Cyber Today

EDITION 1, 2022

THE CHANGING ROLE OF THE CIO AND CISO

THREAT MODELLING: A MISSING PIECE IN THE SECURE SOFTWARE PUZZLE

ZERO TRUST GENERATIONS

AISA

AUSCERT

SAFEGUARD YOUR INFORMATION

WITH AUSTRALIA'S PIONEER CYBER EMERGENCY RESPONSE TEAM

- 24/7 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

PUBLISHED BY :

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

ABN 30 007 224 204

PO Box 256, North Melbourne, VIC 3051
Tel: 03 9274 4200

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

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

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

EDITORIAL ASSISTANTS
Eden Cox, Kate Hutcheson

DESIGN
Abby Schmidt

PARTNER ORGANISATIONS
ALC Cyber Security Pty Ltd, **AUCloud**, AusCERT, **Edith Cowan University**, Netskope, **Rapid7 Australia Pty Ltd,** SANS

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

All stock images sourced from iStock.com

Vegetable based inks and recyclable materials are used where possible.

Proudly Printed In Australia

Contents

FOREWORD

INSIGHT

SPOTLIGHT

SECURITY

CULTURE

EDUCATION AND TRAINING

Foreword

A message from Dr Suelette Dreyfus, Board Director, AISA.

Dr Suelette Dreyfus

Cyber security often focuses on the technical – with good reason. Yet, bringing humans along for the journey to a more secure organisation is also vital. This is particularly the case as we roll in and out of pandemic waves, when we may work remotely more often.

We think we know how to ramp up working from home quickly. Certainly, we've now had enough practice; however, rapid pandemic waves can mean yet another mad scramble out of the building in a faster-than-expected time frame for staff. Working from home may also make staff more relaxed when it comes to cyber security.

International academic research shows that human factors continue to be a weak point in information security.[1] 'Security is not something that can simply be purchased,' says one author.[2]

The research literature points to two well-known 2020 incidents in which attack vectors exploited 'lack of readiness and human preparedness' in order 'to access confidential data or compromised systems'.[3] The first was the series of ransomware attacks on the Australia-based freight company Toll Group, which forced the organisation to suspend its IT systems.[4] This attack was of particular interest as it used non-stealthy ransomware (Mailto). Researchers suggest that 'improved personnel security awareness may have allowed [the company] to detect and prevent the attacks'.[5]

The second was a ransomware attack against health insurer Magellan. Using impersonation, phishing emails allowed the attackers to access the company's systems.[6]

Human cyber security training can take different forms. It may be about changing employees' mindsets at the coalface so they are not vulnerable to phishing or social engineering attacks. It may also be about investing time in deepening their understanding of why added steps are needed in their daily processes to ensure the integrity of systems. Organisations are increasing their focus on cyber security awareness training, which is a positive step forward. People learn in different ways, and tackling awareness from different angles simultaneously – including approaches such as cyber security 'nudges' and gamification – may help to address that.

Organisations often don't put the resources into deeply studying the workflows and processes of staff to ensure that cyber security interventions don't up-end daily work life unnecessarily. Employees need additional time to complete new hurdles – not just in the training phase, but even after that. Instead, this added load may simply be dumped on the employee after the training with the expectation that 'now you get it, just do it'. That's a recipe for failure in practice, and may also create resentment toward cyber security improvements that 'just waste my time and get in the way'.

Staff can be excellent early warning systems if you help them. When they see something that looks or sounds off, the key question is whether your organisation has trained them to speak up, or to just be quiet and look down at their desk. Do they know who to call or email if something 'doesn't smell right'? Is that interaction inviting and easy, or convoluted and time wasting? Are there some friendly public faces your staff feel comfortable reaching out to? Like the patient experience in a hospital, the cyber security experience of the staff member in an organisation deserves regular attention, evaluation and improvement.

The pandemic has had many surprising impacts, one of which seems to be a renewed interest in our fellow humans. Neighbourhoods have become more communal as people reach out to help those isolating, and workplaces have increasingly recognised the importance of the psychological – not just the physical – wellbeing of staff.

Hopefully, some of these changes will flow into strengthening the human factors in cyber security. ●

References

1 Hughes-Lartey, K., Li, M., Botchey, F.E., Qin, Z., 2021. 'Human factor, a critical weak point in the information security of an organization's Internet of Things.' *Heliyon*, Vol 7, Issue 3, e06522, ISSN 2405-8440. https://doi.org/10.1016/j.heliyon.2021.e06522

2 ibid

3 Chowdhury, N., Katsikas, S., Gkioulos, V., 2022. 'Modeling effective cybersecurity training frameworks: A delphi method-based study.' *Computers & Security*, Vol 113, 102551, ISSN 0167-4048. https://doi.org/10.1016/j.cose.2021.102551

4 Osborne, C., 2020. 'Logistics giant Toll Group hit by ransomware for the second time in three months.' ZDNet. 6 May. https://www.zdnet.com/article/transport-logistics-firm-toll-group-hit-by-ransomware-for-the-second-time-in-three-months/

5 Chowdhury, N. et al. Modeling effective cybersecurity training frameworks: A delphi method-based study

6 Davis, J, 2020. 'Magellan health data breach victim tally reaches 365K patients.' Health IT Security. https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients

Navigating the first hours after a breach

BY KEN MIZOTA, CHIEF TECHNOLOGY OFFICER APAC, RAPID7

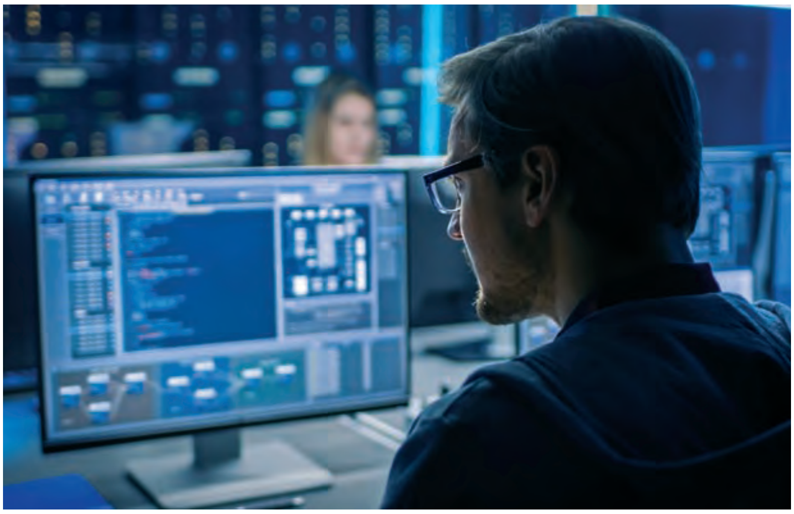
Cyber attacks and data breaches occur daily, but few organisations frequently manage significant incidents or breaches. The first hours after discovering a breach can be dynamic and challenging; and, if it's your first time, you may feel under pressure to act fast.

Understandably, organisations often immediately kick attackers off the network or disconnect compromised systems. Yet, that can alert the attacker and force them to evade your measures or escalate the attack. Depending on the attack, observing the attacker's behaviour first can help you better contain and remove the threat. These nuances demonstrate the value of experience and planning. Here, I share some other insights from years of assisting organisations in detecting, responding, remediating and protecting against cyber attacks.

Preparation counts

Concise playbooks help you to focus on taking action, and to be safe in knowing you developed the steps in a calm, measured way. Following a playbook can help reduce stress and pressure by giving you the confidence to make the right decisions.

Leading security teams conduct simulations and table-top exercises to familiarise their organisation's leaders with likely scenarios. Working with senior stakeholders to create a shared understanding of your cyber security strategy and incident management plans during times of peace enables you to fall back on solid relationships during an actual event.



Prioritise detection

Organisations tend to over-prioritise prevention and fall short on detection. You need to be confident you can detect breaches, and early detection helps you limit the damage and get systems back up faster. Rather than being the recipient of the bad news, seeing a potential breach yourself gives you more control and can make the first hours of a breach less fraught.

Gather the team you need

Incident detection and response is not just a technological matter, and you shouldn't underestimate the importance of people and processes. Sophisticated attacks continue to expose failings in prevention technologies and the lack of specialised skills within organisations. If you face such a scenario, you'll need assistance from outside experts, and they should be one of your first phone calls once you become aware of the breach.

Get emotion out of the way

Major incidents can be intense, and you'll likely experience many emotions. It's a stressful time, and it's only natural to start wondering what it means for your organisation or for you as an individual. The first hour of incident management should be about getting these emotions out of the way by following established and tested processes.

External partners can bring a detached perspective and specialised experience to help you make the right call in the heat of the moment. ●

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

The changing role of the CIO and CISO

BY NICKI DOBLE

There's a unique opportunity for the CIO and the CISO to shape modern business strategy and increase their influence across organisations.

Nicki Doble

The days of the chief information officer (CIO) and the chief information security officer (CISO) running their own race is, and will become, a thing of the past.

As a technology executive of 25 years, I understand that the CIO and CISO roles are different; however, as much as they are different, they are equally of value as strategic business enablers who have an opportunity to work more closely together to find innovative solutions to complex problems.

The concentrated focus on digitisation and digital transformation over the past eight or so years means that CIOs are somewhat ahead in being invited to the executive and board table for key business growth discussions.

With the growing awareness and risk of cyber security, however, boards and C-suite professionals are moving quickly to include the CISO at the top level. This increased awareness means they are also starting to move the conversation beyond risk, and are starting to understand the importance of digital trust.

This rising tide of awareness will soon establish digital trust as a strategic function, and CIOs and CISOs should view each other as allies, with their roles interwoven to guide the organisation to a new way of digital operations.

Consumers will choose brands they (digitally) trust

Brands that establish digital trust with their customers will become the preferred consumer choice, but this requires security by design across the entire C-suite and their functions. I believe that every C-suite leader should be expected to report to the CEO (or board) what they are doing, within their function, about cyber both to address risk and also how they are being innovative in using security to their commercial advantage. This provides the CISO and the CIO an opportunity to collaborate, educate and influence the strategy of the other C-suite executives.

With higher engagement across the C-suite, it also somewhat removes concern from the board to know if they are asking the right questions. Executive teams and boards solve complex global problems everyday, and although they may not possess the technical know-how, they have an active role to play – from the chief

marketing officer promoting security brand value, through to the chief financial officer's understanding of how much a successful attack could end up costing a company and translating that risk into financial language.

