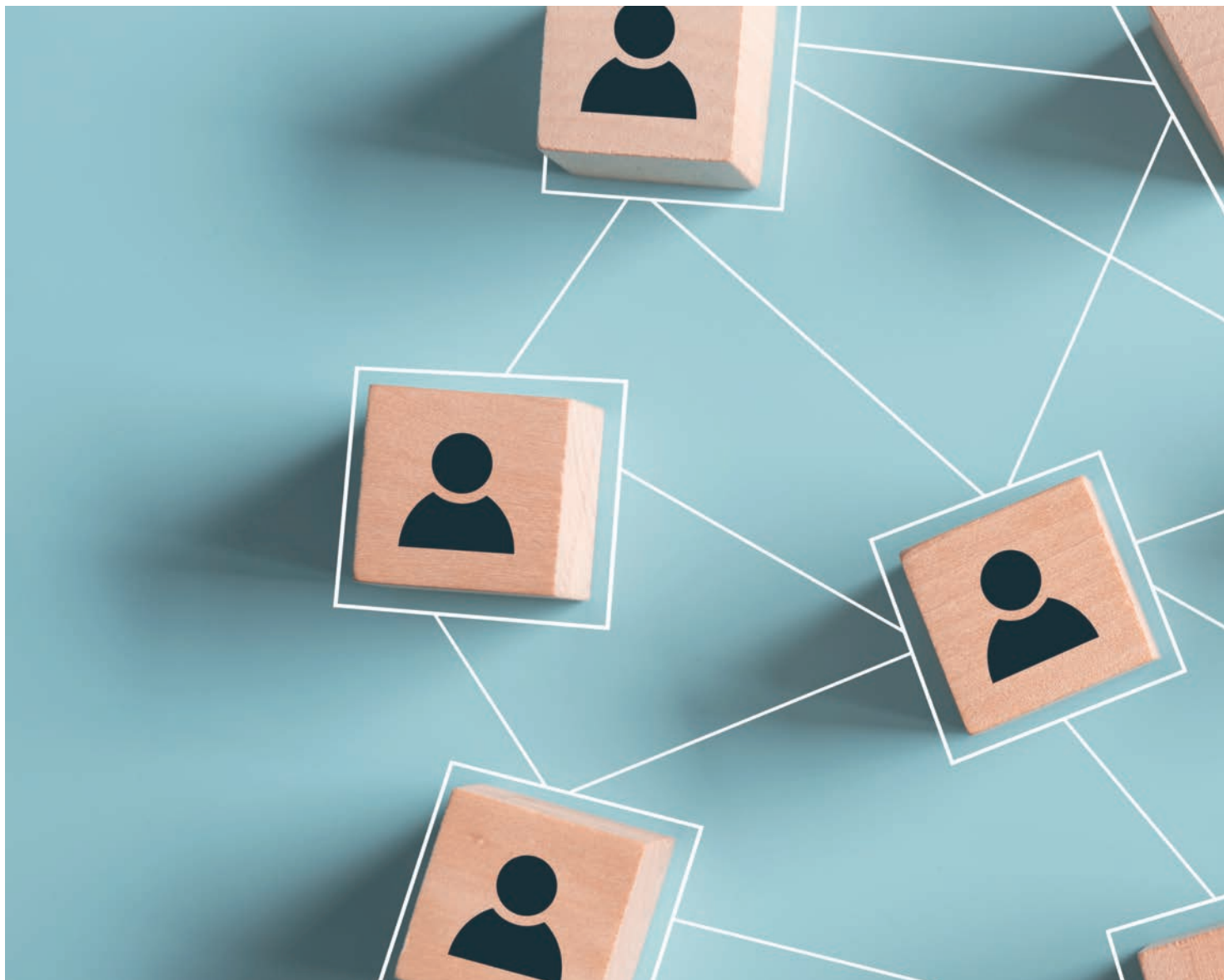
CISSP®, CISM®, CRISC®, SABSA®,
CISA®, CCSP®, CIPM, CIPT,
ISO 27001, CSF+P + MORE...

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

alctraining.com.au

AISA MEMBERS SAVE 10%

To redeem simply quote
your AISA member number
or call 1300 767 592



AUSTRALIA'S CYBER SECURITY SKILLS SHORTAGE VS LOWEST UNEMPLOYMENT RATE

— BY MINA ZAKI —

*In September, Australia's unemployment rate fell to a new low of 4.5 per cent – the lowest since November 2008.
What does this mean for the cyber skills shortage?*



In Australia, skilled cyber security employees are now in even higher demand than before, leaving Australia's growing cyber security industry in a compromising position when it comes to attracting the right talent.

The Australian Cyber Security Growth Network's Sector Competitiveness Plan (SCP) Update 2020 revealed that while the sector seeks accelerated growth, it 'may struggle to maintain a sustainable, high-quality pipeline of skills [that] match employer needs'.

The SCP also highlighted that, while the slowest-growing companies were preoccupied with general startup barriers, such as legal and tax advice, they struggled to attract talent compared to the fastest-growing cyber companies, which found talent acquisition easier.

In the current market, however, even the fastest and most brilliant companies are struggling to find the right talent. While the low unemployment rate and skills shortage both contribute to this, there seems to be another factor being considered by the best companies: the avoidance of 'the brilliant jerk'.

I spoke with Ian Yip, Founder and CEO of Avertro, a New South Wales-based rising superstar of the sector, who has been actively recruiting for various roles over the past six months.

'I've personally interviewed close to 100 people. Above all else, we value a positive attitude, humility, resourcefulness, passion for their craft, and attention to detail in our team members. This has made it difficult to find the right candidates even if they possess the right skills, but it reduces the risk of hiring "the brilliant jerk".'

Employers like Yip are unwilling to compromise on the quality of their employees.

'Forced to choose between a candidate with all the required skills but not the core personal attributes we desire, and one that exhibits those attributes but doesn't quite meet our skill requirements, we will pick the latter 100 per cent of the time. It does mean, however, that we are able to give someone their first shot at a career in cyber security because we take this progressive approach.'

Many have argued that the easiest solution to the skills shortage is to bring in skilled employees from overseas. While this may be true for many roles, it's refreshing to see companies like Avertro putting in the hard yards to give new talent a go and provide them with their start in the cyber security industry.

Earlier this year, I was involved in the formation of the AustCyber/Microsoft Cyber Security Traineeship



Program that secured funding under the Commonwealth Government's Cyber Security Skills Partnership Innovation Fund. The Traineeship Program aims to support around 200 participants to forge a pathway into cyber security by providing initial cyber security training through a bootcamp to prepare participants for entry into the Certificate IV in Cyber Security. This is completed in conjunction with paid, on-the-job training provided by employment partners of the program.

The benefit of this program, among other things, is that it allows employers to take on promising individuals who will form the future talent pool of cyber security. It helps to cultivate the type of future employees we want to see in this industry.

As the focus starts to shift away from the stale measurement of a specific number of years' worth of experience in the sector to a more holistic focus on the strengths and attitude possessed by individuals, we are more likely to see the closure of the skills gap.

There is, however, a lot more that needs to be done. The sector requires more employers willing to take a chance with the future talent pool of cyber security to help cultivate the right kind of talent and attitude to grow the future skills pipeline.

Together, we can close the cyber skills gap even with a decreasing unemployment rate. While importing skills can be extremely valuable and, in some cases, essential, because some roles simply cannot be filled otherwise, it alone is not the answer. Instead, we must be bold enough to invest in cultivating the sovereign future skills pool we want to employ from, and that we want our future generations to benefit from. It's a win-win investment for everyone in the Australian cyber security sector. •

.....
If you would like to take on trainees from the AustCyber/ Microsoft Cyber Security Traineeship Program, email info@austcyber.com



Charles Sturt
University

Upgrade your IT career with Australia's most experienced online university*

Are you an IT professional looking to take the next step in your career?

Whether you're aiming for a more senior role or want to upgrade your skills, we'll keep you moving forward.

Our postgraduate IT courses are taught by highly qualified academic staff with links to global industry.

You'll gain in-demand skills through application of methodologies, using cutting edge tools and technologies. With a strong technical focus, our courses provide you with everything you need to take your career to the next level.

You could...

Upskill with our Master of Information Technology

The IT world is changing fast, and in-demand professionals are changing with it. Build on your existing knowledge. Bridge the gap between users and technology.

Hone your skills across emerging fields, including data analytics, Internet of Things (IoT), mobile app development, digital forensics, networking and server administration.

Choose from a range of specialisations, such as cyber security, data science, computer networking, business analysis, IT management and software development.

Learn more

→ study.csu.edu.au/master-it-12

Branch out with our Master of Cyber Security

As more of life moves online, so do the threats. That means there's a growing demand for qualified professionals to keep us safe.

You'll learn about the dark web, cyber warfare and terrorism, digital forensics, hacking countermeasures and professional systems security. Plus, you'll choose four electives from areas like cyber security management, network security and cryptography, cloud privacy and security, and pen testing.

Learn more

→ study.csu.edu.au/master-cyber-security

Ease back into study with our shorter graduate certificates

Not quite ready to take on a master's? We've got you covered. Our graduate certificates are a quicker way to boost your credentials, and can provide a pathway into a master's degree.

Graduate Certificate in Information Technology

Choose subjects in networking, programming, security, management, or business and systems analysis. Learn about diverse topics, including the dark web, Linux server administration, cloud computing, android app development and digital forensics.

Learn more

→ study.csu.edu.au/gc-it

Graduate Certificate in Cyber Security

New to cyber security? This is the qualification for you.

Learn a range of topics, including digital forensics, dark web, cloud security and more.

Learn more

→ study.csu.edu.au/gc-cyber-security

Be supported every step of the way

Whichever path you choose, we've got your back. From your application, all the way through to graduation.

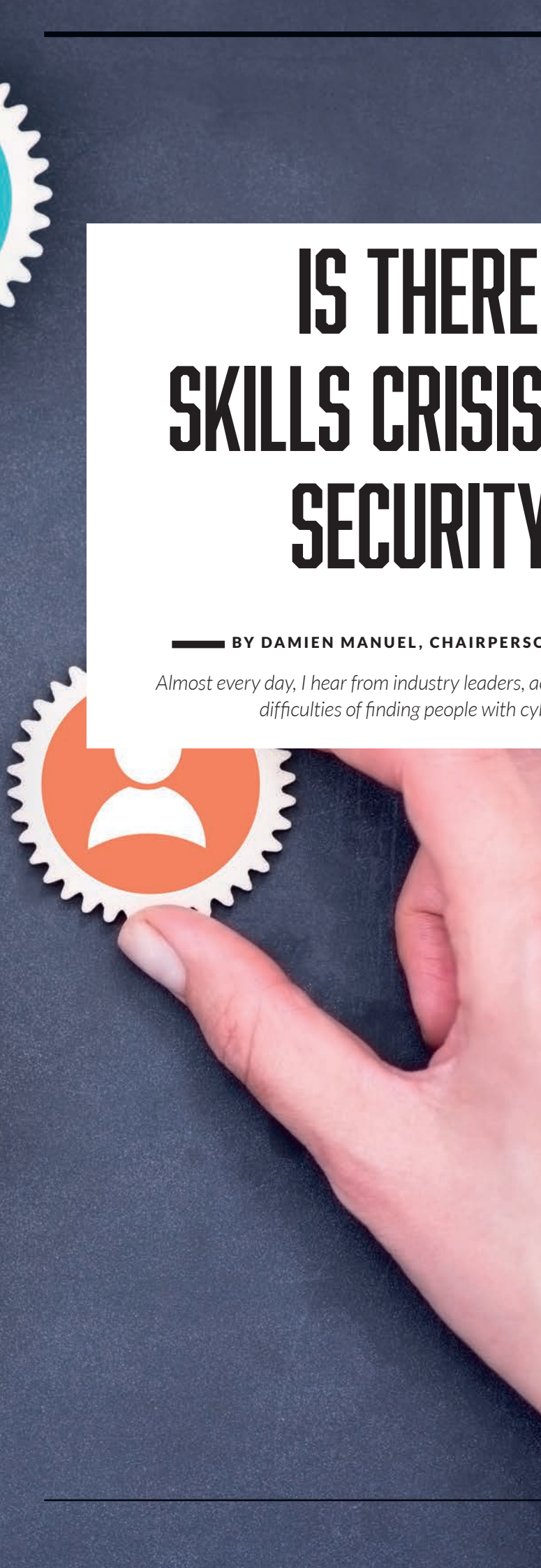
- Admission pathways. Get credit for relevant prior study.
- Online learning. So you can learn while you earn, and fit study around your life.
- Tailored study. Tweak your master's specialisations to suit your interests.
- Financial help. We have more than \$3 million in scholarships available for students just like you every year.
- Academic help. Get advice about your course, a particular project or general study tips.
- Wellbeing services. Access specialist personal support when you need it.
- IT support. Available 24/7, 365 days a year.

Need more information? We're here to help.

☎ 1800 275 278

→ study.csu.edu.au/contact-us





IS THERE REALLY A SKILLS CRISIS IN THE CYBER SECURITY SECTOR?

— BY DAMIEN MANUEL, CHAIRPERSON, AISA, AND INDUSTRY PROFESSOR —

Almost every day, I hear from industry leaders, academic colleagues and industry partners about the difficulties of finding people with cyber security skills in the current market.



I have heard the statement about a 'skills crisis' for the past five years now, but after working in the higher education sector, I know there are thousands of students across the country studying either a Certificate IV (e.g., TAFE), an undergraduate (e.g., a bachelor's) or a postgraduate (e.g., master's) degree in cyber security. So, what is the challenge, and is industry absorbing all the available talent, leaving a net shortfall and making it more difficult to find people with the right level of cyber skills? Or is there a different problem that no-one is really talking about or brave enough to address?

Damien Manuel

With a majority of Australian universities and TAFE institutions teaching cyber security courses, there is a wealth of talent available, from students who have completed up to four years of intensive study, to mature age students crossing over from other backgrounds into cyber security. So how do we make accessing talent easier for both the supply and the demand sides?

WORK-INTEGRATED LEARNING EXPERIENCES

Most tertiary education providers have a team dedicated to working with industry and are able to facilitate student placements or internships in a range of ways. Some of these student placements with industry are actually free, while others are structured to provide tax benefits for industry.

Capstone projects

This is where students work together as a mixed cohort (e.g., software development, IT, business and cyber) of

up to six students, tackling a problem one day per week over 12 weeks. This type of experience helps students to understand how to work in teams and deliver an outcome in a structured project management or agile framework. While the project outcome isn't guaranteed, as it is delivered by first- and second-year students, the end results can often be innovative and a great way to assess future talent. There is no cost to industry to participate in capstone projects – only their time acting as a project sponsor.

Work placements

While still studying, students can spend a short period of time working in industry, either part-time or in a dedicated block. This period ranges in length from 120 to 160 hours, depending on the tertiary provider, and is designed to provide students with an immersive experience while they continue their studies (either undergraduate or postgraduate). It also provides the host organisation with early access to future talent. Typically, this type of engagement is unpaid, but this can vary based on state and territory laws.

Industry-based learning

This is possibly the most important aspect of on-the-job training that most students fail to recognise as a key mechanism to future employment. The reason is that industry-based learning (IBL) is not necessarily part of the course, and often extends the student's course completion date. IBL provides the student with credits towards their course, but may extend the duration of the course from three to six months depending on the IBL length. For example, a course that would be three years may become three years and three months. Often, IBL is undertaken by a student in their final year of study and at a time when they have no other study requirements, ensuring the student can be fully immersed in the experience on site with the host organisation. IBL is a paid placement, and the cost to host organisations is around \$890 plus GST per week per student. Industry can access IBL by providing a position description of the role to the tertiary provider, who then advertises the role among suitable students. The provider then creates a shortlist of candidates and submits this to the host organisation for review. The host organisation then interviews the students of interest. Other than the cost benefits to industry, IBL enables organisations to 'try before you buy' the available talent without any of the complications of the human resources rules and legislation that come with full-time employment. Often, the education provider covers the student under their own insurance, and the payment to the student is made through a scholarship fund, which may have some tax incentives for the host organisation. In general, this mechanism is a win-win for both prospective employers and students, with

approximately two-thirds of students transitioning from IBL to full-time employment with the initial host organisation at the conclusion of their study. The recommended IBL time frame is three or more months to ensure the host organisation can assess the student's suitability and obtain a positive return on investment.