Security is not simply another technology function of a CIO's remit

While some organisations and industries will mandate that the CIO and CISO should remain separate, there will be those that have the CIO leading the security function. Where these responsibilities are merged under technology, it's in the best interest of the CIO to ensure that security is seen as a separate and specialised skill set. Keeping the distinction assists the organisation in understanding that business resilience requires a foundational transformation that needs to move across the entire business.

CIOs should also ensure that they aren't overly confident with their security knowledge, and anyone that feels they can own or lead a security function without experience and education is somewhat naive. I know firsthand that leading a response to a ransomware attack is very different to recovering a failed platform or recovering a large technology program.

It's encouraging to see that more and more CIOs, like myself, are investing in retraining or upskilling themselves to meet this ongoing and growing challenge.

Strong allies in a digital world

CIOs and CISOs are allies; they are the two roles that will enable and guide the other C-suite executives to lead on security, build it into operations and strategy, and create commercial value.

We have heard the adage that businesses should no longer be writing a digital strategy, but rather a business strategy about how to operate in a digital world. The inclusion of cyber security in that business design is vital, and not doing so would be failure. ●

About the author

***Nicki Doble** is the former Global CIO of Cover-More Group (a Zurich Company). She is an Executive Member of AISA Sydney Branch, and General Member of the Australian Institute of Company Directors. She is currently on a short study sabbatical while she focuses on her Master of Cyber Security, geeks out in her home lab, and preps for her CISPP exam.*

Understanding SSE and SASE

The secure access service edge (SASE) journey requires reliable partners with truly integrated platform capabilities, not vendors wielding smoke-and-mirrors-style marketing proclaiming 'SASE' in giant headlines. But clarity is critical, and both SASE and the more recently coined security service edge (SSE) terminology can be a little confusing. Let's examine what distinguishes SASE from SSE, and why both concepts are so fundamental to building cloud-centric security and networking architectures of the future.

SASE: a security and networking architecture

SASE is a framework for designing security and networking architecture in a world in which the use of cloud applications is now ubiquitous in business. The SASE framework includes both the technologies required, and the way those technologies are integrated and delivered, to not only match the flexibility and economics of cloud access, but to also align with the evolution of evaluation, procurement, and deployment practices.

These are necessary changes. In a cloud-first, work-from-anywhere world whose requirements have been accelerated by a global pandemic, security must become perimeterless and must be able to follow a company's most important asset – its data.

SSE: the security capabilities needed for SASE

A good way to view SSE is as a term describing the evolving security stack that sustains the SASE journey – more specifically, a set of capabilities necessary to achieving the security SASE describes, focusing on core platform requirements including cloud access security broker (CASB), secure web gateway (SWG), and zero trust network access (ZTNA).

A simple way to think about SSE, and the work being done by enterprise IT teams toward SSE, is as 'the security side' of SASE – managing access to and protecting an organisation's data. But even with such rapid adoption of SASE architecture, most businesses will not tackle SASE exactly the same way, with some focused on the core security capabilities described under SSE; others continuing to retire legacy networking investments in favor of more modern networking capabilities, such as SD-WAN; and still others working throughout the infrastructure to add ZTNA capabilities, and begin to phase out lagging technologies, such as VPNs.

SASE is the total blueprint; SSE is a subset of overall SASE requirements focused on several key security-related components of the blueprint that, when sourced from a single platform provider, offer previously unattainable efficiency of operation and economy of scale.

The threat and data protection efficacy of SSE within SASE requires detailed context that legacy defenses hosted in the cloud are unable to provide. SASE can support business-driven network and security transformations; but only with the right emphasis on context will SSE enable overall success with app and data transformation in relation to threat and data protection. •

Pentesting – the art of cyber dark magic

BY CRAIG FORD

It's a cold winter's morning, and you've been up all night testing your skills on one of those ethical hacking gamification platforms.

Craig Ford

You're smashing through the runs and kicking goals, all while pumped up on the latest buzz energy drink and sugar lollies. Then it comes to you: 'Hey, I'm a hacker; a wizard of these mystical dark arts; a master of all the things that are only whispered about in the dark corners of the deep web, where all the criminals and ruffians hang out. I'm going to be a pentester. I will pick target clients and throw everything I have at their defences, and then I will sell them the secrets I have unearthed, tell them the holes I found in the systems – all at an exorbitant fee, of course, so I can fund my gaming and energy drink addiction. I don't need to answer to anyone. I will be my own boss.'

So, you get to work. You start scanning the internet to see who will be your first client. You find one with open ports to the internet, and you throw your cyber version of Thor's hammer or Harry Potter's deadliest spell, 'Avada Kedavra' (the one that emits a flash of green light, instantly killing its target). You smash your way through the defences, bringing down the target's systems.

Job well done.

Now you go ahead and send an email to the main contact address on the company's website, informing them of your masterful work, how you single-handedly took down their systems and will inform them of how you did it once they agree to cover your fee. You smile to yourself, happy with your work. It's 4 am now; time to head off to bed. A job well done, indeed – you have done your first pentest, and you will be rolling in it if this progress keeps up.

You take yourself off to bed and fall asleep.

BANG BANG BANG. 'This is the police! Open up.' *BANG BANG BANG.*

What's going on? What is all this commotion about? You head to the front door and open it. It's the police, who then hand you a warrant for your arrest. You have been charged with illegally hacking the company from last night, and taking down their systems. Oh, that's right; you didn't have their permission to do the testing, and you didn't follow any real rules of engagement, causing them massive financial losses from their platforms going down.

You messed up big time, and will likely be spending a fair bit of time in prison overalls in the future.

That escalated quickly, didn't it? Yeah, I know – it's a bit dramatic, and I have slapped a wide and thick layer of creative licence on here. But you get what I am trying to sell here, don't you? The lessons I'm trying to teach you?

There is a lot more to pentesting and ethical hacking than just smashing a cyber hammer at things, trying to find ways into systems.

First, you need to have permission from the client to conduct the engagement, and a thick stack of legal documentation that indemnifies you from any repercussions from attacking the target company's systems that are in the scope of your agreement.

There is a lot more to pentesting and ethical hacking than just smashing a cyber hammer at things, trying to find ways into systems

That is seriously the most important rule. Make sure both you and the clients have a thorough understanding of what you will be doing, and what is in your scope – basically, what you are allowed to do and what you are not. If you don't do this right, you may still have those lovely police officers knocking on your door to give you some new chrome bracelets to wear for a while.

Second, you need to document and record everything you do in the engagement. This is a thorough and necessary record of what you did, when and why. It will help you to create an accurate report for the client and records for you to help fix anything if you do make a mistake and cause a system to go down.

Never do an engagement without keeping accurate records.

The last point I need to make sure you understand and stick to is: never do something that will cause major outages for your client. Don't just go and exploit vulnerabilities, especially ones that are known to be damaging. That will not only see you in court being sued for damages or losses, but it will also very quickly give you a very bad reputation – one that will dry up your work right across the globe. Security is a growing space but is still a reasonably small community, and word spreads quickly.

So, maybe instead of jumping in and doing your thing while on a sugar high, think this all out properly, get some help doing it right, and make sure those legal documents are tight – you don't want a poorly drafted scope/engagement document to get you in hot water.

Do it right. Trust me, you'll thank me for it later. ●

About the author

Craig Ford is the QLD Branch Chair for AISA. Ford is a cyber security professional with experience working in ethical hacking, incident response, security consulting, and more. Ford was named in the global 40 Under 40 in Cyber Security 2022, and he was the AISA Cyber Security Professional of the Year 2020 and AWSN Women in Security Awards – Male Champion of Change 2021 Special Recognition Award recipient. He is the security services manager with Baidam Solutions. Ford is a regular columnist for the Women in Security *magazine, and author of the* A Hacker, I Am *cyber awareness book series (2019–2021) and* Foresight *hacker fantasy novel series launching in June 2022.*

PARTNER CONTENT

Sovereign data protection and control

BY PHIL DAWSON, MANAGING DIRECTOR, AUCLOUD

The very reasonable expectation of citizens in our digital age.

The shift to cloud provides enormous flexibility, agility, and efficiencies in data management and delivery of services.

The last decade is testament to the scale and reach of cloud services. The trend has been worldwide, led mostly by global cloud providers. As more data finds its way to the cloud – with more of it being confidential data about citizens – sensitivity about where that data is stored, moved and who can access it is driving a pivot in that trend.

The ability to protect data breaks down as it is moved, managed, stored, analysed and used across the global digital supply chain. The concern is twofold.

The first being an antagonistic cyber landscape that makes it increasingly difficult to assure protection of data against evolving and more sophisticated security threats. Threats to the confidentiality, integrity and availability of data are real. From energy and logistics companies, to universities and health services, the pain of data breach and/or operational disruption has been acute.

The second concern is jurisdictional control – more specifically, concern about losing it. That data can be moved offshore, or even remain onshore but open to overreach by authorities with jurisdictional control over non-sovereign-owned cloud providers, raises much more serious concerns.

Research this year by IDC throws weight behind previously anecdotal concerns about where cloud data 'goes', how and where it is moved, how it is stored, and who can access it.

Involving decision-makers from the public sector, financial services and healthcare industries globally, the research shows that some 63 per cent of respondents believe it is very/extremely important to have cloud solutions that provide complete jurisdictional control and authority over data.

As the pendulum of globalisation swings back to localised control of citizen data, sovereign data protection is not just about residence. It is fundamentally about ensuring that data is subject only to the jurisdictional control and authority of the nation where the data is collected, with certainty that other jurisdictions cannot assert similar rights. This mitigates the risk and complexity of data being subject to multiple and overlapping legal standards and, importantly, assures sovereign data protection.

In signing up to the cloud infrastructure of global providers, many Australian organisations are unaware of the contractual detail they agreed to. Few have little, if any, transparency of what data (customer data, metadata, support, analytics, etc.) is moved where or the level of extra-jurisdictional access to it.

As well as assurance that your data will never leave Australia and that systems will be operated, managed and supported by security personnel in Australia, sovereignty of cloud services means as implied – they are only ever subject to Australian legislation and judicial process.