CO-DEVELOPMENT OF COURSES WITH INDUSTRY

Cyber security is not 'one size fits all'. Undergraduate and postgraduate courses should be designed so that key fundamentals are taught to students in the first year or trimester. Fundamental subjects might include an overview of cyber security concepts, including networking security, application security and other key areas relevant to all cyber security professionals. At present, some cyber security courses waste units on subjects like discrete mathematics when students would be better off learning risk management fundamentals, something strongly supported by a majority of chief information security officers (CISOs) and chief security officers (CSOs) in Australia. Students should be able to branch their education into specific areas of cyber security based on their aptitude and interests. For example, the branches or tracks could be:

- › *software development* – for those who want a career in secure software development, particularly in designing, developing and testing mission-critical applications on smart devices, artificial intelligence-driven applications, blockchain-based hyper ledgers and even quantum-based platforms
- › *architecture/design* – for those who enjoy building and designing complex systems leveraging existing and emerging technologies, including cloud-based services
- › *governance and compliance* – for those who enjoy auditing, policy development, and understanding regulations and compliance aspects, both locally and internationally (e.g., CPS 234, PCI-DSS, the General Data Protection Regulation and NDS)
- › *consultancy/advisory* – for those who want to go into project management, consulting or advisory roles, which require a high degree of translation between business and technical concepts, and business acumen. This track would have guaranteed uptake from consulting and advisory firms or those who want to move into managerial roles within cyber security.

GOVERNMENT INCENTIVES FOR BUSINESSES

With so many students completing various cyber security courses across Australia, it is important for the federal, state and territory governments to step up and assist by providing programs to connect industry with tertiary providers. The underlying structures exist to



help ramp up accessible talent; however, this needs to be undertaken in a coordinated and facilitated way, rather than being left to each tertiary provider working with a select number of host organisations in industry.

State governments (such as New South Wales) are leading the way as they examine mechanisms to incentivise industry to access the available talent at TAFE and universities. While they are in their early days, the initiatives being established by the New South Wales Government look promising, and they will have a positive impact on jobs growth and innovation.

ASSESSMENT OF COURSES BY AN INDEPENDENT INDUSTRY BODY OR GOVERNMENT DEPARTMENT

The last piece of the puzzle is ensuring cyber security courses across the country are fit for purpose and can be graded based on the needs of the sector. At present, there is no way to tell if one provider's course is better or if it will produce students who are able to meet the needs of the various industry segments. For example, which course is better if you want to be a cyber security software developer, a consultant, an auditor, an architect or even an analyst? Which course is best if you want a career in cyber law, regulation and policy development? This fundamental issue is why so many job ads rely on industry certifications like CISSP, CASP, CISM or any of the other 300-plus global cyber security certifications as a way to baseline the skills of a candidate and demonstrate a candidate's attitude towards continuous learning.

Providing a mechanism to grade or rank courses based on job function/skills would enable greater

Providing a mechanism to grade or rank courses based on job function/skills would enable greater granularity for students selecting the right courses for them

granularity for students selecting the right courses for them, and for industry in employing students from suitable providers based on the type of roles they are looking to secure. As a side benefit, it would also force providers to teach what industry is looking for, and to adjust courses based on a yearly or 24-month review, as opposed to the typical major course review cycle, which is every three to five years; this pace is too slow for a sector that changes on a month-by-month basis.

So, do we really have a skills crisis, when hundreds of students are completing cyber security-related courses each year? Or are the multiple hurdles in the current system really the roadblock, combined with time pressures on businesses, which make it easier for them to poach talent from the existing workforce rather than tap into the new and exciting talent produced by tertiary providers? Oh, and one last note: not all cyber security skills can be found among people studying cyber security. Just like Ben Landers (interview on page 102), some of the new talent comes from people crossing over from the arts and humanities, bringing with them exceptional communication and business skills to a sector that desperately needs more people who can communicate and translate technology speak into business speak. •

INTERVIEW WITH BEN LANDERS

I caught up with Ben Landers, a student who has completed a master of cyber security, to find out more about his journey and experience.

DAMIEN MANUEL (DM): Why did you study cyber security?

BEN LANDERS (BL): I have an undergraduate degree in fine arts and education, but I always had an interest in digital technologies. I shifted my teaching over the years to teaching information technology, and a couple of years ago I decided to further my technical skills by enrolling in a graduate diploma of IT to try to work out where I wanted to specialise. I started off by doing a cyber security management unit and discovered how diverse the cyber security field actually was. It was an opportunity for me to use my refined communication skills from education, combined with my emerging technical skills, so I switched across to a master of cyber security.

DM: Did you ever imagine you would be studying IT or cyber security? What was it that attracted you to the field?

BL: I think it was falling in love with coding that really started my interest in IT, and not really understanding the number of opportunities in the field. When I initially entered the course, I completed a whole range of units, and cyber security wasn't something initially on my radar. But after studying these subjects, I realised it really aligned with what I wanted to do. It was like opening a can of worms. I thought IT was a huge field, but cyber security is this standalone field that is so large and diverse. Even after graduating, I found that it wasn't possible for me to just say, 'I want to work in cyber security'; I needed to be able to identify what I wanted to specialise in.

DM: So what's next for you, and what would you like to do?

BL: What I'm hoping to do is leverage my communication skills from my education background, so I see my first role in industry potentially being in governance, risk and compliance, or even the security analysis space. My skills are managing projects, and also being the conduit between the technical teams and the business community, helping both sides to understand and translate information in a way that resonates with them. I am able to explain complex technical topics and justify why investment needs to be made in that governance, risk management and compliance space to safeguard the business or reduce the risk.

DM: If you had to do it all again, what would you do differently, or what advice would you give to other people looking to get into cyber?

BL: I would undertake more research into the various areas of cyber security to identify the industry career paths,

rather than being a cyber security generalist. I have enjoyed some of the technical things in the course, and in between trimesters I have undertaken my own projects, just out of curiosity. For example, I completed a unit in network security and learnt about homomorphic encryption. So I developed my own homomorphic encryption e-voting program during the university break just for fun and to learn more about it. My advice would be for other students to think about where you want to be at the end of the course before you get to the end, and to think about what that pathway into industry might look like.

I think it was falling in love with coding that really started my interest in IT

DM: Cyber security isn't 'one size fits all'. Do you think it would be more meaningful and beneficial if students completed a core set of subjects in the first year of study, and then streamed off onto various tracks like secure code development, governance and compliance, consultancy, advisory, and secure system architecture or design, enabling students to 'choose their own adventure' based on their interests and talents?

BL: Yes, I do. The course is good at giving you an overview of cyber security, but I think there is potential to include specialisation streams.

DM: From your perspective, what has it been like trying to break into the market after completing your studies, especially when you came in the top one per cent of students studying cyber at your university? What has the journey been like, and what are some of the challenges?

BL: The biggest challenge for me and other graduates is an employer taking a chance on a new person from university or TAFE. The job ads for cyber security roles really tend to focus on past experience, making it difficult to get a foot in the door. It's also hard for graduates to translate some of their learnings and explain how they could be applied in an industry context. Graduates have dedicated the last couple of years of their lives to working towards getting into the industry, and all they need is that last one step to happen – a placement in industry to learn more and give back. ●

ADVANCE YOUR CAREER WITH POSTGRADUATE STUDY IN CYBER SECURITY AT NEWCASTLE



Are you interested in becoming a cyber security specialist? Do you want to learn how to investigate and reduce the impact of security attacks to enable you to become highly sought after in a growth industry?

Make your next move with Postgraduate Study in Cyber Security at the University of Newcastle.

MAKE YOUR NEXT MOVE

Postgraduate study in Cyber Security at Newcastle comes in two programs: Graduate Certificate in Cyber Security and Master of Cyber Security.

The Graduate Certificate in Cyber Security is targeted at people with computing and IT background but not having knowledge in Cyber Security. This program is aimed for people wishing to upskill in Cyber Security. It also provides a pathway to Master of Cyber Security.

Master of Cyber Security is offered for both people with and without computing and IT background. People with relevant computing and IT knowledge or experience will be offered recognized prior learning.

WHERE IT WILL TAKE YOU

There is a significant shortage of cyber security skills and expertise throughout the world. Developing skills to design secure systems and networks, and skills to detect and counteract security attacks together with the ability to analyse secure network and distributed system protocols are essential to organisations looking to employ security professionals to address the needs and demands of both industry and government.



**MODE: FACE
TO FACE
& ONLINE**



**INTAKE: BOTH
SEMESTER 1 & 2**

By upskilling in this area, you will expand your career options to take on roles such as secure system developer, security system manager, security administrator, cyber security specialist, security consultant, cyber security R&D and security policy analyst.

WHAT YOU WILL STUDY

Graduate Certificate and Master in Cyber Security from the University of Newcastle will provide you with professional qualifications to allow you to specialise in safeguarding cyber security across a variety of industry sectors.

With great flexibility and a variety of courses to choose from, you'll be able to tailor your study to your personal interests and career goals. Some courses available include:

- System and Network Security
- Security Attacks and Mitigation Strategies
- Data Security
- Security Best Practice and Standards
- Legal Aspects of Cyber Security Internet Law
- Project Management
- Work Integrated Learning - Project

LEARN FROM GLOBAL LEADERS

The program design was led by the University's Global Innovation Chair in Cyber Security Professor Vijay Varadharajan with the content of the different courses reflecting the current trends in cyber security and addressing the needs of industry and government. You will learn directly from renowned academics like Professor Varadharajan along with researchers from the Advanced Cyber Security Engineering Research Centre located here in Newcastle. The centre is currently working on globally vital issues such as Cloud Security, Internet of Things (IoT) Security, Secure Virtualisation, Big Data Security, Malware and Security Attacks and more.

**NO.1 IN NSW
& NO.2 IN
AUSTRALIA**

for Learner
Engagement¹

**37%
PROJECTED
JOB GROWTH**

in information security from
2012-2022. This is faster
than the average growth
of any other occupation²

PURSUE THE CAREER YOU REALLY WANT. NOW IS THE TIME.

For more detailed course information and admission requirements visit:
newcastle.edu.au/cyber-security

E postgrad@newcastle.edu.au

P +61 2 4921 8856

¹ Student Experience Survey 2019 – Postgraduate, Computing and Technology

² Bureau of Labor Statistics, 2018



Using threat intelligence in your defence strategy

What can be done to combat contemporary cyberthreats, such as ransomware, other than writing playbooks, practising response plans, following the Essential Eight and blocking known malicious indicators?

ORGANISATIONS WITH A strategic approach to cyber defence will most likely survive a ransomware attack, and considering an attacker's motive may be key to a successful defence. For example, if the motive is purely financial and the ransom demand would cause significant business disruption if not met, what controls can prevent this?

If the motive, however, is to hold intellectual property, customer database or another information asset ransom, should priority be given to controls that detect and mitigate data exfiltration? While senior management's risk tolerance level may be 'we must implement all possible countermeasures,' few organisations will have the luxury of doing so.

Using available datasets to form operational 'cyberthreat intelligence' can help mitigate harmful events such as ransomware attacks. Most importantly, to do so is within the reach of most organisations following the explosion of available open-source tools and datasets. Such 'tactical' cyberthreat intelligence usually

consists of indicators of compromise (IoCs) – technical data such as known bad IP addresses, URLs, emails and file hashes.

This is where the value proposition of computer emergency response teams (CERTs) pays off: not-for-profit organisations providing open-source and member-funded services, passionate teams consisting of analyst and dev-ops and engagement functions, CERTs are trustworthy due to their independent status. CIRCL from Luxembourg famously produces the Malware Information Sharing Platform (MISP) and tactical data feeds, used worldwide by other CERTs including AusCERT, governments and private enterprise.

Many organisations do not have resources beyond the tactical level; however, simply using tactical feeds of IoCs has shown to be effective in detecting or even preventing the initial stages of a ransomware attack. Relevant and concise IoCs may be used in content filters, centralised logging, SIEM or even custom-scripted solutions to hunt or block threats. AusCERT's Malicious URL Feed is an example of a high-

confidence, low-volume feed, usually consumed in an automated fashion but also suitable for manual threat-hunting, depending on the consumer's available resources.

Members of AusCERT's MISP community can study operational intelligence, such as attackers' tools, techniques and procedures, even visually. A 'mind map' connects similar events and data, allowing members to correlate campaigns and understand techniques used in incidents such as ransomware attacks. Organisations can then form strategic plans regarding risks associated with cyberthreats.

Most importantly of all, a collaborative approach must be foremost in discussions regarding cyber defence strategy. A common misconception is that sharing threat information may compromise competitive advantage; however, a particular strength of CERTs is coordinating, anonymising and analysing incident data, and then providing operational intelligence to members – even entire sectors. Have you included your local CERT in your incident response plans? •



AUSCERT

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S
PIONEER CYBER EMERGENCY
RESPONSE TEAM



Incident
Management



Phishing
Take-Down



Security
Bulletins



Security Incident
Notifications



Sensitive
Information Alert



Early Warning
SMS



Malicious
URL Feed



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

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

BECOME A MEMBER TODAY

+61 (0)7 3365 4417

MEMBERSHIP@AUSCERT.ORG.AU

AUSCERT.ORG.AU

Making training work is hard – but letting it fail is even worse

— BY DAVID BRAUE —

The right approach to cyber security training might be the only thing that saves you.

Managing cultural change is always hard, but when it is compounded by the intense pressure of an unexpected event like a pandemic or a cyber security attack, effectively guiding teams through the disruption tests both the mettle of the management team and the effectiveness of previous security training.

Beverage giant Lion Australia faced this issue head-on last year, when its systems were twice compromised by ransomware attacks, forcing technical staff to scramble for a resolution and the rest of the 6000-strong company to be patient as compromised ordering and other key systems were slowly restored.

Cyber attacks, like any other unexpected disruption, 'create complexity and ambiguity for team members,' says Lion's People Service Director Anita Cvetanovski, 'and that's where strong leadership becomes really important for teams'.

Leadership is particularly important in helping organisations to focus on new technologies, redesign process workflows, and introduce new skills and capabilities into the team, she adds, noting that leaders 'really do need to dial up their focus'.

'The role modelling of leadership has far-reaching implications for teams,' she says, emphasising the importance of things like accountability and 'having discipline around how you set expectations, circle back on those expectations, and choose to face challenging conversations in a way that's specific and supportive.'

TRAINING IS NOT A CASUAL JOB

When it comes to challenging conversations, ensuring that employees remain abreast of cyber security considerations remains one of the toughest ones.

Despite years of exhortation, task-focused employees still struggle to internalise the messages they are getting around cyber security. This can lead to ongoing ransomware and other attacks when employees simply forget to do the right thing.





Human error was the culprit in 30 per cent of the 446 data breaches reported to the Office of the Australian Information Commissioner during the first half of 2021. Many others were related to the 289 malicious attacks often facilitated by employee security slip-ups in areas like phishing (involved in 30 per cent of cyber incidents), compromised or stolen credentials (27 per cent) and ransomware (24 per cent).

Given the risks of such an incident, Accenture Security Managing Director Howard Marshall notes in the company's latest Cyber Threat Intelligence Report that business and security leaders need to bolster human defences against these threats by training staff effectively, thoroughly, and repeatedly.

'Enterprise risk management is a team sport that requires a variety of capabilities, a cohesive team, excellent execution of the basics and a willingness to adapt to changing conditions,' Marshall says.

'Security leaders must demonstrate to the C-suite [executives] and the board not only that they understand the criticality of the continuity of operations, but also the importance of working in partnership with the whole business to effectively manage risk.'

WORKING WITH THE BUSINESS

Although the importance of training may seem intuitive, companies' effectiveness at actually delivering it varies dramatically.

Some organisations run regular simulated phishing attacks, for example, and chart their progress by changes in click-through rates from participants. Others implement point-in-time training systems, which build on email security scanning tools to inject a learning moment into a worker's day anytime they click on a malicious URL or attachment.

Another recent Accenture study found a direct correlation between not only the frequency of training, but also the breadth of workers to whom the training was delivered.

Among companies judged as security leaders, almost one-third said that over three-quarters of their users received training for new security tools adopted by an organisation, compared with the nine per cent of security non-leaders that trained an equally large proportion of their users.

Security non-leaders were far more likely – 53 per cent versus 32 per cent of leaders – to train fewer than half of their users on new security tools, highlighting a major weakness in user training that leaves many users well-behind the security curve.

Importantly, Accenture notes, within companies that are the best at training, only six per cent of cyber security attacks resulted in a security breach – compared with 11 per cent of attacks in companies that are less effective at training.

'Right now, cyber security is where health and safety was 30 years ago: disparate, patchy and often optional,' a Deloitte analysis recently noted. 'A more concerted effort will see cyber security undergo a similar evolution to be a key part of employee safety – from initial inductions when they start a role, all the way through their employment at that organisation.'