Once upon a time, the insistence of (data) localisation and control raised the hackles of protectionism; however, without the ability to ring fence and protect citizen data, managing risk and growing trust in a national digital infrastructure and building much-needed sovereign resilience is fundamentally undermined. ●

To read the IDC report, 'Deploying the Right Data to the Right Cloud in Regulated Industries', visit www.vmware.com/content/dam/learn/en/amer/fy22/pdf/987789_AMER_22Q2_IDC_Sovereign_Cloud_WP.pdf

AUCLOUD AUSTRALIA'S SOVEREIGN CLOUD

AUCloud Sovereign Data Protection

For Australian Government, Defence, Defence Industry, Critical National Industry organisations & security conscious enterprises

How secure is your data?

- Do you know where it goes?
- Are you confident your data is in Australia - that it stays in Australia?
- Do you know who can access it?

AUCLOUD: Australian owned and operated by security cleared Australian citizens. Your data stays in Australia – ALWAYS - subject only to Australian legislation and jurisdictional authority.

CONTACT | 1800-282-5683 | sales@australiacloud.com.au

Services available across AUCloud's PROTECTED and OFFICIAL environments

- Compute as a Service
- Storage as a Service
- Disaster Recovery as a Service
- Backup as a Service
- Desktop as a Service
- M365 Backup as a Service
- SOC as a Service
- WorkspaceONE

ISO 27001 INFO SEC Certified System

vmware SOVEREIGN CLOUD

vmware CLOUD VERIFIED

Data security is our DNA

australiacloud.com.au →

SPOTLIGHT

Cybernetics and cyber security

BY DR MICHAEL DONEVSKI, FOUNDER, OMALIS

Many might associate the field of cybernetics with robotics, cyborgs, cybernetic body enhancements, cybernetic tattoos, microchip implants, or brain-computer interface; however, it's much, much more than that.[1]

Cybernetics is a multidisciplinary science that, over the past 70 years, has cross-pollinated across many diverse fields. It therefore means different things to different people, but, in general, cybernetics is a study about systems.[2] The term 'cybernetics' was coined by Norbert Wiener in 1948 to refer to control and communication in the animal and the machine, and to describe a self-regulating machine that uses feedback loops.[3]

The importance of cybernetics to cyber security, and vice versa, is evident in the definition given by Wiener, where his emphasis on 'control' anchors both domains and provides the link to their symbiotic relationship. The intrinsic role of cyber security is to provide sustainable assurance of this control and integrity of any software-driven technology that manages this control today and in the future.

Complete control of an individual system in diverse and hyper-connected environments appears to be unattainable; thus the original meaning of 'cyber' – to steer or govern – is more suitable as described by Wiener, where the sharing of networks, systems, software and data is necessary for any cyber activity today.

Cybernetic anthropology

One might think, for example, that they have complete control of their smartphone, and in a physical sense, this is true. This is not the case, however, regarding control of the software and data on that system, which is dynamic and evolves over time.

To identify cybernetic dependencies, we study how a system behaves in its environment, and look at the necessary relationships that the system must have in order for it to retain its core purpose or function. In the example above, there are many parties that share this control, such as hardware and firmware manufacturers, operating system providers, app developers, software supply chains, telecommunication companies, and data brokers. The percentage of data control each has is debatable. But over the years, one thing is certain: end users' control has slowly corroded. Control of a smartphone as a physical entity is no longer relevant, and the digital divide is no longer about who has access to technology and who does not, but rather who is generating the data, and who is truly benefiting from that data.

Software patching – one of the most important cyber security mitigations for a smartphone – relies heavily on digital supply chains, over which the end user has very limited control. The cyber security industry is working hard to find solutions to assure the integrity of these supply chains; however, we tend to forget that these supply chains are also bi-directional. End users receive software patches, and software companies receive a supply of genuine social feedback or behavioural data from their human sensors. While the cyber security industry protects us from cybercriminals, it has no solutions as to how to protect people from software companies that use persuasive technologies unethically to manipulate end user behaviour for company gains. Cybernetic anthropology could help to identify social threats of technologies that control human behaviour, and to build better cyber security controls to protect systems and people in the future.

Cybernetic art

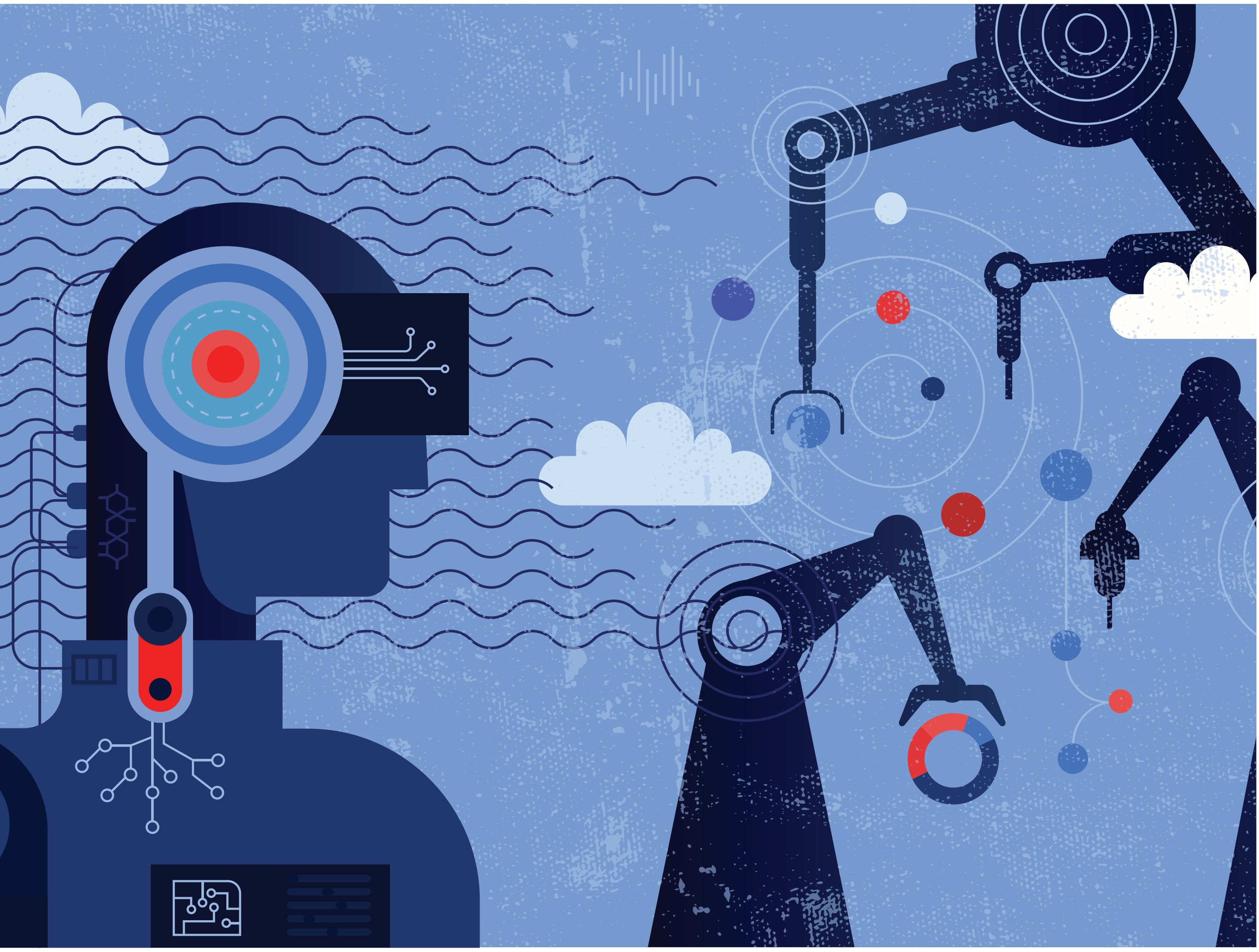
All exponential technologies fall under the umbrella of cybernetics, but artificial intelligence (AI) appears to have gained the most momentum, including its influence in creation of new cyber security solutions. But what is the role of cyber security in the AI community?

An artist will most likely not think about cyber security when creating a digital artwork with AI, and will possibly fail to protect their data and models. An attacker can potentially manipulate these data and models, and change the final artwork or intellectual property. Why would someone do that? This is possibly the most asked and irrelevant question that cyber security researchers face when trying to explain a costly security problem that may be trivial to exploit.

What if the digital AI artwork was not the work of a creative AI artist, but rather the work of a cybernetic anarchist that wants to flood the market with abstract and industrial art incognito? Could proof of tampering change the value of that artwork in the future?[4]

Cyber security inside any AI system is responsible for the control of that system, and to preserve the integrity of data, software, hardware, behavioural

Dr Michael Donevski



interactions that the system has with its environment, and for the intellectual property. Time and time again, security researchers use complex adversarial machine learning techniques and trivial hacks to deceive production AI systems that use traditional or no security controls at all.

An AI system with no cyber integrity is just an A

The biggest cyber security problem is not ransomware, supply chain attacks or zero-day attacks, but rather the lack of diversity – not just in people, but also in technology, creativity and new ideas. Cybernetics is the bridge to the diverse fields – such as anthropology, art, AI, and many more like biology, medicine, chemistry and engineering – that cyber security desperately needs for diversification and provision of holistic solutions that work. •

About the author

__Dr Michael Donevski__ is the Founder of Omalis, a cybernetic research organisation that specialises in providing cyber security solutions. Donevski's current focus is on the application of cybernetics to cyber anomaly management. He has over 25 years of experience in IT and cyber security in both the public and private sectors. He has held security roles in the Commonwealth Government, Department of Defence, and Lockheed Martin, Australia.

References

1 https://uk.pcmag.com/news/136666/cybernetic-body-enhancements-are-a-ok-with-most-of-us

2 ANU School of Cybernetics, https://3ainstitute.org/about

3 Wiener N. (1948), *Cybernetics: Or Control and Communication in the Animal and the Machine.* Paris, (Hermann & Cie) & Camb. Mass. (MIT Press)

4 https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital- artwork-NFT-to-come-to-auction-11510-7.aspx

Shadow IT a 'ticking time bomb' for corporates in the new reality

BY PAULA JANUSZKIEWICZ, FOUNDER AND CEO, CQURE

The remote model of work without proper security training is a headache for cyber security teams.

Paula Januszkiewicz

A fundamental part of a tool's identity is its functionality. A hammer and a quantum computer share a fate; their role is to support a person in the implementation of specific tasks. Because of that, network security often loses in favour of functionality.

The phenomenon known as 'shadow IT', where employees use hardware and software not approved by the employer or IT security department, is not a new phenomenon; but in the new reality defined by COVID-19, it has become a serious threat to many organisations.

It turns out that for many companies, the priority is to maintain work continuity at the expense of security. According to 76 per cent of IT teams participating in the Hewlett Packard (HP) report, 'HP Wolf Security Rebellions & Rejections', security in their organisation lost its priority to business continuity, and 91 per cent said they felt pressure to relax security policy.

The increasingly common model of remote work causes the blurring of the boundary between private and professional life. Working hours are more and more difficult to put into clearly defined frames. These changes also affect the office equipment used for work at home. Maintaining the continuity of work imposes the use of employees' private resources because employers most often provide the necessary equipment to perform the entrusted tasks to a limited extent. A company computer connects to the network via a home router, and a private printer is activated much more often in a dusty corner.

According to the aforementioned report, as many as 45 per cent of office workers bought IT equipment (e.g., printers and laptops) in the past year. Of these, 68 per cent stated that security was not an important factor in their purchasing decision. Moreover, 43 per cent declared that laptops and desktops have not been checked by the company IT department, and 50 per cent of respondents said the same about their new printers. The problem is not only new devices, but also those connected to the home network for many years. Most often, their software is either not updated or the hardware manufacturer no longer provides technical support, which makes devices vulnerable to the latest threats. Altogether, this makes them an easy target for criminals looking for weaknesses in the company's security architecture.

Hardware is not the only problem for IT departments, which, according to another study by HP ('HP Wolf Security Out of Sight & Out of Mind'), were much more loaded with work during a pandemic year (83 per cent of IT teams expressed such an opinion). It translates into the cost of IT support related to security, which, according to the respondents, increased by 52 per cent in the past 12 months. A huge challenge is the installation of software on company equipment by employees without the consent or even notification of the IT department. This action threatens the security of the company to a large extent because it makes it much easier for malicious software to penetrate the internal resources of the company.

Knowledge of cyber hygiene, discussed lately in a larger extent in public debate, is becoming more and more common. Unfortunately, the awareness of creating

appropriately strong passwords, the use of multi-factor authentication and limited trust, turns out to be insufficient when we move the work environment to home. The functionality that enables the fulfilment of work duties wins the battle with security. COVID-19 was a classic 'black swan' event; and at the beginning of pandemic chaos, companies didn't have time to properly train their employees in this regard.

According to 'HP Wolf Security Out of Sight & Out of Mind', almost half of younger office workers (18–24 years old) viewed security tools as a hindrance, leading to nearly a third trying to bypass corporate security policies to get their work done. Forty-eight per cent of office workers surveyed agreed that seemingly essential security measures lead to a lot of wasted time. As a result, 83 per cent of IT teams believe the increase in home workers has created a 'ticking time bomb' for a corporate network breach. Maybe we should take a step back and train workers properly before we send them to work at home? ●

About the author
Paula Januszkiewicz *is the CEO and Founder of CQURE Inc. and CQURE Academy. She is also Cloud and Datacenter Management MVP, Honourable Microsoft Regional Director for CEE, and a world-class cyber security expert, consulting customers all around the world. Januszkiewicz has 15 years of experience in the cyber security field, performing penetration tests, architecture consulting, trainings and seminars. She has performed hundreds of security projects, including those for governmental organisations and big enterprises, and has been a top speaker and a keynote speaker at many well-known conferences.*

AusCERT in 2022

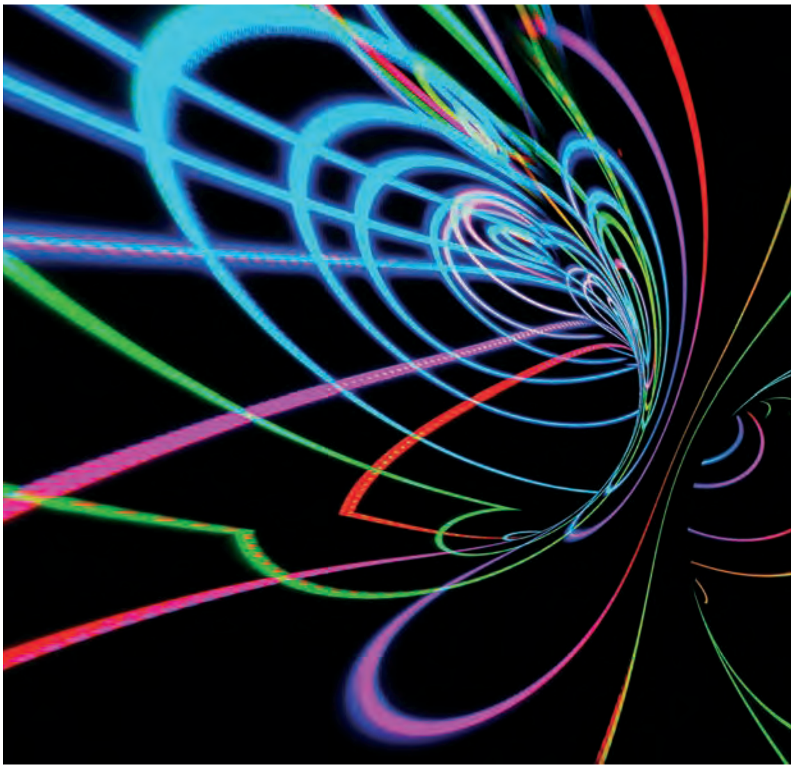
A goal of long-term and mutually beneficial partnerships.

The previous two years have presented challenges, with a degree of uncertainty still lingering for 2022; however, at AusCERT, we are buoyed by an industry that has an abundance of skilled and motivated individuals and organisations. We engage with an array of industries and people eager to enhance and broaden their cyber security knowledge, skills, and strategy.

It is our role to assist our members on this journey. A key goal at AusCERT is to help our members in a 'life cycle', not just in one-off incidents or pieces of work. For example, we provide members with pertinent information (Malicious URL Feed, MSINs, SIAs, DFNs and Security Bulletins) that is valuable. To complement this, AusCERT also provides several training courses for organisations still nearing the maturation stage of their cyber security capabilities.

Our focus is on ensuring that members have the right tools for the situation and environment, allowing each to effectively manage incidents.

Education is ongoing, with our team constantly reviewing and updating content as needed, and adding new courses when we identify a need for our members.



Of course, AusCERT is on hand to provide incident management, but as service provider numbers grow, it becomes increasingly difficult to wade through them all and gauge how one differs from the next.

A long-term goal at AusCERT has been to coexist within the current ecosystem of vendors, consultants, and suppliers to learn from and help each other.

As one of Australia's only cyber emergency response teams (CERT), and one of the oldest CERTs in the world, our longevity has resulted in an extensive body of cyber security research that is shared with members and other CERTs globally.

A key AusCERT forum for collaboration and knowledge sharing is our annual conference. This year's theme ties in with our ethos of continual growth and learning: Rethink, Reskill, Reboot. It is, as always, an optimum opportunity for professional development and upskilling.

The range of services we provide has developed from our understanding and awareness of what the industry, and our members, need. Under AusCERT membership, we offer constant access to a trained team of analysts (most have one or more SANS courses and other qualifications).

So, whenever members need a piece of suspected malware analysed, that is covered under membership. Need quick advice or a second opinion on something? That is also covered. ●

The AusCERT Membership team can provide more information on services and training courses for current members, and the wider information security community.

Email membership@auscert.org.au for further information on our services and upcoming training courses.

The cyber security landscape is ever changing, and AusCERT continues to be passionate about engaging our members to empower your people, capabilities and capacities.

Threat modelling: A missing piece in the secure software puzzle

BY DR BAZARA BARRY, PRINCIPAL CYBER SECURITY ADVISOR, CYBER SECURITY NSW

According to the latest report from the HackerOne security platform, there was a 20 per cent increase in software vulnerabilities in 2021 compared to the previous year.

The computer software industry remains the most profitable for bounty hunters who look for weaknesses in software systems, with at least a 25 per cent higher average bounty payout compared to other industries. Sadly, there is no sign to indicate that the latest scramble to fix the Log4Shell vulnerability will be the last one the cyber security community will have to go through.

Although there is a growing level of awareness among software developers to include security features in their final product, that is still a far cry from having a secure product. A secure software product is one that ingrains security in core product features, defines clear security goals, and establishes a process to minimise security risks to an acceptable level. Software development teams have to come to an understanding that product security as an afterthought comes at the expense of users, software quality, and the software development teams themselves.

This article highlights threat modelling as an important tool in the secure application design/development processes, and provides high-level guidance on how it can be practically applied.

The art and science of threat modelling

Some may consider threat modelling an art, while others believe it is a science.

Regardless of which school of thought you follow, what should be agreed is that threat modelling provides a structured approach to understand and deal with threats to the software application with the goal of reducing the overall risk. With the systematic process it proposes, threat modelling assists greatly with critical thinking during the software design phase.