WHAT TO TRAIN, AND HOW

Deciding just what areas to cover during security training is one issue, since employees will fade out if they're being subjected to theoretical cyber security training that has little bearing on their everyday activities.

To keep their attention for longer, consider targeting or rotating training content across a range of topics, including secure remote working, phishing training, compliance, social engineering, the dangers of malicious software, and information security in general.

Other valuable training topics include removable media, passwords and authentication, physical security, public wi-fi, social media use, cloud security and other key aspects of employees' daily technology interactions.

Over time, however, repeating the same messages over and over is likely to wear thin. Responding to generally accepted ideas that time-poor employees often lose a significant portion of their classroom learning within hours – and retain only a fraction of their learning after a week or two – some training providers have tried different approaches to security training.

Email security firm Mimecast, for one, has complemented its scanning tools with Security Awareness Training, an ever-growing library of training videos scripted for humour and performed by actors.

Fast-growing startup NINJIO has taken that ball and run with it, producing a monthly series of topical anime shorts – voiced by a range of Hollywood talents – that have proven far better at capturing employees' attention and communicating key concepts.

Fun-focused training firms, including Curricula and Digital Defense, have also leaned on humour to drive engagement, while HoxHunt has gamified the process by rewarding users who report its regular simulated attacks.

Despite the serious implications if cyber security training fails to sink in, leaders should frame the training within the broader context of pastoral support that has



become particularly important in the pandemic-era world of remote work.

'Humour is something that has kept me sane over the last couple of years,' Lion's Cvetanovski says. 'Keeping it light during challenging times, such as the ransomware attack or a simultaneous major SAP HANA system implementation, is a great way to support your team members' wellbeing.'

UPSKILLING FROM THE OUTSIDE

Yet, even as companies work to maximise the effectiveness of their internal training systems, external providers – pushed by the pandemic to put classroom learning on ice for the time being – have also been working to overhaul their offerings, splitting up extensive training programs into more modular, accessible pieces.

The federal government's Digital Skills Organisation, for one, recently began a trial of new digital qualifications that use new approaches for online training delivery, while its Cyber Security Skills Partnership Innovation Fund is supporting a range of new cyber security education and training innovators.

Private sector training and consulting firms are also taking up the call. PwC's Skills for Australia program involves a range of cyber security-related VET and DDLS units, expanding its remote-delivered

content through steps such as a recent partnership with Practical DevSecOps.

Companies wanting to bolster their resistance to cybercriminal attacks should combine regular on-the-job training with broader skills-development frameworks to ensure that staff are both aware of changing threats and engaged with their learning.

Time after time, says DDLs CEO Jon Lang, the implications of inadequate cyber security training are becoming painfully clear. At the time of a recent breach of Transport for NSW, for example, just 7.2 per cent of staff had completed basic cyber security training.

'This number really needs to be a lot higher,' Lang says. 'We are living in an age where there are more entry points into the network than ever, and all it takes is one person to make a mistake, or one device to be compromised, to give cyber hackers access to the whole network.'

Blanket training of all staff, not just executives or technical employees, is equally important. "The people being targeted by phishing attacks are usually not cyber security specialists or IT people. They are receptionists, administration or payroll – anybody who has access to corporate emails or servers," says Lang.

'This is why we desperately need to boost the level of cyber education, not just in our critical infrastructure sectors, but across all Australian organisations.'

DO YOUR LEGAL ADVISERS PRACTISE CYBER SECURITY THE WAY THEY SHOULD?

Too many legal firms are protecting the crown jewels with rubber bands, reports David Braue.

The completion of a major content migration by the New South Wales Crown Solicitor's Office (NSW CSO) marks a significant step forward for the organisation's modernisation efforts – and highlights the significant exposure that law firms face as they struggle to keep cybercriminals away from sensitive information about some of the world's most important businesses.

As a legal adviser to New South Wales Government agencies, the NSW CSO had been managing cases and documents using an aging content management solution that was earmarked for replacement as part of a workplace modernisation program that last year saw the implementation of a new practice management system.

The NSW CSO has 'reasonable' cyber security protections in place, but is continuing to 'review and refine the agency's governance and cyber security response posture,' Crown Solicitor Karen Smith notes in the agency's latest annual report, which also states that cyber security 'will continue to be a focus for the CSO'.

In migrating its content management system to the cloud-based Micro Focus Content Manager Select platform, the project – spearheaded by Citadel Solutions – was completed within a week and moved what the NSW CSO called its 'highly sensitive, protected' content into an IRAP and ISO 27001-certified, cloud-hosted platform, enabling encrypted remote access for all staff.

Yet, not all legal organisations are as proactive: one industry survey, conducted by legal technology firm GlobalX and the Australasian Legal Practice Management Association, found that 15 per cent of firms had suffered a security breach and few were aware of their obligations under data-breach notification legislation.

Despite increasing guidance by legal associations, ongoing reports of law firm breaches suggest little has changed in recent years, with 2021 alone seeing breaches at the likes of Australian law firm Allens, US-based Campbell Conroy & O'Neil and UK-based Gately.

Attack mechanisms vary: Allens, for example, was caught up in the massive Accellion file-storage appliance compromise, while the others suffered ransomware strikes.

Cybercriminals are also moving up and down the legal services supply chain, with a series of attacks on bar associations in several US states targeting renewal services that process members' credit card data on the associations' behalf.

A MEANS TO AN END

Due to their roles as consultants on high-stakes business projects, all professional services firms face a particularly high risk of targeting by cybercriminals.

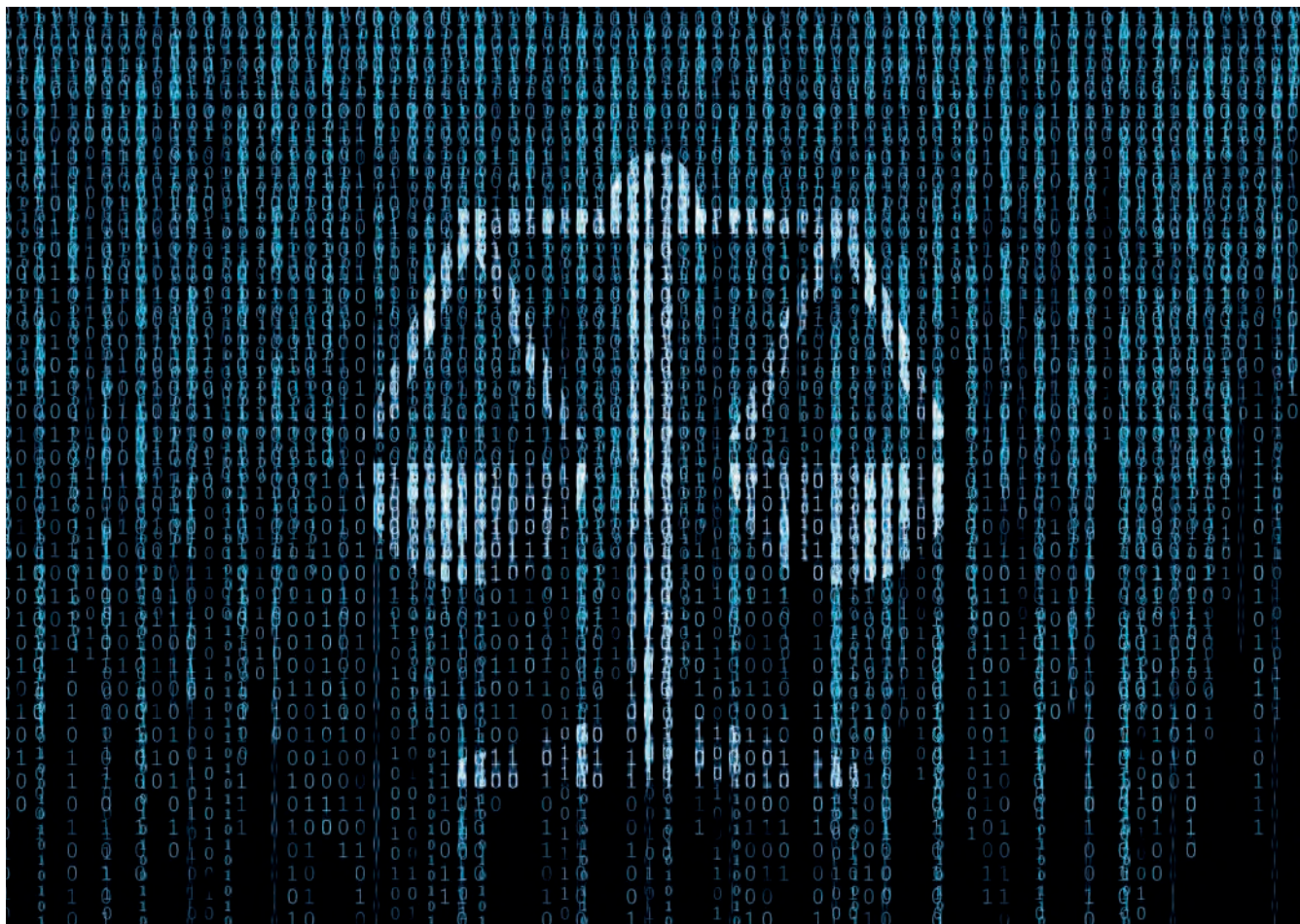
Yet, while many cyber security-focused firms have bolstered their own defences by hiring cyber security teams en masse, legal and other professional services firms have often struggled to free themselves of legacy environments built around highly structured databases of case notes, documents, files and other work products.

Protecting these work products is essential, but strong inertial forces have made digital transformation difficult in the sector – directly leading to data breaches as cybercriminals circumvent protections and plunder data stores for sensitive client information.

Only 43 per cent of law firms are using encryption to protect their files, a recent American Bar Association (ABA) technology survey found, while 39 per cent were using email encryption and just 26 per cent were encrypting entire disks.

If such lax data protection practices are any indication, it is little surprise that Australian legal, accounting and management services firms reported 35 data breaches during the first half of 2021 alone, according to the latest figures from the Office of the Australian Information Commissioner.

Twenty-five of those breaches were attributable to malicious or criminal attacks, including 17 cyber incidents and 10 blamed on human error.



The malicious attacks included six phishing compromises, five cases of breach using stolen or compromised credentials, five ransomware attacks and just one infiltration by other malware – highlighting the major attack vectors that continue to compromise the sector.

Defending against these breaches requires a concerted effort to both modernise the technology protecting it, and to ensure that ancillary issues are addressed – most importantly in the case of law firms, ensuring that user credentials are well-controlled and well-monitored.

Cybercriminals realised long ago that the easiest way into a system is to use legitimate access credentials that will allow them to enter systems unnoticed and download data unchallenged.

‘All of the law firms’ valuable information is hidden in a hardened database far from the perimeter,’ F5 Networks Threat Research Evangelist Sander Vinberg noted during a recent webinar about the company’s 2021 Application Protection Report, which found that the professional, scientific and technical services industry was the fourth most frequently hit sector during 2020.

‘We tend to see access attacks predominate against these kinds of targets because attackers know that a set of stolen credentials is very valuable in terms of conducting reconnaissance within an environment, finding valuable data and exfiltrating it,’ Vinberg said.

Content management applications, such as the one adopted by NSW CSO, are designed to restrict access to case-related information, both for governance purposes and to prevent lateral movement by cybercriminals.

Ideally, of course, legal organisations will prevent cybercriminals from entering the systems at all, in most cases through use of multi-factor authentication (MFA) that challenges users trying to access sensitive legal systems.

Yet, just 39 per cent of firms responding to the ABA survey said they are actually using MFA, with 29 per cent relying on intrusion detection and prevention tools, 26 per cent using web-filtering tools, and 23 per cent using tools to monitor employees’ system usage. Just 12 per cent had implemented biometric logins, which provide another form of MFA that also requires supporting hardware, such as fingerprint scanners or face recognition software.

Given the large-scale targeting of legal firms by cybercriminals, companies considering engaging a firm’s services should take steps to ensure that the firm has appropriately modern software, robust data-protection practices and systems for ensuring that its users can’t be spoofed by cybercriminals with the right passwords.

In a world where cybercriminals are routinely targeting companies’ operational supply chains to find exploitable weaknesses, such precautions should rightly be an integral part of relationships that have become more important than ever.

Given the inevitable complexity of a cyber security response and the need to engage legal experts in any such response, building close working relationships early on is essential to ensure that you’re prepared when disaster strikes – and so is your legal support. •

Leading cyber security from the top: the next challenge for boards

BY MICHAEL DO ROZARIO, PHIL CATANIA AND JUSTIN FOX

New standards to enhance the cyber governance landscape are on the way, and they will have far-reaching effects on how companies – and their boards – deal with cyber security risks.

IN JULY 2021, the Australian Government released its Strengthening Australia's Cyber Security Regulations and Incentives discussion paper as part of its \$1.67-billion 2020 Cyber Security Strategy.

A key recommendation of the discussion paper is the introduction of cyber security governance standards for businesses not currently covered by sector-specific cyber governance rules – around two-thirds of ASX 200 companies. The discussion paper sets out two potential governance standards:

1. voluntary governance standards for larger businesses describing the responsibilities and processes for managing cyber security risk
2. mandatory governance standards that larger businesses would need to comply with within a specific time frame.

These proposed standards will likely define the minimum scope of reasonable cyber security planning and response for companies. This will, in turn, inform the standard

against which boards and other company officers will be assessed in the discharge of their statutory duties under the Corporations Act.

The introduction of the cyber security standards will send strong signals about the steps that a 'reasonable person' in the position of a director or company officer would be expected to undertake in managing the company's cyber risk. While a breach of the standards will not always mean that a governance failing has occurred, the discussion paper points out that the standards will assist the court in identifying the types of cyber risk failures that suggest a breach of directors' duties may have occurred.

To the extent that a cyber breach exposes the company to a breach of law or reputational damages, directors could face an argument that their failure to properly manage cyber risk was a 'stepping stone' that led the company to experience loss in respect of which shareholders should be compensated.

We expect the formulation of the cyber standards to provide ASIC with sharpened tools to better enforce directors' and company officers' management of cyberthreats and risks, potentially opening up the suite of liability and enforcement options under the Corporations Act (e.g., civil penalties, disqualification or orders to pay compensation). We also expect



Michael Do Rozario



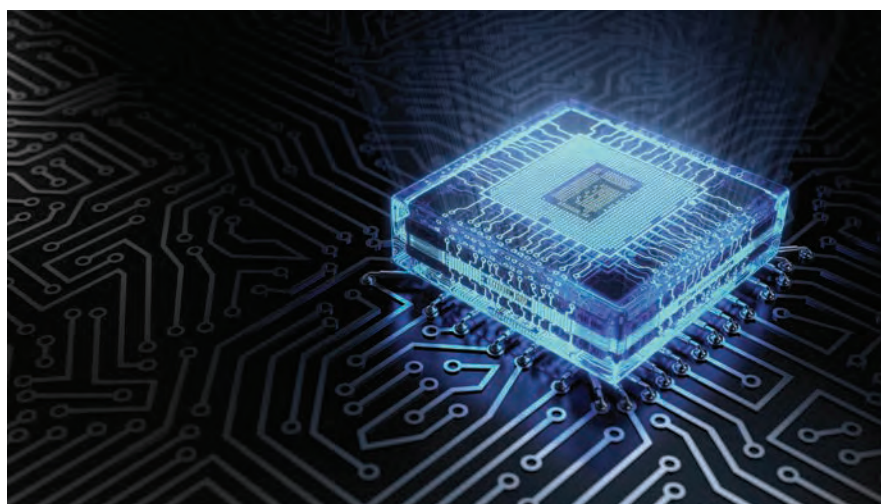
Phil Catania



Justin Fox

the standards to play a significant role in class action and third-party litigation where a failure results in loss. Directors must also bear in mind the specific obligations that may also apply to their organisation, such as the Security of Critical Infrastructure Act, APRA's CPS234 and the ASX's continuous disclosure obligations.

The proposed standards require boards to lead cyber security from the top. The government's proposal will solidify the risk of directors being held liable for breaches of their Corporations Act duties in the event their companies do not have the necessary risk management framework in place to safeguard against cyberthreats. •



Connect with Australia's leading independent law firm.

Tier 1: TMT –
Data Protection

Legal 500 Asia-Pacific 2021

Tier 1: TMT –
IT & Telecommunications

Legal 500 Asia-Pacific 2021

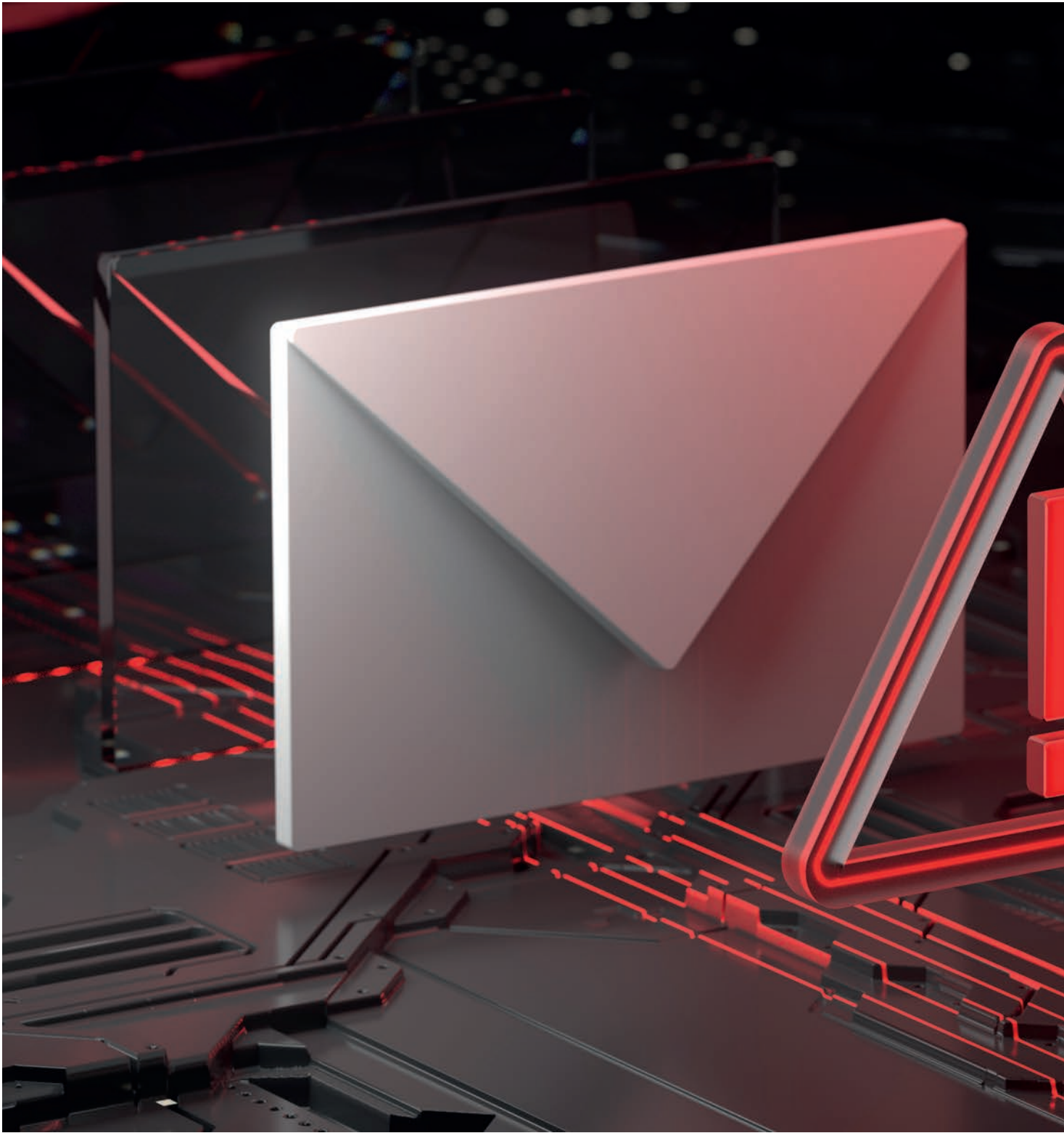
Band 1: TMT –
IT & Telecommunications

Chambers Asia-Pacific Guide 2021

Sydney
Melbourne
Brisbane
Perth
Port Moresby

corrs.com.au

**CORRS
CHAMBERS
WESTGARTH**



Consulting giants

— BY DAVID BRAUE —

Professional services giant Accenture was keeping its cards close to its chest in the wake of an August infection by LockBit ransomware, after which a cybercriminal gang reportedly demanded a \$69-million (US\$50-million) ransom for the return of 6TB of company data.



Accenture confirmed that it had suffered a 'cyber incident', but declined to confirm the amount of the ransom, details of the attack or speculation that it was caused by a malicious insider. The lack of confirmed details revealed little about the status of the company, which only said that it had 'isolated the affected servers' and that the incident had had 'no impact' on its consulting business.

In a cyber security climate in which companies are sharing more information than ever about their breaches, Accenture's low-profile public response reflects much more than just media shyness.

As a fast-growing professional services firm whose recent 21 per cent year-on-year quarterly growth was driven in no small part by its expanding cyber security capabilities, a fully fledged breach by cybercriminals would not only be a headache for the company, but would also potentially compromise the company's reputation as a paragon of cyber security practice.

Notations on the LockBit 2.0 screen confirmed that the cybercriminals are well aware of this: 'These people are beyond privacy and security,' the note says. 'I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases, reach us.'

Accenture's assurances that it had contained the incident were challenged by the publication of data stolen from Ethiopian Airlines and Bangkok Airways, two Accenture clients that were subsequently infected with LockBit – using, attackers claimed, information taken during the Accenture breach.

Accenture strenuously denied the claim, but the sequence of events highlights the stakes in professional services – an industry in which firms both large and small face the dual challenges of protecting systems saturated with confidential information about their clients, while maintaining their reputations as effective, trustworthy sources of business and technology advice.

One of Accenture's fastest-growing businesses, after all, has been its own Cyber Incident Response Service, which helps its clients, and those of partners like insurance giant AXA, to respond to cyber security incidents.

Ironically, as the ransomware infection took hold, Accenture had just published its latest Cyber Investigations, Forensics & Response (CIFR) midyear update – which noted that cyber intrusion activity was up 125 per cent in the first half of 2021 on a year-on-year basis.

Significantly, Australia was the third most frequently targeted country – accounting for 11 per cent of incident volume overall.

'Many organisations today are only securing their core corporate systems and not fully protecting their supply chain, subsidiaries and affiliates,' says CIFR Head Robert Boyce. 'That's why it's critical for companies to have a holistic plan to cover their entire ecosystems.'

'Industries that previously experienced lower levels of cyber attacks during the pandemic – such as consumer goods and services, industrials, travel and hospitality, and retail – should re-evaluate their cyber security posture as increased consumer activity in these industries presents renewed opportunities for cybercriminals.'

A BROAD AND DEEP TARGET

Professional services firms have become regular targets for cybercriminals attracted to their large financial resources and massive repositories of proprietary information, the latter of which is both valuable in its own



right and may provide details to support future attacks on their clients.

Last year alone saw 1892 reported incidents on professional, scientific and technical services (PSTS) firms, according to Verizon's 2021 Data Breach Investigations Report – which confirmed that 630 incidents had led to data disclosure.

Professional services firms were the fourth most affected industry out of the 20 industries the DBIR tracks, with 516 of the incidents targeted at large companies – those with more than 1000 employees – and 793 targeted at smaller operations.

Eighty-one per cent of incidents were executed using system intrusion, social engineering and basic web application attacks, Verizon found, with 26 per cent of incidents involving internal threat actors, and 97 per cent of incidents perpetrated by malicious actors with financial motives.

Professional services companies' 'wildly different footprints in terms of attack surfaces' make it hard to generalise about their security deficiencies, Verizon's analysts noted; however, 'One thing they seem to have in common is their reliance on internet-connected infrastructure, and the risk inherent in that architecture.

'Combine this with social engineering, and you have to worry about not only your infrastructure, but your people's ability to withstand social tactics, as well,' the

DBIR noted, warning that nearly 80 per cent of breaches in the sector were attributed to phishing.

WORKING FROM HOME EXPOSURE

In addition to reflecting their appeal as cybercriminal targets, the high rate of compromise in professional services organisations may have been exacerbated by the COVID-19 pandemic's large-scale push to remote working, in which most firms pushed employees to work from home as a matter of course.

The link between working from home and higher breach rates was evident in VMware's recent Australia Security Insights Report, in which 89 per cent of Australian cyber attack victims agreed that the climate of cyber attacks had increased due to having more people working from home.

Industries such as finance and insurance were particularly driven to working from home, with one Roy Morgan survey finding that 58 per cent of employees in those businesses had set up shop at home.

For cybercriminals, the redistribution of a professional services workforce is a dream come true – and breach statistics reflect this.

F5 recently reported that in 2020, 63.8 per cent of data breaches against PSTS firms were caused by access breaches – the highest of any studied industry – suggesting that despite their strengths as advice providers,



many such companies were still struggling to manage users' access credentials well enough to keep malicious cybercriminals from discovering and abusing them.

CLOSING THE SKILLS GAP

For all their investment in cyber security expertise, the ongoing success of breaches against professional services firms reflects the myriad challenges companies in the sector face as they increasingly inject themselves into the cyber security industry.

Because they are based around acquiring and capitalising on people skills, professional services firms are particularly driven by acquisition – with Deloitte recently completing its fifth cyber security acquisition of 2021 as it firms up its capabilities in crucial cyber security disciplines, such as 5G and Internet of Things (IoT) security.

'We are committed to growing aggressively in cyber security,' says Wendy Frank, Deloitte Risk & Financial Advisory Cyber 5G and IoT Leader.

'There's only a limited number of people with the right cyber tools and understanding,' she adds. 'This is a way for us to [move] in an aggressive fashion.'

Accenture, for its part, recently opened an Adelaide-based Australian Delivery Hub focused on cyber security, national security and advanced technologies, which is expected to employ 2000 people over five years.

Boston Consulting Group late last year appointed Melbourne executive Paul O'Rourke to lead its 400-strong global cyber security group from Melbourne, while PwC Australia – which recently helped the federal government avoid a repeat of 2016's embarrassing online Census – centralised its cyber security and digital businesses in 2020, and launched a hiring blitz that will double its 15 partners and 260 employees by 2024.

French consulting giant Atos has parlayed a large-scale services win with the South Australian Government, as well as success hosting the Tokyo 2020 Olympics infrastructure, into a whole-of-government opportunity after its cloud services and consulting capabilities were added to the government's Digital Transformation Agency Cloud Marketplace.

As with all government contracts, robust security is fundamental to such wins, and it will continue to be crucial for professional services firms expanding their remit and staff numbers across the gamut of cyber security services.

According to Atos Australia Managing Director Mike Green, 'When governments have control over their national sovereign data in the cloud, they can not only provide better and faster public services, but [can] also generate trust and provide leadership in times of challenges and disruption.' ●

Secure your future with cyber security at UQ

CYBERCRIME IS A complex problem. Fighting it requires a deep understanding of key technologies, delving into criminal motivations and driving innovative strategy.

There's more demand for cybercrime fighters than ever before, with experts estimating that Australia will need an additional 18,000 cyber security professionals by 2026 to keep systems and data secure.

The University of Queensland (UQ) offers a postgraduate suite of cyber security programs that bring together social science, technology, business, mathematics and law disciplines, offering a truly integrated learning experience.

Cybercrime is a human problem, and people play a pivotal role when it comes to cyber security. The University of Queensland's specialisation in cyber criminology allows you to gain knowledge of the social science perspectives often lost in the technical side of the field.

Whether it's committing a crime, being a victim of it, preventing it or investigating it, people are central to cybercrime and cyber security, and understanding the human factor is critical.

The cyber defence specialisation will equip you to defend against the growing sophistication of cyber attacks, exploring key concepts including blockchain, cloud computing and artificial intelligence.

According to cyber security firm Checkpoint, cyber attacks on organisations jumped 29 per cent



worldwide during the first half of 2021. Every major business now needs to invest in the security of its data, brand, revenue and legacy – you could be at the front line, providing this protection.

Have an appreciation for mathematics and problem-solving? UQ's cryptography specialisation will allow you to explore encryption methods, decryption and authentication, diverse cryptosystems, error correction and detection, cryptocurrency, quantum algorithms and quantum-safe cryptography.

Cryptography allows us to store sensitive information or transmit it across insecure networks in a way

that stops anyone apart from the intended recipient reading it. It's a vital component in safeguarding digital data across a seemingly endless array of digital platforms and devices. With a cryptography career, you can contribute to this valuable work.

Or you could take the reins with our leadership specialisation. Discover the key role that strategy plays in finding new ways to defend, adapt to and pre-empt threats.

By studying innovative management skills, you'll gain a better understanding of how to implement projects, engage and inspire technical teams, and ultimately, create safer environments.

Become empowered to protect systems, data, organisations and people against a variety of cyber attacks, while providing leadership and advocacy.

Whether you're looking to upskill or enter the cyber industry, be unique and ahead of the game by choosing the Master of Cyber Security at UQ. •



Contribute to a resilient, more productive digital world and enrol now at future-students.uq.edu.au



Study Cyber Security at UQ and go beyond traditional thinking

From six months to two years, our postgraduate suite of cyber security programs bring together students from technology, business, mathematics, social science and law to offer an integrated learning experience, unique to UQ.

Our aim is to create specialists with a deep understanding of cyber security's impact on every aspect of modern life, and to empower cyber security leaders for a resilient, more productive digital future.



Cryptography



Cyber Criminology



Cyber Defence



Leadership



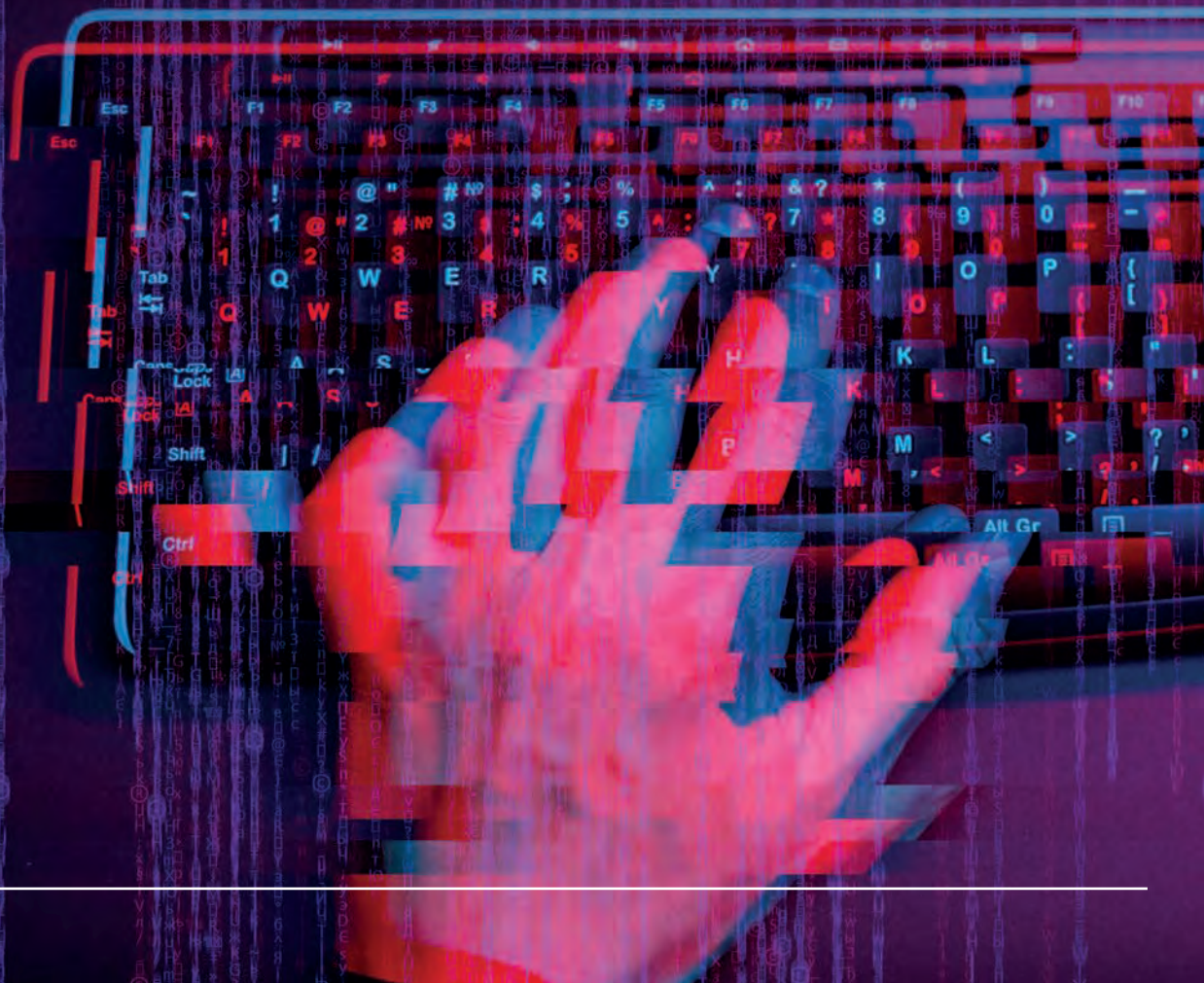
**THE UNIVERSITY
OF QUEENSLAND**
AUSTRALIA