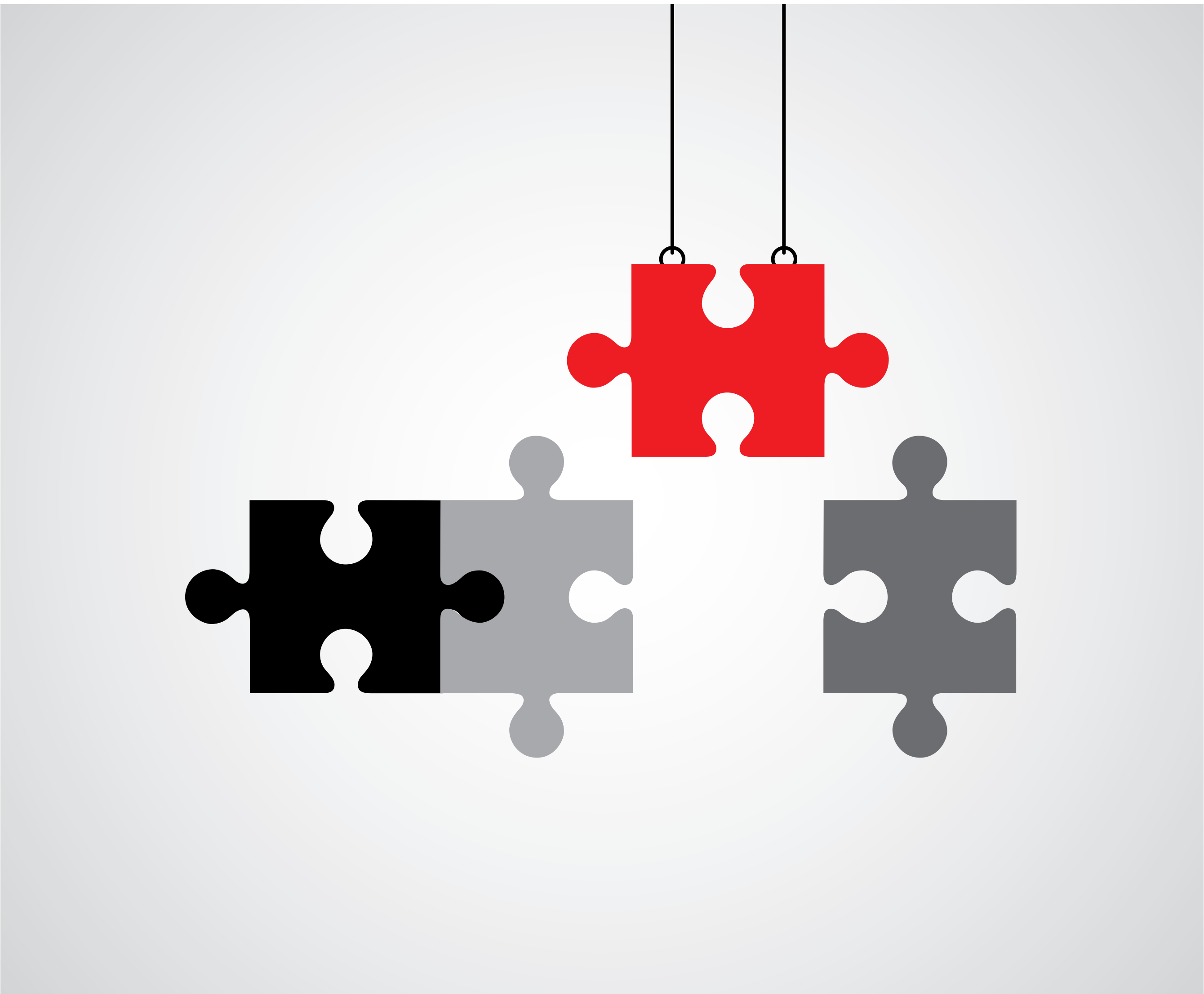
Different threat modelling frameworks propose different processes with varying steps. However, the high-level steps that may be common between the different frameworks are:

- Identify the constituent parts of software/application and data flows
- Identify threats to the system/data
- Rank the threats according to their impact
- Determine techniques/technologies to mitigate threats.

A STRIDE in the right direction

STRIDE stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Escalation of privilege. These are six main threat categories that violate desirable secure states of a system. This model suggests these categories to help system designers identify threats and propose mitigation techniques/technologies in an organised manner.

A simple way to apply the STRIDE model starts with a model of the system/application



to be protected. For each of the constituent parts of the application, the team brainstorms potential threats to that part and records them based on the six categories. Brainstorming may include information about target, likelihood, impact, attack vectors and mitigation status.

Next, the team ranks threats and decides on how to respond by suggesting high-level techniques (e.g., authentication) and technologies (e.g., Security Assertion Markup Language). Any issues that might stem from technology implementation are recorded and dealt with during early design phases. A rule of thumb is to include wider team members in brainstorming sessions, such as system architects, product managers and business analysts.

Although threat modelling and the STRIDE model seem like common sense, it does not mean they are common practice. Whether the team uses sophisticated tools or simple spreadsheets, it is crucial to embed threat modelling in the software design phase and follow a proactive approach to threat management. Moreover, collaboration with wider software product teams during threat modelling ensures instilling the right security culture and a more secure final product. ●

The views, thoughts and opinions expressed in this article belong solely to the author, and not necessarily to the author's employer, organisation, committee or other group or individual.

About the author
***Dr Bazara Barry** is Principal Cyber Security Advisor at Cyber Security NSW, which is the whole of NSW Government cyber security function. He brings a decade of leadership experience in cyber security operations and strategic management, security policy architecture, governance frameworks, and risk assurance.*

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

Achievements
JEFF

The future of passwords is… no passwords at all

BY DAVID BRAUE

Anything is better than relying on users to think up and remember their own passwords.

For all their weaknesses, passwords have remained at the frontline of user authentication for many decades, creating an easy vector for cybercriminals that wasted no time leveraging the 'keys to the kingdom' to breach perimeter defences.

So many systems have been breached that sourcing working credentials is still child's play: a recent Digital Shadows review found more than 15 billion credentials – sourced from over 100,000 data breaches – circulating on dark web hacker forums and available for cybercriminals to share, purchase, trade and use.

The sheer volume of such breaches has highlighted the inherent insecurity of passwords, and helped the use case for passwordless authentication virtually write itself over the years, as users' intransigence around password hygiene kept desperate chief information security officers (CISOs) and industry figures scrambling to keep up.

According to a 2020 Kaspersky survey, 83 per cent of users reported that they think up their own passwords, and 55 per cent reported that they generally remember their passwords.

That might seem like a respectable result, except for the fact that few users would be able to remember large numbers of passwords that satisfy cyber security complexity requirements. That implies that many users are choosing easy-to-remember passwords whose simplicity violates every precept of good cyber security.

Other users weren't even working that hard, with 31 per cent saying they write their passwords in a notebook, 19 per cent storing them in a file on the computer, and 15 per cent writing their passwords on a piece of paper near the computer.

No wonder credential stuffing has become a thorn in the side for CISOs, who have kept busy fighting against credential-stuffing attacks – of which, the 'Verizon Data Breach Investigations Report 2020' observed, companies reported a median of 922,331 attempts in 2019 alone.

'Granted, a good number of those login/password combos attempted will be as complex as "admin/admin" or "root/hunter2",' the report notes, 'but those sustained attacks over time are succeeding according to our incident dataset.'

Will users accept the alternative?

A raft of early alternatives has coalesced around the FIDO Alliance's FIDO2 standard for passwordless authentication, which combines the W3C Web Authentication specification (WebAuthn API) with the Client to Authentication Protocol (CTAP).

Significantly, FIDO2 can work either in a two-factor authentication environment in conjunction with passwords and an external authenticator (such as phone, hardware USB key or smart watch), or in a one-factor authentication scenario where one of the authenticators is used as a complete replacement for passwords.

In the latter scenario, FIDO2 leans on CTAP to connect the browser with on-device authentication – for example, hardware security central processing units, fingerprint scanners or face recognition. This is integrated with the Platform Authentication API and browser's WebAuthn API, which conveys the FIDO2 authentication information to the host server.

The FIDO Alliance's broad membership has given the FIDO2 standard rapid ubiquity, with support across major web browsers and additional applications coming to the party, as well. But will users, who have been used to using passwords as long as they have been using computers, buy it?

A recent study of 94 users by researchers at Germany's CISPA Helmholtz Center for Information Security explored just this question, and found that users perceived the FIDO2 passwordless authentication as being 'more usable than traditional password-based authentication'.

'Lay users are very satisfied when directly replacing text-based passwords with a security key,' the study's authors note – including using hardware authentication devices like the Yubico security key as a single form of authentication.

That outcome 'is an encouraging result on the road to replace passwords, and indicates that FIDO2 has the potential to be the Kingslayer of text-based passwords,' the authors write on the back of findings that found the Yubico device was more accepted than traditional password-based authentication.

When asked what they disliked about conventional password usage, participants reported that they found it 'a difficult and demanding task' to have to create and remember secure, unique passwords – particularly given the growing number of accounts for which they have to remember credentials.

'The reduction of cognitive effort compared to password-based authentication was seen as a great advantage of passwordless technology,' the report notes.

A number of other participants found it 'problematic and annoying' to have to carry a physical device for authentication – restricting 'spontaneous and ad hoc use' – while others were concerned that their account would be 'completely unprotected' if they lost control of their access device or there were any hitches in delivery of passwordless authentication codes.

The study also identified concerns that passwordless authentication could be 'very problematic' if it cannot cover every current use case – for example, being able to spontaneously delegate access by sharing a password over the phone, or accessing systems from a public terminal that doesn't offer an accessible USB interface.

Ultimately, users were largely willing to use passwordless authentication – with 35 per cent saying they would use the system as is, and another 28 per cent saying their decision would be contingent on reassurance around issues such as potentially losing access to their account, access by others, universal access and general mistrust.

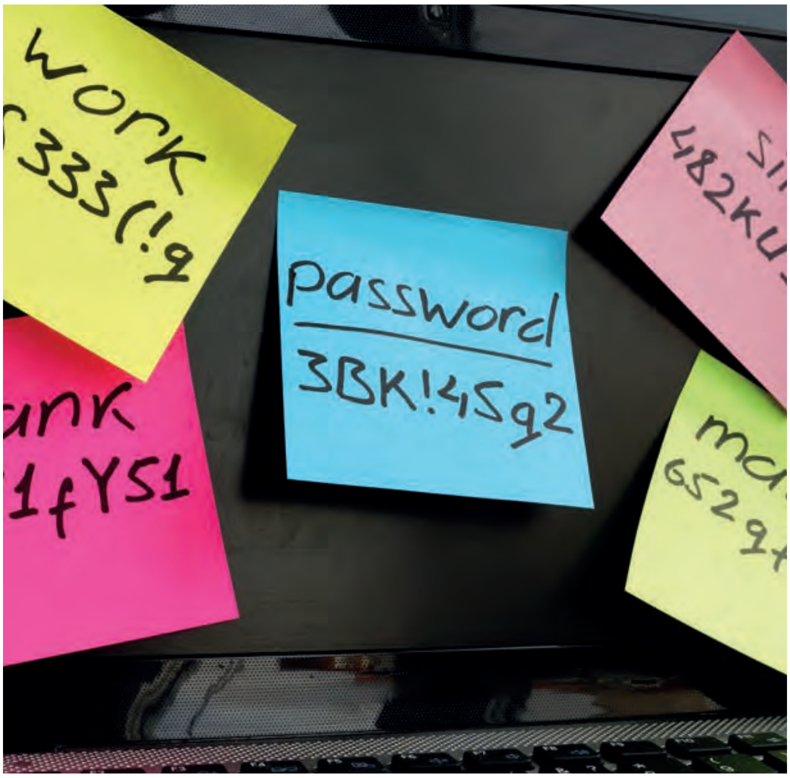
Conversely, 13 per cent said that they simply were not willing to use passwordless authentication, citing a range of factors, including the annoyance of carrying an extra device, fear of losing access to their account, lack of knowledge about the system and fear of account access by others.