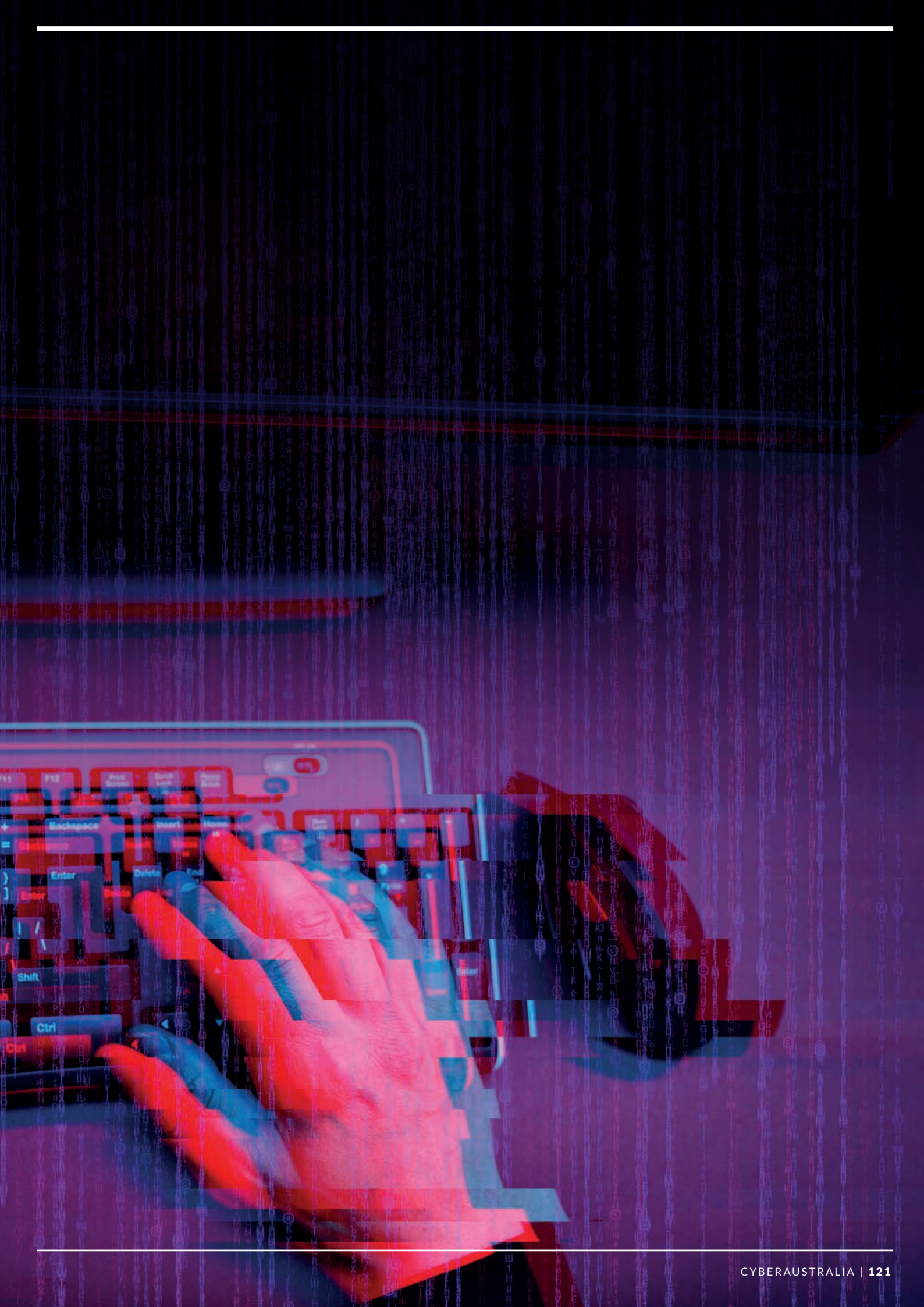
Visit **future-students.uq.edu.au**

CREATE CHANGE

RANSOMWARE GANGS HAVE BUSINESSES ON THE ROPES

Government weighs mandatory reporting and insurance ban as cybercriminals tighten the screws, reports **David Braue**.





Even by cybercriminals' already low standards, the latest iteration of LockBit ransomware, which appeared in recent months, was a pretty shifty move.

Not only was the code designed to lock companies' critical systems until they paid a ransom, but the gang responsible for writing it was, it was discovered, actively recruiting corporate insiders with promises of big commissions for planting the malware inside their company network.

All insiders have to do is provide remote access, email or VPN credentials – or just 'open our letter in our email' and 'launch the provided virus on any computer in your company'.

As if it wasn't damaging enough to flood the market with ransomware-as-a-service offerings, actively trying to recruit moles with privileged access to company systems represents yet another escalation in cybercriminals' devious tactics.

'Ransomware attacks are now a global epidemic, and Australia is a prime target,' Rachael Falk, CEO of the Cyber Security Cooperative Research Centre, wrote in introducing a recent Australian Strategic Policy Institute analysis in which she noted that 'ransomware is scalable, ransomware attacks can be commoditised and ransomware criminals are essentially "guns for hire".'

Malicious insiders were responsible for 35 data breaches in Australia during the second half of 2020 alone, according to figures from the Office of the Australian Information Commissioner (OAIC), up from 23 incidents during the preceding six months. This poses new problems for an industry that has plumbed the depths of ignobility by leveraging the COVID-19 pandemic's chaos to hit companies when they can least afford it.

Ransomware volumes are up 60 per cent over the past year, the Australian Cyber Security Centre warns, with the growing list of Australian victims reading like a who's who of industry; victims since the pandemic began include Toll Holdings, Bluescope Steel, Nine Entertainment, Lion, UnitingCare Queensland, Taylors Wines, Victoria's Eastern Health and others.

Ransomware has been so profitable for cybercriminals that they are winding back their use of other attacks. Security vendor F5 notes that malware comprised just six per cent of US data breaches in 2019, while ransomware alone was involved in 30 per cent of US breaches during 2020.

The OAIC found that the number of reported data breaches actually dropped by 16 per cent during the first half of this year, even as the number of ransomware incidents increased by 24 per cent (from 37 to 46) over the same time.

That means that ransomware was involved in one-quarter of Australian data breaches, reflecting a global trend in which attacks are increasingly being targeted at

critical supply chains that can scarcely afford an hour of downtime, much less days or weeks.

HITTING BUSINESS WHERE IT HURTS

The real-world impact of the attacks was painted in stark relief during June's attack on meat processor JBS Foods, whose Australian and US operations were stalled for days as the company negotiated with cybercriminals, to whom it ultimately paid a \$14.1-million (US\$11-million) ransom.

The incident came weeks after another massive attack in the United States – the compromise of petroleum pipeline operator Colonial Pipeline, which ultimately paid a \$5.5-million (US\$4-million) ransom to restore service. The JBS attack confirmed that ransomware attackers have no scruples about going where the money is, even if it brings critical supply chains to their knees.

With their expanding repertoire of pressure tactics, cybercriminals have also expanded their ransomware demands. According to Palo Alto Networks' 2021 Unit 42 Ransomware Threat Report, the average ransom demand increased from \$1.2 million (US\$847,000) in 2020 to \$7.3 million (US\$5.3 million) in the first half of 2021.

As the LockBit recruitment drive illustrated, cybercriminals are also becoming increasingly creative in the way they push victim companies against the wall.

Last year saw the emergence of 'double extortion' attacks, in which attackers downloaded large volumes of sensitive data before locking a victim's systems, then threatening to release the data online if the ransom wasn't paid. This year, the situation has become even worse.

Security researchers now report the emergence of 'triple extortion' attacks that complement double-extortion techniques with public humiliation: cybercriminals will actually contact your customers, business partners, employees and media organisations to tell them that you've been hacked.

Also emerging are 'quadruple extortion' attacks, with the fourth vector being the threat of denial-of-service attacks that will cripple a company's online operations until they pay the ransom.

'Cybercriminals have continued to adapt their working practices to exploit the shift to hybrid working, targeting organisations' supply chains and network links to partners to achieve maximum disruption,' Check Point Software Vice President of Research Maya Horowitz noted in launching the company's 2021 Mid-Year Report. The report flagged a 13 per cent increase in cyber attacks on Asia-Pacific organisations since the beginning of the year.

Regional companies are facing an average of 1338 cyber attacks weekly, the report found, with the number of ransomware attacks globally increasing by 93 per cent in the first half of 2021.

'Organisations should be aware of the risks and ensure they have the appropriate solutions in place to



prevent, without disrupting the normal business flow, the majority of attacks,' Horowitz said.

CALLS FOR GOVERNMENT INTERVENTION

Countless reports have highlighted how bad ransomware has become, but the biggest change for business professionals is yet to come as politicians, industry regulators, and insurers grapple with ransomware's prudential and financial implications.

Ransomware was once a niche attack that was looked at as something of a novelty by company boards, but cybercriminals' increasing success rate – and the growing recognition that no target is off limits for ransomware artists – has fuelled a growing movement to shift the onus of company protection onto company executives.

Canberra legislators, for example, progressively floated the Ransomware Payments Bill 2021, which would force companies to declare any ransomware payments they made, putatively to help law enforcement agencies prepare to track the payments.

Others considered the idea of making company directors personally liable for cyber attacks, an idea that was incorporated into a recent discussion paper, while some were contemplating banning insurance companies from covering the cost of ransoms.

The latter issue has become a defining factor during the explosion of ransomware. Cyber insurance

providers who had no issue covering \$5000 ransom payments a few years ago are increasingly concerned about their exposure to potential six- and seven-figure ransoms.

That exposure has increased rapidly in countries with more mature cyber insurance markets. Reports suggest ransomware payments accounted for 41 per cent of all cyber insurance claims filed with one major US insurance provider, and Australian insurers could see their premium reserves depleted quickly if the potential ransomware losses aren't curbed.

Ransomware payments have become such a significant issue for Australian businesses that the government recently launched a multi-agency task force called Operation Orcus, which will add 22 staff members to Australian Federal Police-led cybercriminal investigations.

Even as the United States Government consolidates its ransomware response, clarity from Australian policymakers can't come soon enough, Falk says, noting: 'There's a policy vacuum in Australia that makes it an attractive market for ransomware attacks, [and] the problem will only get worse unless a concerted and strategic domestic effort to thwart the attacks is developed.'

She adds, 'Ransomware isn't an abstract possibility. Organisations can't deal with the attacks on their own. There is a central role for government to play... When it comes to ransomware, prevention is the best response.' ●

CYBERPROTECTION AND STRESS: TAKING BACK THE 66

It's estimated that security breaches take 66 days to remediate.

That's 66 days of extreme pressure, anxiety, and hardship on the entire security staff. In a nutshell, teams are in the spotlight and under the gun to get endpoints up and running and productivity back to normal ASAP. If they fail, the organisation may be in jeopardy.

This leads to incredible stress that's impacting both the mental and physical health of CISOs, SOC leaders, and cyberprotection professionals. It's a critical issue that needs to be addressed as we move forward when tackling the increasing number of breaches organisations now face.

Why does stress in security matter?

Simple: As stress builds, employees suffer and so does cyberprotection.

To see the impact of stress on security practitioners, look no further than a recent study by the US National Security Agency (NSA). They report that 88% of US/UK CISOs consider themselves to be under moderate or high stress, while 90% would take a pay cut if it improved their work-life balance. It also revealed they're missing numerous milestone life events as they battle remediation.

Needless to say, this dire situation is causing employees to leave and stress levels to rise. As the same report notes, 66% of SOC workers say stress has forced them to consider changing their careers or leaving their jobs, while 54% of cybersecurity professionals have either left their job due to burnout or have worked with someone who has.

Stress in security is only getting worse.

The rise in stress is causing teams to lose security employees at an alarming rate. As staffs get thinner, there's even more work required for each employee. Stress drivers are also increasing dramatically, including lack of resources, discrimination and lack of diversity (particularly among women), skill shortages, today's digital transformation creating more vulnerabilities, tougher regulations, and of course rising threat levels.

All together this not only adds a greater burden, but also job security stress as professionals fear they're on the brink of termination.

The impact of stress on security itself

As if the strain on cyberprotection professionals isn't bad enough, this stress naturally leads to dangerous security issues. With teams understaffed and under pressure to act quickly, their decision-making is often compromised.

The result can lead to additional breaches, where the cycle of stress begins again. Not to mention an organisation suffering financial and reputational damages from breaches.

Contact Malwarebytes to reduce stress and increase protection

To explore how your team can improve endpoint protection, and get back those 66 days, visit bit.ly/66DaysAISA. Together we can overcome this growing challenge.



IT TAKES AN AVERAGE OF 66 DAYS TO REMEDIATE A SECURITY BREACH.

Get your 66 days back plus enjoy a
FREE month-long “less-stress” subscription.*

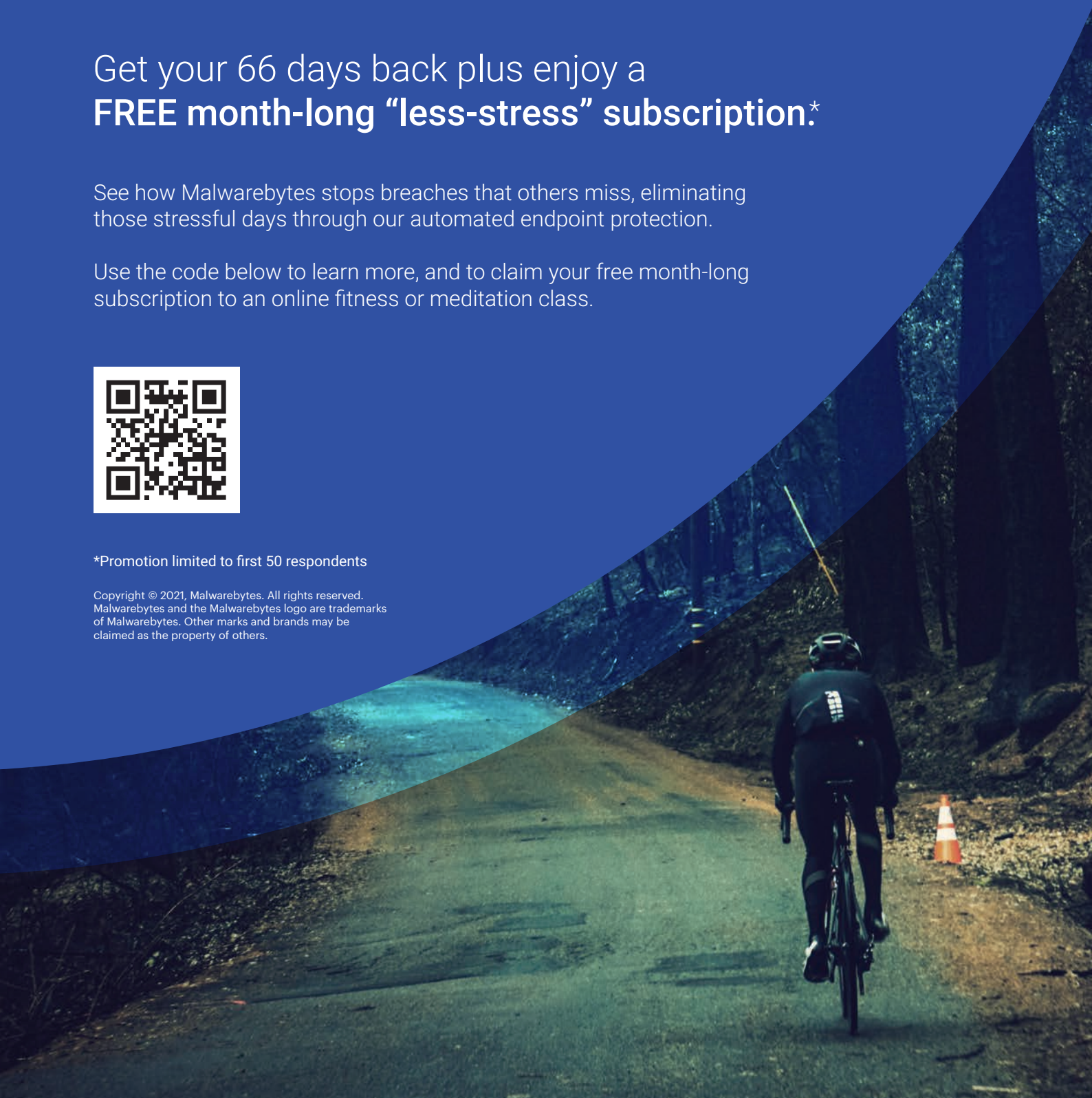
See how Malwarebytes stops breaches that others miss, eliminating those stressful days through our automated endpoint protection.