Targeting your war on passwords

In a COVID-19-driven climate where remote access has become the norm, reducing corporate exposure to compromise through password theft has become a critical priority for security executives.

In this context, the promise of workable passwordless authentication – which refocuses access-control security around credentials that users don't know, don't have to remember and can't inadvertently compromise – is a breath of fresh air.

Yet, as the research suggested, many users have concerns about security and usability that must be addressed through targeted education before use becomes more widespread.

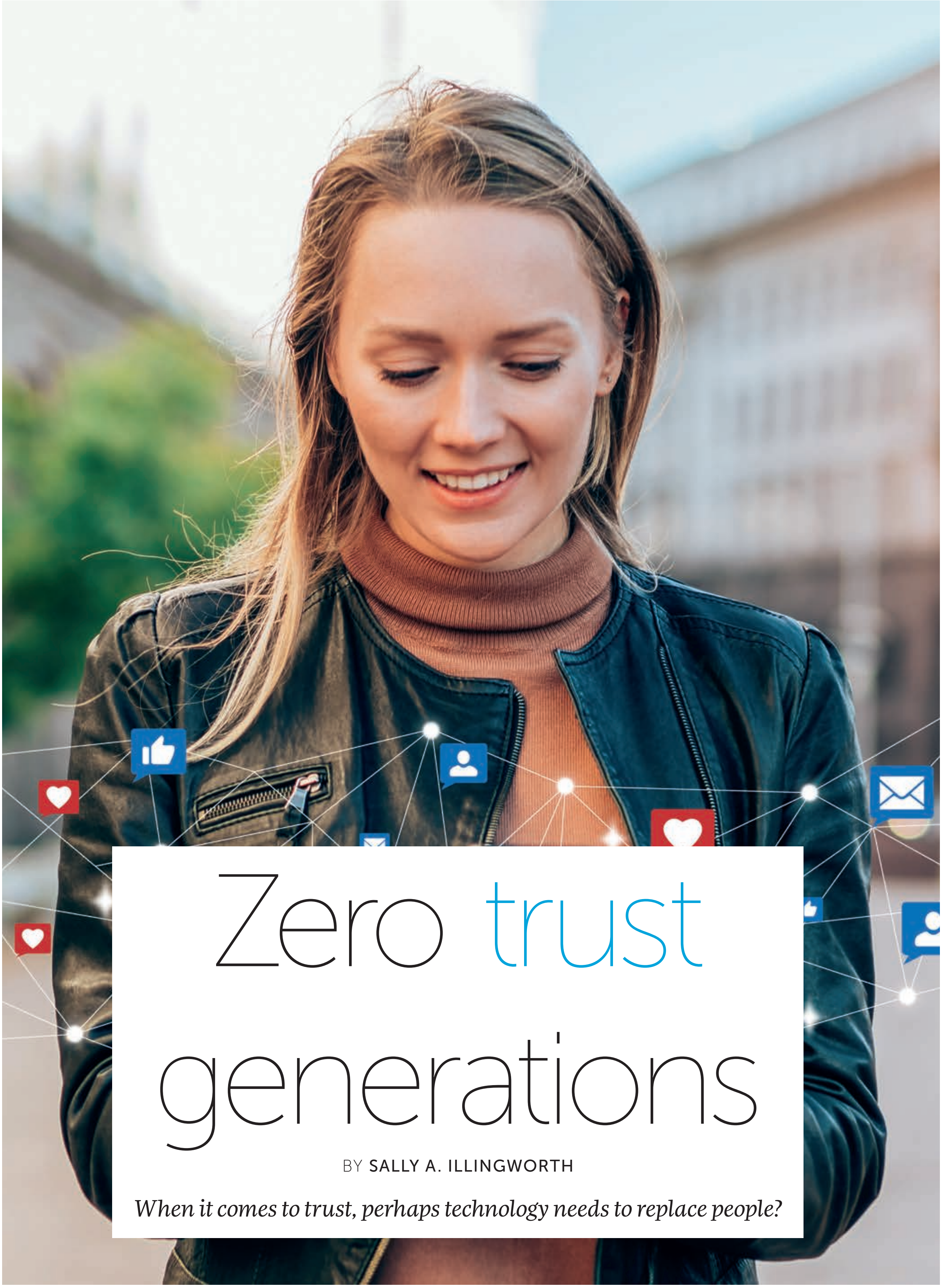


Fast-evolving endpoint devices will intrinsically address some of these issues, both by providing mechanisms – such as fingerprint and face scanning – and familiarising users with their everyday use.

Gartner, for one, has predicted that 60 per cent of enterprises and 90 per cent of mid-sized businesses will move to passwordless authentication by 2022 – a very short time line that highlights both the maturity of the technology, and its rapidly growing appeal to address the challenges of the new operating environment.

'The reliance on, and use, of passwords as the principal means of authentication... disrupts the customer experience, which is becoming one of the most important brand differentiators,' FIDO Alliance Executive Director Andrew Shikiar wrote in the preface of the World Economic Forum report 'Passwordless Authentication: The next breakthrough in secure digital transformation', also noting that passwords are 'paradoxically... very difficult to secure'.

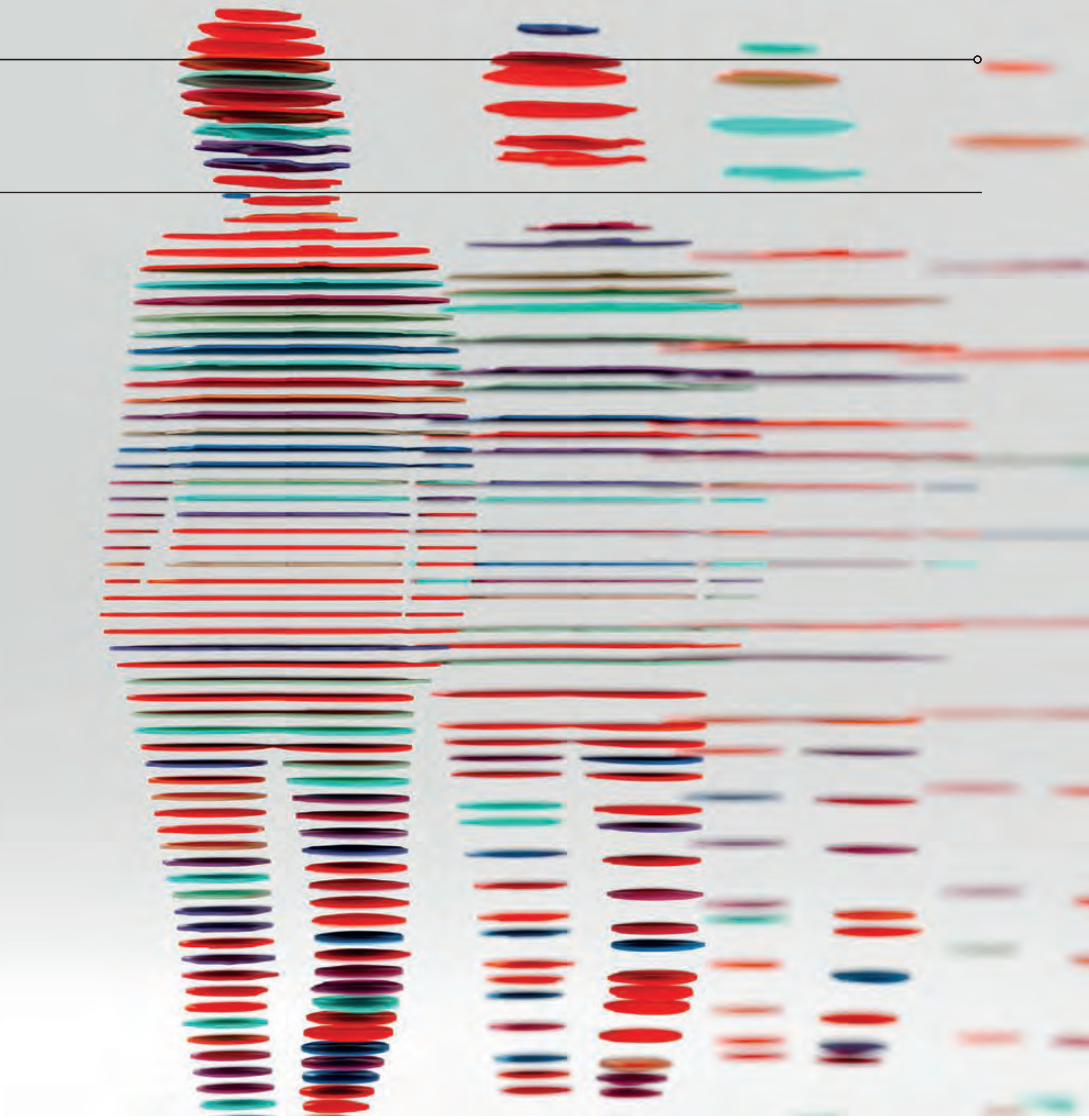
'Authentication is so much broader than passwords,' wrote Shikiar. 'It is the foundation of digital trust, an enabler of cyber security in the digital economy and... a critical enabler of the future.' •



Zero trust generations

BY SALLY A. ILLINGWORTH

When it comes to trust, perhaps technology needs to replace people?



Sally A. Illingworth

As the tangibility of our routine livelihoods evaporates and we increasingly become connected to each interaction across the globe through a swipe and a tap between our hand and a screen, we remain uncertain as to why we feel our most vulnerable when media discussions suggest it's devices and applications that are vulnerable.

While the technologies and digital ecosystems we've befriended are vulnerable in their own right, once upon a time their vulnerabilities were far from ours as the relationship between us required pattern-interrupted effort and a proportionately greater disposable income to expose ourselves to their vulnerabilities.

Our unprecedented vulnerability across digital ecosystems has necessitated a dramatic global shift in how we harness cyber security to protect our information and interactions without geographical constraint.

Many security concepts emerging in popularity, including zero trust architectures (ZTAs), make trust a redundant factor in influencing the flow of information, and the granting of permission to interact across technologies and digital ecosystems. For example, ZTAs by design assume that trust is a native vulnerability; hence, the presence or absence of trust is irrelevant.

Interestingly, trust conceivably remains a part of the governance framework for ZTAs – the benchmark for trust is simply no longer based on goodwill associated solely with a personally identifiable data point – such as an email address – but instead on a series of authentication, authorisation and validation steps on a per-activity basis for every occasion.

Upon reflection, it becomes obvious as to how we got here.

I remember walking from the kitchen to the study and waiting patiently for the Windows OS to boot up on the computer that was, in hindsight, of subjectively poor aesthetic design. Navigating to the start menu to command MSN Messenger and its simple

interface, yet captivating computerised character, I would exchange chat messages that I now know weren't as instant as possible.

Each time I flipped the top half of my phone up, I would feel capable pressing the same buttons two or three times to type with grammatical correctness without the support of spell check, and a sense of endless possibilities would filter through me.

My trust still belonged to me and the friends I chose to give it to conditionally. I could still see my circle of influence standing in front of me routinely as I went about my day. My temptations to trust the spectrum to interact with someone else who also trusted the spectrum were limited, because it was 10 cents each time I flipped the top half of my phone up and gave in.

MSN then found a friend who shared status updates with me, and let me publish photo albums to share with others who also found MSN's friend.

As I reflect on meeting MSN and its friend, Facebook, I remember it feeling so easy to trust them, even though they might not have trusted each other. Perhaps it was because I didn't have to carry the photo albums or because I didn't have to say out loud what I was thinking. They made it so easy for me to do things, so I never doubted them, and I still don't absolutely know who they are or what they have of mine.

If a stranger at the supermarket had offered to pass on a message for me to someone I know, I would've felt uncomfortable. If a stranger had offered to take my photo albums and share them with people I know, I would've reported the stranger to the police.

But I didn't because these strangers (MSN and Facebook) didn't seem so strange; they actually seemed familiar, and I felt like they understood me as a person.

MSN knew that sometimes I wanted to talk to people I know when I'm not near them and couldn't because I'm not telepathic, and Facebook knew I wanted to share my most treasured photographed memories with my friends, but it was not convenient to carry photo albums with me at all times.

And my Samsung flip phone knew I didn't want to have to wait until I was in the study to speak to someone I know who isn't nearby, but I couldn't because my voice isn't loud enough and pushing your finger at the air in front of you two times and then three times to the centre left doesn't do anything.

As scepticism surrounding the trustworthiness of information and interactions becomes an ordinary concern, taking rank alongside a backdoor burglary, we must contemplate how our perceptions of trust and, subsequently, the way we trade it as a commodity have changed.

Have you ever contemplated that if we took the time more often to override our innate human wiring to opt for the path of least resistance and susceptibility to biases, then perhaps we wouldn't be so passively, yet aggressively, sceptical about information and interactions across digital ecosystems?

For example, perhaps the spread of misinformation – information to the contrary of superior agendas – is only a threat because of the common failure for audiences – people – to interrupt their passive consumption habits. The dissemination of misinformation is not a new phenomenon – it's just published, deployed and consumed more dynamically and quickly than previously possible due to the democratisation of information distribution, particularly thanks to the likes of social media.

It's long been economically acceptable to trade our trust based on gut instinct at will, with emotion and individual subjectivity being key influencers on our trading decisions thereof.

Once upon a time, we (generally) trusted each individual to grant their trust conditionally at their absolute discretion, which, in turn, created unique value exchange streams through creative, contextual and strategic thinking previously not possible through computerised mechanisms.

As our routine livelihoods have increasingly been digitised at scale, and with unbelievable ease, via the internet, has trust become a commodity to the extent that human factors – such as emotional goodwill and subjective diligence – are no longer valued across economies?

With people continuously reported as being the greatest threat to the security posture of any entity, perhaps it's become obvious that we can no longer be trusted to grant trust conditionally in our unique human ways.

Breathtakingly, it's conceivable that the humanness associated with trading trust traditionally no longer holds economic value in our digital age; it's become a liability of status that can never be wiped from a balance sheet of historical norms.

While robots may not actually conquer the world and retire the role of cohorts across geographies, we are at a pivotal moment that will be of historical importance to the rapidly evolving interdependent relationship between humans and technology.

The statistics flooding through every media feed across the world insinuate that we as people have no choice but to surrender our connectedness to the subjective trading of trust, and put this important economic activity in the hands of technologies that are, hopefully, less victimised by their biases and ability to develop habits where machine learning, and the like, are present.

Poor judgements in the trading of trust by good-intentioned people have given rise to the growing profitability of cyber warfare and criminality. Simply put, cybercriminals cannot be trusted because law-abiding cyber citizens cannot be trusted.

As a global society, we find ourselves at the mercy of familiarity's simplistic beauty fuelled by our hunger for effort preservation and profit.

It's not our fault, we're only human.

What concerns me is the strengthening and seemingly substantiated debate, by consequence of humanness, that although it may not be our fault, perhaps the way we are is code incompatible, to a fault, with some of our technology counterparts who we have intertwined with our livelihoods. •

About the author

Sally A Illingworth is regarded for her distinguished ability to assimilate, analyse and interpret information to bolster communications. She is a globally recognised business personality on LinkedIn, boasting more than 89 million organic content impressions.

Analysis of real cybercrime operators

BY JACOB LARSEN, SENIOR CONSULTANT, CYBERCX

When executives see ransomware attacks in news headlines, pressure is applied downwards to the cyber security function of the organisation to ascertain whether the business may also be vulnerable to a similar attack.

Jacob Larsen

Some of the questions that are often asked are, 'Could our organisation be targeted by a similar type of hacker?' or 'What do we need to do to make sure this doesn't happen to us?'

Answering these questions is not easy, and there is no simple way to provide assurance. A time line must be established of the steps that the attacker took to achieve their objective and assess the effectiveness of controls that are implemented at each stage.

Despite news headlines allocating perpetrators of cyber attacks on organisations as typically one large, powerful and all-evil hacker, data breaches in modern times are often caused by multiple different threat actors with varying skill sets and sophistication. These threat actors operate highly independently from one another but broker their services and access to each other in an organised fashion, congregating and transacting on underground forums.

This article will review three cybercrime operators that support the different stages of the life cycle of a ransomware attack (as displayed in Figure 1); perform analysis on their tools, techniques and procedures; and provide important recommendations to improve organisations' resilience.

Phase 1: initial access

As the ransomware monetisation model has grown exponentially in the past year, the demand for compromised initial access has surged, which has encouraged a new wave of 'initial access brokers'. This is a term that is used to describe actors who supply initial low privilege access to the highest bidder,

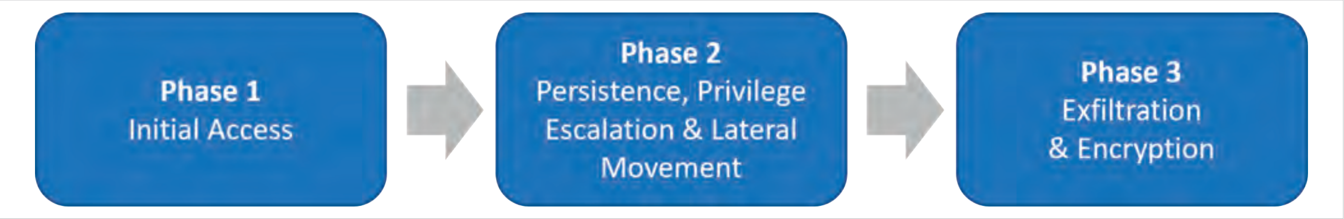
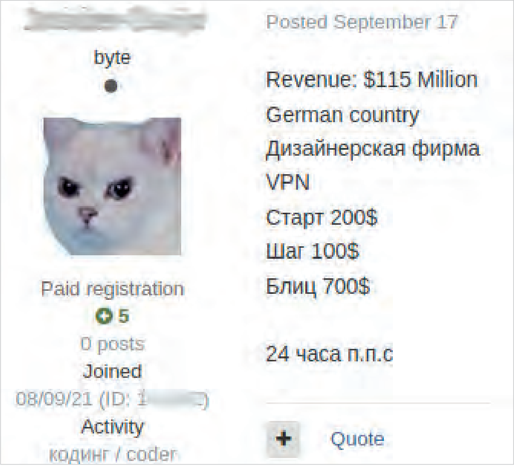

Phase 1
Initial Access
Phase 2
Persistence, Privilege Escalation & Lateral Movement
Phase 3
Exfiltration & Encryption

Figure 1. Three phases of compromise



[redacted]
byte
Paid registration
5
0 posts
Joined
08/09/21 (ID: 1[redacted])
Activity
кодинг / coder

Posted September 17

Revenue: $115 Million
German country
Дизайнерская фирма
VPN
Старт 200$
Шаг 100$
Блиц 700$

24 часа п.п.с

Figure 2. Initial access broker spotlight

namely malicious penetration testers and ransomware operators.

There were four primary techniques that were observed to be in use by initial access brokers on underground forums. These methods included opportunistic access through information-stealer malware distribution, password attacks, exploiting vulnerable internet-facing infrastructure and social engineering through phishing.

Figure 2 displays a Russian-speaking initial access broker that was observed selling virtual private network (VPN) credentials for a German-based graphics design firm with US$115 million in revenue. While the buy-now price for this access was US$700, it was later sold to a malicious penetration tester for just US$150. It was discovered that their method for compromising this organisation was opportunistic and they weren't intentionally targeted. They even went as far to write on a thread (translated from Russian): 'I don't know what the rights are, and I don't know how to look at a VPN, and I won't.'

The threat actor had compromised VPN credentials by deploying an information-stealer malware to a range of victims by masquerading it as a legitimate software download. This malware was spread like a giant net being cast in the ocean, and stole credentials stored on infected machines from browsers, auto-fill forms, and passwords saved in the system and in cookies. In this case, the VPN credentials were likely compromised from an employee's infected personal device.

Employees will store their organisational credentials insecurely without appropriate security awareness training. Building a situationally aware and cyber-resilient workforce is not something that will happen overnight, and it requires a top-down approach with managers and executives leading by example. Organisations should consider implementing a password manager to prevent the exfiltration of credentials using this method.