Use the code below to learn more, and to claim your free month-long subscription to an online fitness or meditation class.



*Promotion limited to first 50 respondents

Copyright © 2021, Malwarebytes. All rights reserved.
Malwarebytes and the Malwarebytes logo are trademarks
of Malwarebytes. Other marks and brands may be
claimed as the property of others.



Six principles for boards on cyber risk governance

— BY SHELLEY DEMPSEY —

The World Economic Forum's Principles for Board Governance of Cyber Risk outlines six principles for boards and business leaders to follow to improve cyber security in their organisations, set strategy, and deal with stakeholders.



As businesses face the increasing acceleration of digitisation, the World Economic Forum Global Risk Report 2021 showed that cyber security failure ranks fourth among the top short-term risks facing entities.

‘As a result of a rapidly changing cyberthreat landscape and proliferating regulations, it has become clear that boards, especially, need stronger foundations to govern cyber risks effectively,’ the report says.

Board directors are advised to adopt the principles outlined in the report when forming an effective cyber risk governance regime. The report specifies that ‘the board needs to understand cyber risk and its role in governing this threat, to perform its oversight function effectively.’

WHO OWNS CYBER RISK?

While the chief information security officer may be some organisations’ foremost cyber risk expert, and the main point of contact for the board on cyber risk issues, directors should look to a variety of executives and managers to ascertain the full impact of cyber risk on an organisation.

Other executives who can support the board’s understanding of cyber risk include the chief risk officer, general counsel/chief legal officer, chief information officer, chief technology officer, chief trust officer and chief privacy officer.

The six principles of cyber-resilience are discussed below.

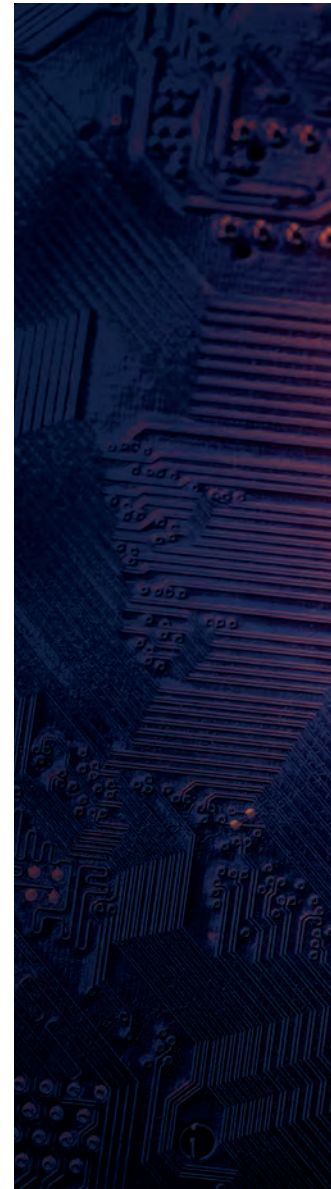
PRINCIPLE 1: SEE CYBER SECURITY AS A STRATEGIC BUSINESS ENABLER

Cyber security is more than just an IT issue. Cyberthreats are persistent, strategic enterprise risks for all organisations, regardless of the industry in which they operate, the report says.

Key considerations for the board are the need to hardwire cyber risks into key operational and strategic decision-making processes, including the adoption of cyber risk as a recurring agenda item for full board meetings.

Boards should also view each major new digital transformation initiative through the lens of cyber risk, determine which board committees should have primary oversight of cyber risk issues, and analyse cyber security issues as part of strategic implications and as part of enterprise risk. Executives should be asked to identify opportunities to use cyber security as a market differentiator or business driver, and analyse business strategy and business model considerations with respect to cyber security issues, the report says.

In a survey of more than 400 global companies conducted by PwC in the fourth quarter of 2020, 52 per cent of board member respondents reported making significant progress in improving customer trust in the past three years as a result of strengthened cyber security practices.



PRINCIPLE 2: UNDERSTAND THE ECONOMIC DRIVERS AND IMPACT OF CYBER RISK

Many business initiatives that drive profitability can also increase cyber risk; so for organisations to make effective business decisions, scenario planning should be carried out to assess risks that could financially impact the organisation, including trade-offs between digital transformation and cyber risk, the report says.

For example, choosing to enter a new market may have substantial business advantages; however, cyber risks – such as additional network connections, theft of intellectual property (IP) and new regulatory exposure – could be just as, if not more, substantial.

Key considerations for the board include:

- › reviewing and approving the cyber risk appetite or tolerance that informs decision-making
- › ensuring that a consistent framework is in place for calculating the potential economic impact and likelihood of cyber security scenarios
- › continually examining comparative measurements and metrics for cyber risk.

The board should receive detailed rationales for the organisation's determination of the materiality of risks based on an indication of their reputational, customer, financial and other relevant impacts.

PRINCIPLE 3: ALIGN CYBER RISK MANAGEMENT WITH BUSINESS NEEDS

By focusing on how to treat cyber risks (through avoidance, acceptance, mitigation or transfer), organisations can build a security profile that aligns with business needs and defined risk tolerances or risk appetite, the report says.

Effective governance requires clear alignment between cyber risk management and business objectives across decisions to do with mergers and acquisitions, business transformation, innovation, digitisation, pricing, product development and market expansion.

Key considerations for the board include:

- › reviewing the organisation's business strategy and drivers (e.g., digital growth) in the context of cyber risk implications
- › requiring management to report to the board on the cyber security implications of their activities
- › requesting written and tested plans to counter adverse cyber events
- › management integrating cyber risk analysis into significant business decisions (e.g., launching a new product or publishing an app).

PRINCIPLE 4: ENSURE ORGANISATIONAL DESIGN SUPPORTS CYBER SECURITY

The internal governance structure of an organisation should integrate and support cyber security on an enterprise-wide basis. The report recommends defining clear ownership, authority and key performance indicators

(KPIs) among all internal stakeholders for critical risk management and reporting responsibilities.

Key considerations for the board include:

- › reviewing the organisational structure to ensure that the cyber security function is represented across the business, internal groups and leadership
- › understanding the basis for, and challenging the assignment of, important roles and lines of accountability for cyber security strategy, policy and execution
- › setting expectations that cyber security and cyber risk functions are to receive adequate staffing and funding.

The board should inspire a cyber security culture across the various levels of the organisation (e.g., compliance, privacy, etc.), as well as ensure that an accountable officer has authority and responsibility for coordinating enterprise-wide cyber risk strategy, and that the organisation has a comprehensive plan for data governance.

PRINCIPLE 5: INCORPORATE CYBER SECURITY EXPERTISE INTO BOARD GOVERNANCE

Considering how pervasive cyber risk has become, many companies are questioning whether they may need a cyber expert on their board.

In determining what is right for an individual organisation, the board should consider whether they would be better served by increasing the entire board's understanding of cyber risk, rather than relying on a single member. The board should also consider the cyber risk management structures already in place, as well as the availability of 'cyber experts' for recruitment and the specific attributes of expertise necessary in a candidate.

While some companies may choose to recruit board directors with cyber risk or cyber security expertise, the report says that boards need diverse sources of cyber security expertise, and should at a minimum seek external industry guidance, and tap into the cyber security expertise of fellow directors and internal resources to oversee the organisation's cyber risk effectively.



Also, as the report notes, ‘In light of the rapidly changing cyber landscape, board directors themselves must continually seek to expand their own knowledge of this topic.’

Key activities the board should be considering are:

- › building relationships with internal stakeholders who can provide expertise to guide strategic cyber security decisions
- › taking part in opportunities to increase board directors’ level of knowledge of cyber risk
- › engaging third-party advisers and assessors who can report to the board regularly to ensure effective oversight of management
- › periodic audits, reviews of cyber security strength and benchmarking by independent third parties
- › regular sessions to update the board on recent cyber incidents, trends, vulnerabilities and risk predictions, using external third parties where necessary to ensure accuracy and competence.

PRINCIPLE 6: ENCOURAGE SYSTEMIC RESILIENCE AND COLLABORATION

Cyber risks can arise from a company’s network of partners, suppliers and vendors. Therefore, ensuring

effective cyber risk strategy includes improving the cyber resilience of industries and sectors, the report says.

Senior leaders must encourage collaboration across their industry, as well as with public and private stakeholders, to ensure that each entity supports overall resilience.

Key considerations for the board include:

- › developing a 360-degree view of the organisation’s risk and resilience posture
- › developing peer networks to share best governance practices
- › ensuring that management has plans for effective collaboration, especially with the public sector, on improving cyber resilience
- › ensuring management considers risks stemming from broader industry connections (e.g., third parties, vendors and partners)
- › encouraging management participation in industry groups, and knowledge- and information-sharing platforms.

To help boards manage cyber security effectively, the Australian Institute of Company Directors has published resources for directors on managing a data breach, and on data and privacy governance. ●

The digital god problem

BY MALCOLM CROMPTON AM, FOUNDER AND LEAD PRIVACY ADVISOR, AND MICHAEL TROVATO, MANAGING DIRECTOR AND LEAD SECURITY ADVISOR, IIS PARTNERS

Legislative enforcement is critical for trusted digital identities.

FOR THE TRUSTED Digital Identity Framework (TDIF) to survive and thrive, legislative backing is a must. It cannot be built simply on contracts and the goodwill of parties. A strong legal framework to protect the users is critical for a trusted and trustworthy system.

Legislation to enforce the TDIF seeks to facilitate more trustworthy exchange of verified claims about relevant attributes without establishing an all-seeing, all-powerful digital god.

TDIF seeks to answer an age-old risk management challenge: to establish a system allowing two parties to reduce the risk that they face, to a point where they are willing to engage each other.

One method is for the relying party to assess claims made by the other party. In the digital era, a claim often verified is 'identity'. This general term usually refers to 'name', birthdate and residential address, but also evidence of long-term presence in society through presentation of years of utility invoices, presence on the electoral roll, and so on.

Verification of inappropriate claims or their inappropriate sharing and use, however, creates significant privacy risk to individuals, as well as security risk.

Hence, the optimal way of viewing this challenge is to see it as an exchange of verified claims about relevant attributes.

VERIFIED CLAIMS ABOUT RELEVANT ATTRIBUTES

As an example, to enter licensed premises, the only relevant claim is whether the individual is over the legal drinking age – not the birthdate or name. If that claim is vouched for by a trusted third party, it is more likely to be accepted as correct.

The digital era creates new risks: if parameters about the claim are also recorded – such as time and location, who the relying party is, etc. – information about the individual's lifestyle patterns emerges.



THE TDIF, DEVELOPED BY THE DIGITAL TRANSFORMATION AUTHORITY AND OTHERS, SEEKS TO VERIFY CLAIMS ABOUT RELEVANT ATTRIBUTES WHILE AVOIDING THE EMERGENCE OF A DIGITAL GOD

The risk to individuals increases if there is only one verifying party, or if the verifying party is able to monitor all verifications of the claims made during individuals' use of that 'identity'.

If that 'identity' must also be used for leading almost all aspects of life, then such an arrangement creates the digital god problem.

THE DIGITAL GOD PROBLEM

A digital god model might sometimes be appropriate – for example, the employer/employee arrangement – however, Australians have repeatedly rejected such asymmetric power constructs, especially if the digital god is a government – showed by the failed Australia Card and Access Card initiatives.

The TDIF, developed by the Digital Transformation Authority and others, seeks to verify claims about relevant attributes while

avoiding the emergence of a digital god. The TDIF also seeks to relieve both the individual and relying parties from having to manage the different 'identities' sought by the relying parties.

The TDIF seeks to achieve all these objectives by separating the relying party from the verifying party: neither is able to know anything about the other through a securely encrypted and Australia-stored digital identity. They are 'blinded' to each other through a trusted intermediary.

The TDIF seeks to make the system more trustworthy, and for that relies on the compliance and honesty from all parties in the long term. This is also to avoid 'function creep'.

Without legislative backing of the TDIF, a range of abuses would likely result with the system consigned to the failed history of prior initiatives. ●



SECURITY & PRIVACY

If you want your
customer's trust,
use a **trusted advisor.**

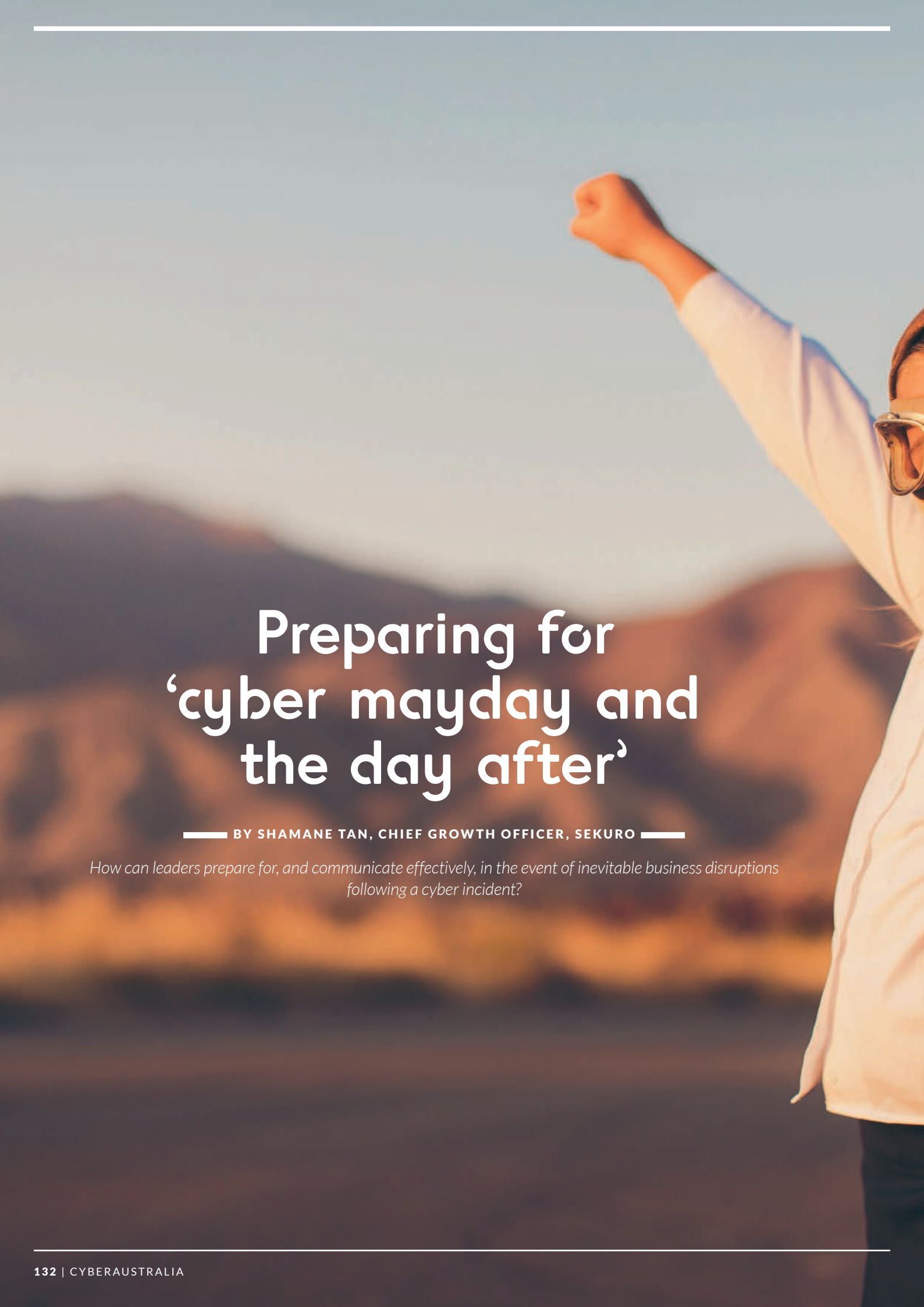
IIS Partners.

A community contributor in trusted
digital identity since 2004.
iispartners.com/identity-management

We help move our clients from compliance
to performance with people-centric,
innovative privacy and security advice,
assuring customer trust.

contact@iispartners.com, +61 2 8303 2438

iispartners.com



Preparing for 'cyber mayday and the day after'

— BY SHAMANE TAN, CHIEF GROWTH OFFICER, SEKURO —

How can leaders prepare for, and communicate effectively, in the event of inevitable business disruptions following a cyber incident?



This is a loaded question, and there is no single answer to it. Chief information security officers (CISOs) are all driven by different business goals, whether they are responsible for managing the risk of launching rockets into space, fighting international crime around the world, safeguarding national security, or running the security of global financial banks.



Shamane Tan

After more than a thousand executive leadership coffees, the book *Cyber Mayday and the Day After* was born, with the aim of creating a connection between these different goals for diverse industry leaders across the world.

The common questions asked by leaders usually include, 'Why do we never learn from our lessons?' and 'Why do these mistakes constantly occur?' Yet, before the business undergoes cyber mayday, have we actually asked the question: 'What is our role in crisis response and disaster recovery? Do we know how we should be communicating in times of crisis?'

As Chief Growth Officer at Sekuro, I lead the security outreach strategy aimed at helping our CIOs and CISOs manage their cyber risk to achieve their business growth objectives. It's a fascinating role as I have the privilege of having a bird's-eye view of the industry landscape, and seeing cross-sector challenges, which strategies have previously worked, and those that have not.

LESSONS FROM THE SKIES

We often have our heads in the ground when a crisis strikes. Yet, if we look up, there is an opportunity to gain a clearer perspective on the problem and subsequently formulate better solutions. There are many lessons we can learn from research literature on aviation mysteries and missing aeroplane events, including how they are communicated.

Crisis communications researcher Kevin Kok-Yew Tan shared with me the details of development and research for the CONSOLE (Coherence, Orientation, Nuance, Support, Ongoing, Leadership, Emotions) framework.

This 'framework is used to guide practitioners on how to break bad news effectively to stakeholders during crises, arguably the first framework integrating established medical protocols with crisis communication literature.'¹ The research examined great aviation crises throughout history and their crisis communication shortcomings against the CONSOLE framework. As I further researched

1 *Breaking bad news with CONSOLE: Toward a framework integrating medical protocols with crisis communication*, <https://www.sciencedirect.com/science/article/abs/pii/S036381117303697>

CONSOLE, I realised the core of it can be effectively applied when dealing with cyber incident scenarios.

The following contains extracts from Chapter Eight of *Cyber Mayday and the Day After*, 'What went right.'

- › *Always state the incident clearly; be specific and consistent (C – for 'coherence').*

'Company X would like to provide an update regarding the status of the data breach of XYZ records (containing names, birth dates and addresses) that were found publicly accessible on a web server managed by a third-party provider. This was due to a human error of an employee of the third-party vendor, and we will provide more updates as we progress in our investigations.'

Do not downplay the seriousness of the incident or the risk of access and misuse, and avoid leaving information vacuums for others to fill. Include the date that the incident occurred, the date in which the company found out about it, and then how timely this communication is. Ownership and accountability needs to be taken.

- › *Communicate messages high in emotional support and exhibit sensitivity (E – for 'empathy').*

'Company X is deeply regretful to have caused any concerns with their customers, as we realised this has damaged the trust between us, and we will work hard to repair that. We are conducting a thorough review of our overall security technology, process and people. We are focused on customer protection and have developed a comprehensive service to support everyone, regardless of whether they were impacted by this incident.'

Next is to state the actions taken to perform the remediation: 'Upon being notified, Company X took the immediate steps XYZ to contain the breach and notified affected individuals.'

- › *Organisations need to take the lead to show the way ahead and the options available to the stakeholders (L – for 'leadership').*

'Company X has established a dedicated website that customers can visit if there are additional questions, or call [a dedicated call centre/toll-free number] for direct assistance.'

- › *Don't forget to mention support teams and channels (S – for 'support').*

'Company X will continue to exert great effort in providing customers with any assistance during the ongoing investigation of the incident. Company X remains committed to achieving the best outcome for its customers and will take all reasonable steps necessary to achieve this.'

It is important to state actions or changes that will be taken moving forward to prevent future occurrences.

- › *Organisations need to provide easy-to-understand technical information (N – for nuance) and have a strong understanding of their audience, as well*

as anticipate stakeholders' concerns or questions (O – for orientation). Lastly, communication needs to be continuous and a two-way engagement (O – for ongoing).

Provide stakeholders with the opportunity to address their concerns and questions, and look at a variety of platforms to reach out to the affected individuals. Over-notification is not an issue – on the contrary, individuals are more appreciative of receiving direct and comprehensive communications.

SEEDING IN ADVANCE

While information might not always be available, instead of letting online discussions or rumours add fuel to the fire, having an official and verified source (that is also the most senior person in the company) that provides information and updates is vastly beneficial, and maintains control of the narrative.

The current communication landscape across the world has seen many misinformation sowers leveraging silence, which can be detrimental to your organisation's reputation. Hence, crisis communication processes should be planned before a crisis, where third parties can also be seeded as advocates to offer an alternative voice for your organisation.

We all know the importance of running regular war-room exercises and crisis simulations as a key strategy to build on any organisation's cyber resilience capabilities; however, in planning such scenarios and digital communication at a global scale, the cultural context is a key nuance to be attentive to. A crisis can be fuelled by opportunists, especially if there are racial, religious or political insensitivities involved.

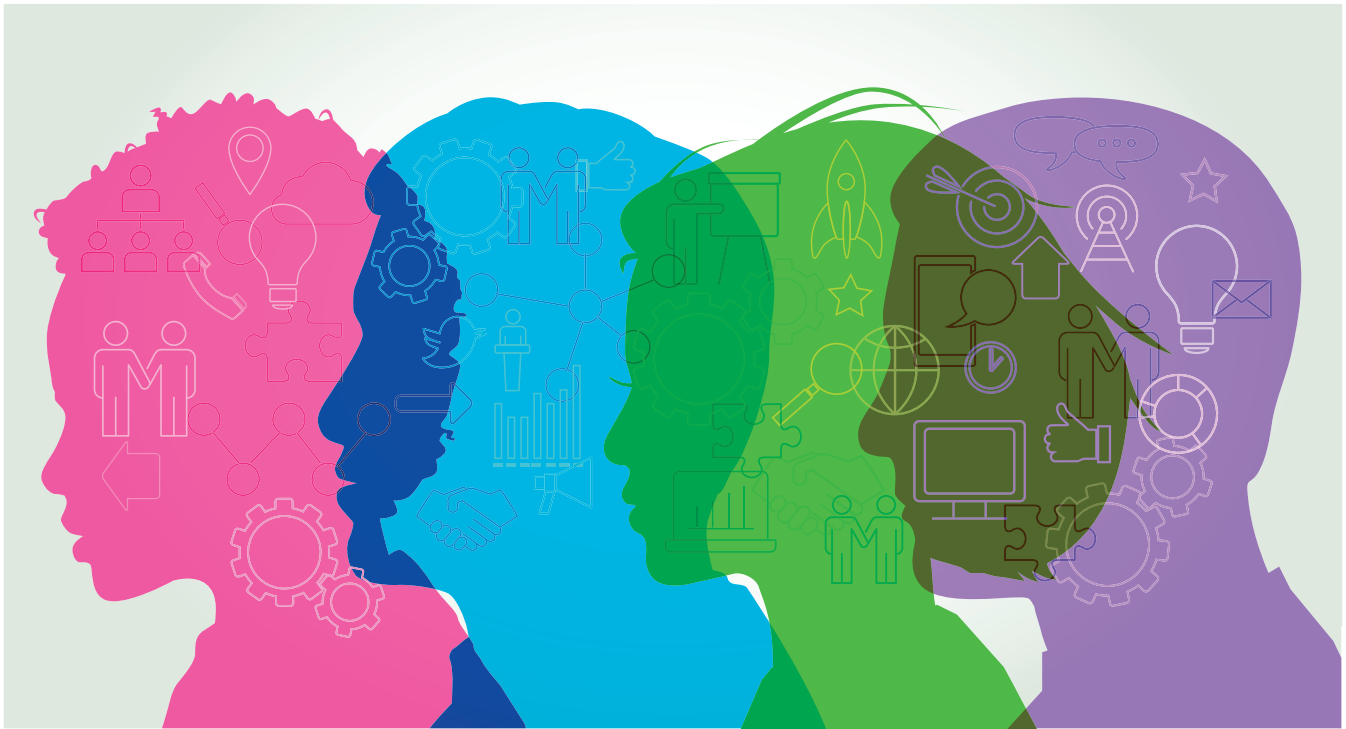
Melissa Agnes, CEO at Crisis Ready Institute and a globally recognised authority on crisis preparedness and reputation management, highlighted the Crisis Ready Formula, which is detailed in *Cyber Mayday and the Day After*; however, for the purpose of this article and topic, I would like to concentrate on the 'decisive' element.

It is critical to take a decisive stance that aligns with your organisation's values. Know that you will not appeal to or please everyone, as controversy segregates. In these times, make a decision that you will not go back on, and ensure that your team understands that some stakeholders will most likely not be happy.

COMMON EXCUSES FOR REPEATABLE MISTAKES

The timeliness of your crisis response will be based on the severity of the crisis. There are different degrees of cyber maydays that organisations across sectors have experienced over recent years, and there are many lessons we can learn from studying these true stories.

How many of us have taken time to examine the actions of those leaders who have been in crisis mode and had to take their businesses through a disaster?



With the hindsight they now possess, I find that such lessons are often invaluable in helping us to have better foresight and action plans. ‘Start early,’ they always advise. The midst of a crisis is not the time to start thinking or planning.

Yet, how many of you have found these common excuses come into play when best practices are not implemented?

We did not have the time

We could not afford it

The business didn’t understand why it was necessary

We tried it before, and it didn’t work

It’s too hard

To be honest, we were afraid of what we might discover

In Chapter 11, ‘Turning cyber incident lemons into organisational lemonade,’ I provide a comprehensive coverage of tips and solutions to help overcome these common excuses. But for our security leaders, here are some question checklists I would first suggest to challenge your thinking and ensure you are asking the right questions.

- › Where are we spending the bulk of our time? Are we allocating our time proportionately according to the criticality levels of risks?
- › Are there other areas we are spending our budget on that can be reallocated? How does our budget align with the company’s strategy and business risk?
- › What is the current security awareness culture like in the leadership team and among the different divisions?
- › What was the organisational environment like before, when our approach didn’t work? How can change be executed differently this time? Have we looked at the mechanics of influence?
- › Have we tried getting allies so that it is not just us fighting an organisational battle? Are there other battles that might result in better outcomes? What are some other, smaller initial commitments we

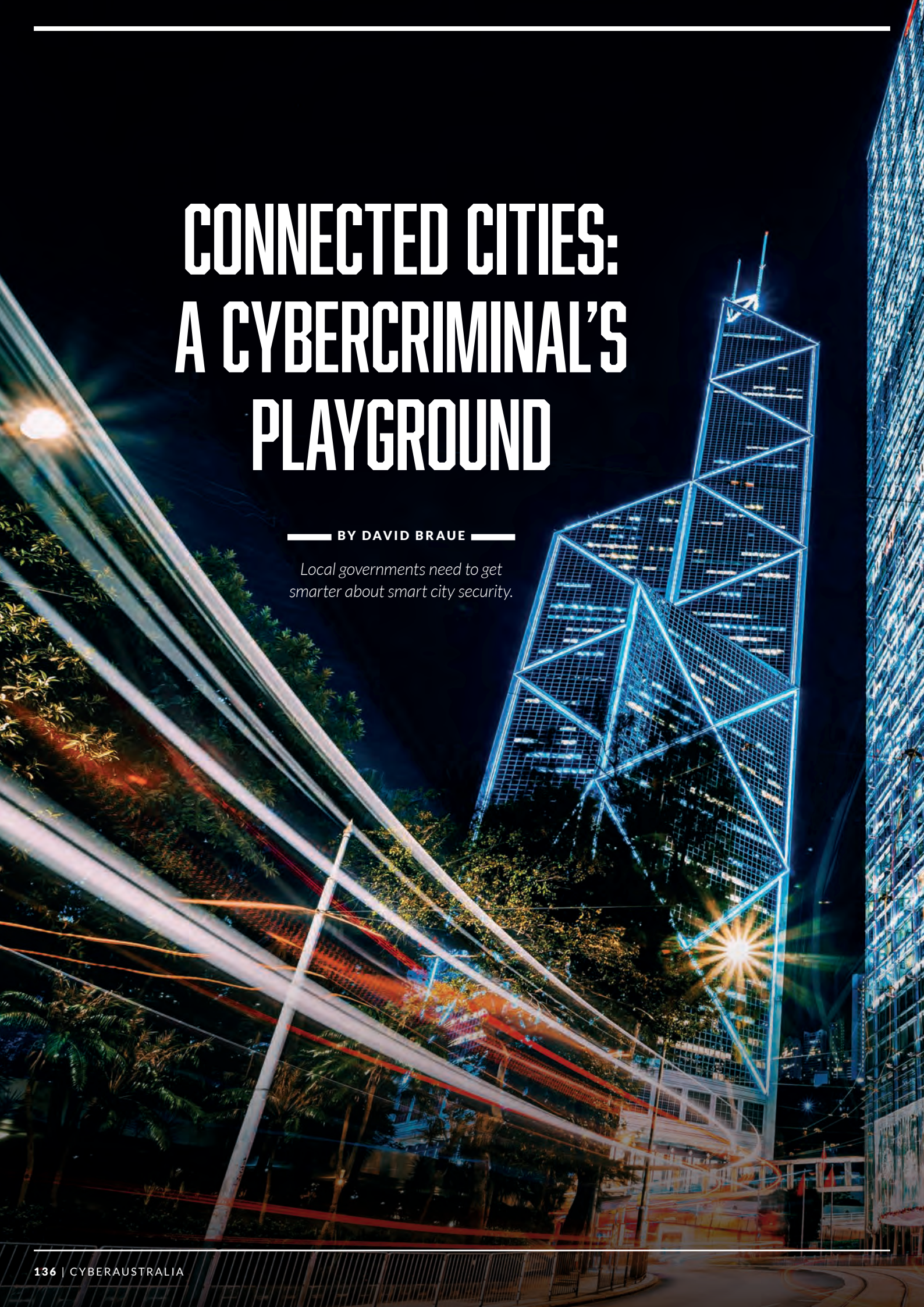
can focus on securing from our stakeholders first, then working on getting more buy-in from there?

- › Are we comfortable with not knowing what the malicious attackers out there know about our company? How are we managing your risks if we do not know what needs to be managed?

As Preston Miller, former NASA Jet Propulsion Lab CISO, shared on my *Mega C-Suite Stories* show, security leaders ‘should be in the office of KNOW and not in the office of NO’. Let’s not be too quick to always put up objections, and instead be on a mission to educate and impart knowledge. To add value, knowledge that is communicated has to be easy to understand, and relevant to your audience before it is effective. ●

As one of the most established women in the fields of technology and cyber security, Shamane Tan is the Chief Growth Officer at Sekuro, leading the security outreach strategy with the C-suite and executives. Recognised by IFSEC as one of the global top 20 cyber security influencers, the *Cyber Risk Leaders* author was also recently listed in the ‘40 under 40 Most Influential Asian-Australians’ and given the Highly Commended award by the Australian Women in Security Network as the One to Watch.

A TEDx speaker and podcaster, Tan is also the founder of Cyber Risk Meetup, an international community and platform for cyber risk executives to exchange learnings. She is passionate about educating, raising awareness and fostering collaboration within the cyber risk ecosystem. *Cyber Mayday and the Day After* is a collection of true cyber emergency stories, as well as a leadership guide to preparing, managing and recovering from inevitable business disruptions. Co-authored by Tan and Dan Lohrmann (former CSO of the State of Michigan), and published by American multinational publishing brand Wiley, the book will be available in the United States from 16 November and in bookstores around the globe (including Australia) soon after.



CONNECTED CITIES: A CYBERCRIMINAL'S PLAYGROUND

— BY DAVID BRAUE —

*Local governments need to get
smarter about smart city security.*





When Victoria entered its latest lockdown, one Melbourne shopping centre rapidly scaled back its facilities' power consumption by leveraging a specialised CIM analytics platform integrated with its building management systems (BMS).

By leveraging detailed data about the building's environmental systems, the facility's manager, GPT, was able to remotely adjust over 300 BMS parameters, shifting the facility into a lower-power lockdown mode within hours after the lockdown was announced.

The process used to take two weeks from go to whoa, but the increasing automation of the process allowed GPT to complete the process in just 90 minutes.

Such applications represent the cutting edge in building management systems, which have become smarter and more adaptable as automatic systems monitor every aspect of their operation.

Yet, such automation also increases the risk of smart cities, which are increasingly leveraging artificial intelligence (AI) and pervasive Internet of Things (IoT) technologies to make cities smarter, more environmentally friendly, more responsive to residents' needs, and more exposed to a whole new world of cyber security threats.

Just as GPT's operators were able to scale down power consumption and remotely reconfigure environmental systems, malicious cybercriminals could use such a system to raise temperatures in a facility, lock escalators at top speed, change circulation patterns to concentrate potential COVID-infected air rather than venting it, turn lights on and off at random, or whatever else tickled their fancies.

BMS operators have naturally worked hard to avoid such compromises, but they are just one part of a broader risk surface that is rapidly expanding as increasingly automated smart cities become the norm.

Local government systems have already been hit with ransomware attacks launched through system compromise – and it's happening frequently enough that the Australian Cyber Security Centre recently partnered with the Australian Local Government Association on an awareness campaign to ensure local governments remain vigilant to the new threats they face.

Former White House CIO Theresa Payton, now CEO of security firm Fortalice Solutions, recently predicted: 'A 5G smart city will be held for ransom... I don't see anything happening now that tells me that this prediction is not going to come true.'

MANY WAYS TO BE SMART...

Making cities smarter has become a driving goal for administrators the world over. The Institute for Management Development's Smart City Index 2020 currently lists 109 different smart cities, which it

defines as 'an urban setting that applies technology to enhance the benefits and diminish the shortcomings of urbanisation for its citizens.'

Australian cities were well-positioned in the top 20, with Sydney (ranked 18) and Melbourne (20) pipped by Brisbane (14), while the top four comprised Singapore, Helsinki, Zurich and Auckland.

Each city is pursuing a different mix of smart city technologies depending on their attributes, but the idealised end state for smart cities is being writ large by Japanese market giant Toyota, which this year broke ground on a completely new, 70-hectare 'Woven City', layering smart city innovations on a framework of completely renewable solar and hydrogen power.

Amenities range from pedestrian-free roads designed for electric autonomous cars, to AI-powered IoT sensors that optimise power consumption, to smartphone-driven government services and robotic assistants helping the city's populace throughout their everyday lives.

City designers are using digital twin technology to design, model, test and change smart city designs more than five times faster than using conventional processes.

While the Woven City may demonstrate smart cities' long-held efficiency dream, its intrinsic reliance on IoT technologies represents a lingering weak spot given their ongoing compromise by malicious cybercriminals and nation-state actors.

Security firm Kaspersky recently observed a doubling in attacks on IoT targets during the first half of 2021, with some 1.5 billion attacks on smart devices as attackers mercilessly probed connected devices for exploitable vulnerabilities.

'The one thing all of these processes have at their core is that they are... supported by cyber-physical systems,' says Gartner VP Analyst Katell Thielemann. 'That's why the focus of security and risk management leaders really needs to change.'

Apart from conventional ransomware, data theft, system manipulation and the like, smart cities' blurring of the lines between human spaces and technology-driven processes – the 'cyber-physical interface' – opens the door for a whole new range of compromises.

Early examples include the exploitation of an HVAC control system to perpetrate the massive Target data theft, the hacking of a fish tank thermometer



to target an American casino, and ongoing concerns about abuse of data collected by surveillance systems in public spaces.

By building entire systems around such technologies, smart cities reframe the risk in different terms. Think about a self-driving smart city car being hacked to kidnap a VIP passenger, security cameras being re-aimed during a crime, denial-of-service (DoS) attacks impeding the operation of key public safety systems, or traffic management systems directing drivers across bicycle lanes against the light.

‘These types of attacks will continue as more and more cyber-physical systems are deployed,’ Thielemann says. ‘When the attack surface is now expanding in both the cyber and the physical world, those bad actors are going to take advantage of that.’

...BUT ONLY ONE WAY TO BE SAFE

Credential theft, identity spoofing, privacy breaches, manipulation of smart meter data – conventional cyber security risks are magnified in pervasively connected smart cities, with one recent survey of 76 cyber security experts concluding that the riskiest smart city technologies include emergency alerts, street video surveillance and smart traffic signals.

‘Local officials should consider whether cyber risks outweigh the potential gains of technology adoption on a case-by-case basis,’ the researchers say, ‘and exercise particular caution when technologies are both vulnerable in technology terms and constitute attractive targets to

capable potential attackers, because the impacts of an attack are likely to be great.’

Recognising the digital push that the COVID-19 pandemic has given to smart city efforts, researchers and consultancies have this year compiled lessons learnt to date into new guidelines that finally offer clear guidance for local governments struggling to align smart city theory and practice.

While 80 per cent of smart cities acknowledge their legal obligations for privacy and data protection, for example, a recently published World Economic Forum (WEF) analysis notes that fewer than 25 per cent actually conduct privacy impact assessments when deploying new technologies.

With few cities having formal cyber security plans or cyber security experts to design them, the report warns, even world-leading smart cities have ‘serious gaps’ and must improve their governance in order to build resilience and improve technology practices.

Cities struggling with this process received new support from the UK-based National Cyber Security Centre, which this year published formal guidelines that complement physical security guidelines to help authorities manage security considerations when building smart cities.

‘The pandemic has been defined by home-working and remote education,’ the WEF report notes, ‘but many cities lack the digital infrastructure needed to support or sustain this shift... City leaders need to take a longer-term view and identify governance gaps before they become material risks.’ ●

SOURCE CODE SECURITY

— BY DAVID BRAUE —

Find the weaknesses in your software supply chain before the cybercriminals do.





As the security world processes the SolarWinds hack, companies must decide how proactive they will be about ferreting out vulnerabilities.

The world was rightfully stunned by the recent discovery that allegedly Russian operatives had piggybacked on a commercial network security application to infiltrate dozens of businesses and government agencies, going undetected for months. Yet, as the post-mortem from the hack of SolarWinds' Orion tool continued, many quickly pivoted towards the even more important question: what other tools might already have been compromised in the same way?

In an era when applications are increasingly complex, and comprise myriad components and interlinked services, SolarWinds' compromise was a blunt reminder of just how exposed many companies' software supply chains remain.

Its discovery happened by chance, after security staff at security research firm FireEye noticed an existing employee had begun remotely accessing the company's servers by registering a second device to the account of a legitimate employee.

When the employee was questioned about the second device, he denied knowing about it. This set off a chain of events that led from FireEye's two-factor authentication system all the way – after thousands of hours of forensic work – to reverse-engineering its Orion installation and discovering that the system contained around 4000 malicious lines of code.

In an era when applications are increasingly complex, and comprise myriad components and interlinked services, SolarWinds' compromise was a blunt reminder of just how exposed many companies' software supply chains remain

'You never want to just start by reverse-engineering a platform you bought from somebody,' FireEye CEO Kevin Mandia told a recent Aspen Institute webinar, but 'when we started investigating and looking at thousands of computers trying to figure out if they had been accessed without authorisation, the earliest evidence of compromise for us kept coming up [as] a system that harboured the SolarWinds product.'

Yet, while reverse-engineering and analysing code is a core part of FireEye's capabilities, for most companies such a breach might have gone completely unattributed and undetected – as it was at NSW Health, Rio Tinto, Serco

Asia Pacific and others of the reported 18,000 companies that use Orion.

With hundreds or thousands of applications running inside most businesses, then, the potential attack surface of such a breach is significant – and most companies are far less capable of detecting such an attack if it had happened.

It's not the first time the software supply chain has been targeted, notes Katie Moussouris, Founder and CEO of Luta Security.

'Microsoft itself was the original supply chain attack vector for most organisations. We try to make this into a different thing and recategorise it as all being new,' she says – citing cases such as 2017's CCleaner compromise, where malicious code was digitally signed to circumvent detection – '[but] every single component of this attack is not new'.

WHAT'S OLD IS NEW AGAIN

The SolarWinds breach's enmeshment with Russian counterintelligence efforts, and its timing coincident with the US election, have raised alarms worldwide – but supply chain security is something that every developer deals with, or should be dealing with, every time they integrate an open-source software module or use an API to link with a cloud-based service.

Security holes are being discovered continuously, and the COVID-19 pandemic made things even worse, with crowdsourced code-scanning firm Bugcrowd recently reporting that the number of priority one submissions – reflecting critical software vulnerabilities – increased by 65 per cent during 2020, while the total number of vulnerabilities grew by almost a quarter year-on-year.

This uptick may represent increased scrutiny of software by locked-down security researchers with plenty of spare time, but other metrics suggest that increasingly security-conscious user communities recognise the importance of addressing security concerns earlier in the software development life cycle.

Eighty five per cent of users in Snyk's recent State of Open Source Security report believe developers are responsible for open-source security, while 55 per cent believe security teams should carry the burden, and just 35 per cent see security as an operational issue.

Those findings suggest significant support for greater adoption of development, security, and operations (DevSecOps) that spin off of DevOps focused on rapidly testing, remediating and iteratively stamping out security vulnerabilities as the systems development life cycle progresses.

Detecting security issues earlier rather than later promises fewer problems later on – particularly since, as Snyk found, 34 per cent of identified vulnerabilities are fixed in fewer than 20 days, while 36 per cent take longer than 70 days.

These time frames have direct implications for the speed at which fixes – even for serious open-source

vulnerabilities like 2014's Heartbleed and last year's Ripple20 Internet of Things device compromise – can be created and tested, pushed to users and propagated across user environments.

The fact that the SolarWinds breach persisted for months highlights the risks attendant on slow vulnerability resolution that is still more common than companies would like.

Around 30 per cent of large-company breaches analysed in Verizon's Data Breach Investigation Report 2020 took months to discover, and just under 10 per cent took years. Cybercriminals are often left to their own devices because they are better at finding software vulnerabilities than companies are at patching them.

WHAT'S IN THE SECRET SAUCE?

Aiming to improve the discovery of vulnerabilities and the communication of these to corporate software users, many developer advocates are pushing for broader use of software bill of materials (SBOM) that maintain detailed registers of the components that corporate applications use.

The US National Telecommunications and Information Administration (NTIA), for one, is finalising an SBOM standard called NTIA Software Component Transparency, which has gained momentum as a common mechanism for developers to track the software components they use – and security analysts to more quickly narrow down potential vulnerabilities without having to find someone capable of reverse-engineering their applications.

Given the natural delays attendant in updating vulnerable software, however, many security engineers are looking for a more actionable response to application vulnerabilities.

'At the end of the day, do those of us in the trenches really care who it is?' asks John McClurg, Chief Information Security Officer at security and mobility firm BlackBerry. 'I'm not allowed to hack back, and I can't go to war with them – not that I have the resources any more in this space.'

'But I will be more interested in what the indications of compromise are, so I can take a defensive posture and figure out what it was that I was doing that allowed them in in the first place.'

By having a ready inventory of installed software and its subsidiary components, companies would be better



positioned to quickly meet this goal by evaluating and re-evaluating their security exposure as new vulnerabilities are discovered.

The process can be tied into existing security automation processes, helping to remove the variability of human dependence, and supporting the actioning of security processes and procedures – and speeding a response that could be critical in finding and blocking unwanted outsiders.

Introducing more structure around the detection and reporting of cyber security vulnerabilities could become invaluable if government regulations and industry best practices can support scaling such processes to national or global levels, notes John Carlin, Chair of the Aspen Institute's Cyber & Technology Program.

'Currently, there is insufficient reporting, and perhaps we're not paying much attention on the reporting, or how to defend our systems or learn from it,' Carlin says.

'Right now, we have a patchwork of reporting requirements that primarily fall around the theft of personally identifiable information – but in this type of hack, that's often not an issue and doesn't trigger reporting.'

Yet, many companies, Moussouris notes, are reluctant to share details of their compromises and have found a middle ground in efforts such as bug bounties – which, she says, are 'low-hanging fruit'.

The question about those bugs, she says, is, 'Why didn't they catch them themselves? Why are they congratulating themselves on this performative security? More times than not, they are suffering from some level of cyber security hygiene negligence in some area – and they missed something, or something was left unsecured that should [not] have been.' ●



The future of cloud security

BY ERIC JOHNSON, SENIOR INSTRUCTOR, SANS INSTITUTE

AS IT WORKLOADS move to the cloud, organisations face a fundamental shift in how to develop and deliver systems, as well as in their security practices. Deploying and running production systems has become abstracted from the underlying hardware and network. Infrastructure is defined as code, and operations teams work through cloud service APIs. With the cloud providers abstracting and presenting functionality through services and API calls, system and network implementation occurs using code.

KNOW THE CODE

Cloud security moves security teams away from selecting and implementing network appliances and writing checklists towards Security as Code: reviewing infrastructure and service configuration templates, understanding how to correctly use cloud security services and APIs, and writing automated tests and continuous compliance policies.

Security professionals need to know how to read and write infrastructure as code. They must understand and use modern

software development tools to catch security misconfigurations, and to build guardrails in the cloud. They need to understand and use continuous integration/continuous delivery (CI/CD) build pipelines and programmable configuration management tools to automatically check and enforce security and compliance policies on every change. They need to understand different cloud architectures and platforms, including both their strengths and weaknesses. They also need to do all of this at high velocity, without getting in the way of delivery.

NEW SKILLS AND NEW THINKING ARE NEEDED

Thus, security becomes security engineering: writing security and compliance policies in code; reviewing, scanning, and testing cloud infrastructure code and service configurations; and understanding how application development and system engineering teams work, and helping them to find and implement tools to inject security testing directly into development. Security as Code requires new skills, new ways of



Eric Johnson

thinking, and new workflows: more collaborative, transparent, faster and more iterative. It requires leaning on automation to solve common problems, and to reduce costs and risks.

Security as Code represents the future of cloud security. •

Eric Johnson is the lead author and an instructor for SANS Course SEC540: Cloud Security and DevSecOps Automation, and is a co-author and instructor for SEC510: Public Cloud Security: AWS, Azure, and GCP.

For more information on all SANS Cloud courses, visit: https://www.sans.org/cloud_courses_AISA, email anz@sans.org or call 02 6174 4581.

SANS CLOUD SECURITY

SANS believes that the cloud is a transformative technology that will define the technology landscape for many years to come. Given the unmitigated growth of Cloud, we have launched the Cloud Security Curriculum to give you the training and skills you need to become a cloud security expert. Our curriculum provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and applications in the cloud against the most dangerous threats.

LONG COURSES

SEC488: Cloud Security Essentials

Learning the language of Cloud Security.

SEC510: Public Cloud Security: AWS, Azure, and GCP

Multiple clouds require multiple solutions.

SEC522: Defending Web Applications Security Essentials

Not a matter of “if” but “when”. Be prepared for a web app attack. we'll teach you how.

SEC540: Cloud Security & DevOps Automation

The cloud moves fast. Automate to keep up.

SEC557: Continuous Automation for Enterprise and Cloud Compliance

SEC588: Cloud Penetration Testing

Aim your arrows to the sky and penetrate the Cloud.

SEC584: Cloud Native Security: Defending Containers and Kubernetes

Deliver securely at the speed of cloud native.

MGT516: Managing Security Vulnerabilities: Enterprise and Cloud

Stop treating the symptoms. Cure the disease.

FOR509: Enterprise Cloud Forensics and Incident Response

SHORT COURSES

SEC534: Secure DevOps: A Practical Introduction

Principles! Practices! Tools! Oh My! Start your journey on the DevSecOps road here.

SEC541: Cloud Security Monitoring and Threat Hunting

Attackers Can Run But Not Hide. Our Radar Sees All Threats.

MGT520: Leading Cloud Security Design & Implementation

Building and leading a cloud security program.

NEW GIAC Cloud Security Certifications

Recently released GIAC Cloud Security Essentials (GCLD) affiliated with SEC488 and GIAC Public Cloud Security (GPCS) affiliated with SEC510



To find out more about Cloud Security Courses,
visit sans.org/cloud-courses-AISA





mimecast®

When it comes to Ransomware
A good defence is a good offence

Be ready with Mimecast

www.mimecast.com/anz/ransomware