Other observed techniques by threat actors included attacks targeting weak passwords, such as password spraying, dictionary attacks and credential stuffing. The Australian Cyber Security Centre recommends that organisations ensure passwords use all complexity requirements, are a minimum of 14 to 20 characters in length, are changed every 90 days, and that users who do not set their initial password are required to change it on first use.[1] Accounts should also be locked out after a defined sequence of failed attempts.

Social engineering attacks, such as phishing and vishing, are also widely known to be used by initial access brokers, and it was observed that valid Office365 credentials for Australian organisations were sold for as little as US$6 each on underground forums. This signals the utmost importance of organisations using controls such as multi-factor authentication, and conditional access controls such as IP allow-listing and geoblocking.

While exploiting vulnerable internet-facing infrastructure is also a known method, it was not observed as being widely used for obtaining an initial foothold, due to the required investment of time and resources; however, to mitigate this, organisations should implement a defined patch management schedule that prioritises patches based on the criticality of the system and the type of information processed.

Phase 2: persistence, privilege escalation and lateral movement

Persistence consists of techniques that threat actors use to ensure their initial foothold on the network is not lost due to changes in the environment, such as system restarts or changed credentials.[2] The most common techniques observed to maintain persistence included launching a command

[1] https://www.cyber.gov.au/acsc/view-all-content/advice/guidelines-system-hardening

[2] https://attack.mitre.org/tactics/TA0003/

and control (C2) implant, modifying dormant accounts to create a backdoor, and setting scheduled tasks to create a reverse shell.

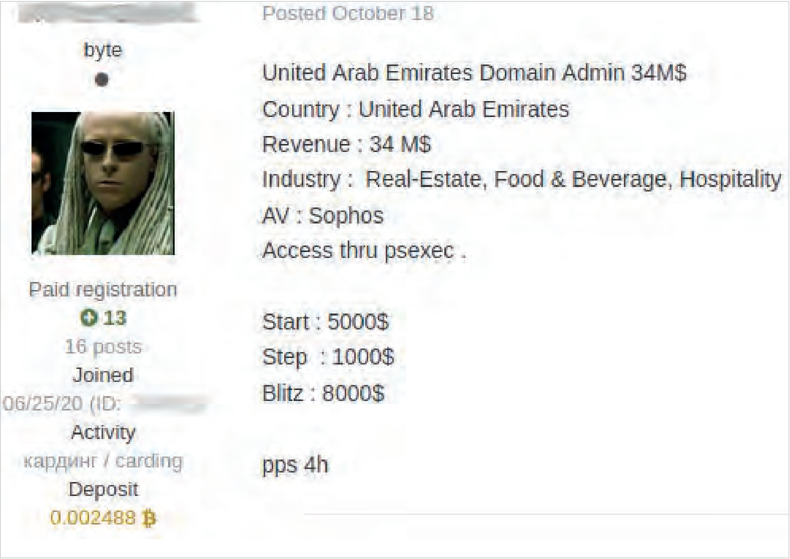
Cobalt Strike is a common threat emulation tool used by both industry penetration testers, and cybercriminals to maintain persistence. It includes functionality to set up a C2 server and implant malicious code on targets that call back to receive scheduled tasks.

Once a C2 implant is on infrastructure, it will maintain persistence by being launched at system start-up or user log-on, by either modifying registry run keys, adding it to the start-up folder or by using Windows logon scripts.[3] To mitigate this, organisations must analyse network traffic for uncommon data flows. This includes reviewing processes that typically do not use network communication, and analysing packet contents to detect application layer protocols that do not follow the expected standard. This can be quite expensive and difficult to implement, therefore it is recommended to focus on using Endpoint Detection and Response software for alerting.

Adversaries also look to control dormant accounts within the network, which are usually from staff on extended leave. To mitigate this, organisations should ensure there is integration between the human resources and system administration functions of the organisation. When an employee's working status changes, a ticket should automatically be raised with the system administration team to temporarily disable the user's account and remove them from unnecessary Active Directory groups.

Threat actors also use scheduling functionality to recurringly execute malicious code to create reverse shells. This technique has also been observed being used in the wild by malware families such as LokiBot and Remsec.[4] Mitigations for operating systems will vary, but ultimately rely on scheduled tasks being audited locally or through a centralised logging source.

While privilege escalation and lateral movement are separate techniques, they are often combined together as it is easier for a threat actor to laterally move throughout a network and compromise other accounts than it is to escalate privileges from a standard user account to a local administrator on a single workstation. This is also due to initial compromise being in heavily controlled and monitored environments such as Windows Virtual Desktops, Citrix Gateways and Standard Operating Environment workstations.



[redacted]

byte

●

Paid registration

⊕ 13

16 posts

Joined

06/25/20 (ID: [redacted]

Activity

кардинг / carding

Deposit

0.002488 ฿

Posted October 18

United Arab Emirates Domain Admin 34M$

Country : United Arab Emirates

Revenue : 34 M$

Industry : Real-Estate, Food & Beverage, Hospitality

AV : Sophos

Access thru psexec .

Start : 5000$

Step : 1000$

Blitz : 8000$

pps 4h

Figure 3. Malicious penetration tester spotlight

Privilege escalation refers to gaining a higher level of privilege than the initial access originally had. This can be completed at the host level, by upgrading from a standard user to a local administrator (NT_AUTHORITY/SYSTEM on Windows and root on *nix), or it can be completed at the domain level, by moving laterally throughout the network to new systems and resources that have higher privileges or trust, such as an exchange server or domain controller.

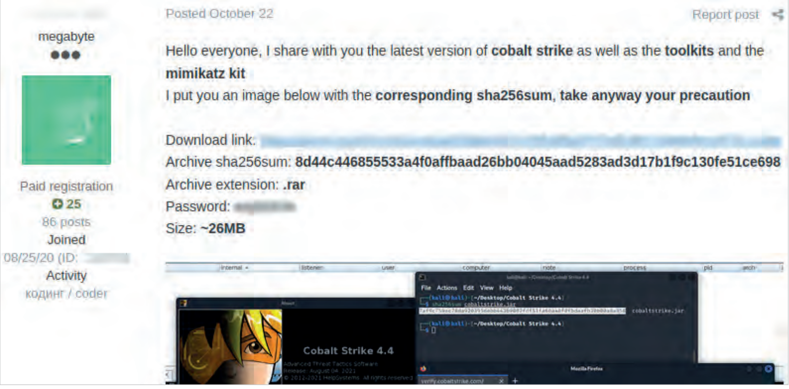
The most common observed privilege escalation techniques included attacks leveraging Kerberos, adversary-in-the-middle attacks such as LLMNR (Link-Local Multicast Name Resolution) poisoning, LSASS (Local Security Authority Subsystem Service) credential dumping and gaining access to passwords misplaced in network shares.

Figure 3 displays a malicious penetration tester selling Domain Admin access to a US-based real estate organisation with a revenue of more than $350 million, for a buy-now price of US$24,000. This user primarily relied on Kerberos-based attacks to escalate privilege and move laterally through compromised networks. This user was also seen purchasing access from the initial access broker in Figure 2.

Kerberos is a network authentication protocol used by default in Windows Active Directory environments, based on utilising tickets to allow nodes to communicate and

[3] https://attack.mitre.org/techniques/T1547/001/

[4] https://attack.mitre.org/techniques/T1053/



[redacted]

megabyte

Paid registration

25

86 posts

Joined

08/25/20 (ID: [redacted]

Activity

кодинг / coder

Posted October 22

Report post

Hello everyone, I share with you the latest version of **cobalt strike** as well as the **toolkits** and the **mimikatz kit**

I put you an image below with the **corresponding sha256sum, take anyway your precaution**

Download link: [redacted]

Archive sha256sum: **8d44c446855533a4f0affbaad26bb04045aad5283ad3d17b1f9c130fe51ce698**

Archive extension: **.rar**

Password: [redacted]

Size: **~26MB**

```
┌──(kali㉿kali)-[~/Desktop/Cobalt Strike 4.4]
└─$ sha256sum cobaltstrike.jar
                                                      cobaltstrike.jar
┌──(kali㉿kali)-[~/Desktop/Cobalt Strike 4.4]
└─$ 
```

Figure 4. Use of Cobalt Strike

prove their identity.[5] Kerberoasting is used to steal tickets and retrieve service account credentials as a standard user. A threat actor is able to request a Kerberos service ticket, capture that Ticket Granting Service (TGS) from memory, and then crack the targeted service account hash offline. This is possible because a component of TGS tickets are encrypted using ciphers with the service account's NTLM hash by design.

With low complexity requirements, the NTLM hash can be cracked and the password can be used to move laterally. Organisations should mandate complex passwords of 25 or more characters for service accounts, and if possible, be changed every 30 days. Kerberos encryption should also be changed to AES-256. In general, the principle of least privilege should be applied, to ensure that the minimum required number of users are assigned to the domain admin group, and other admin functions should be delegated to separate accounts to prevent the extent of compromise.

LLMNR is a protocol used by default in modern Windows operating systems and allows hosts to perform resolution on the same local link.[6] When Domain Name System (DNS) resolutions fails, the host will broadcast to all other machines on the local network for the correct address via LLMNR or NBT-NS. If the host was attempting to open a Server Message Block (SMB) connection and it identifies the machine, it will pass across its username and NTLM hash (v1 or v2).

In an enterprise environment, there are often legacy scripts regularly attempting to broadcast messages to decommissioned or renamed hosts, and therefore DNS resolution will fail and the LLMNR protocol will be used. An attacker can exploit this by masquerading as the target machine that the host is trying to resolve to, and if a SMB connection is attempting to be opened, can receive a copy of its credentials.[7]

Organisations can mitigate this by disabling both LLMNR and NBT-NS. This is required because NBT-NS is used automatically if LLMNR is disabled. Inter-VLAN communication should be limited to reduce the success of local network attacks. Additionally, automated scripts should only use the lowest privilege possible to perform tasks, to prevent the extent of compromise.

LSASS is a process used in Windows operating systems for enforcing the security policy on the system, and verifies user logons, handles password changes, and creates access tokens. To undertake its function, the LSASS.exe process will cache a copy of previously logged in user passwords and password hashes. With access to the NT_AUTHORITY/SYSTEM account, the LSASS.exe process can be snapshotted, having the contents of its memory 'dumped'. This dump will contain any cached credentials.[8] These credentials can then be used by an attacker to pivot to other machines in the network, and then repeat the process on a new machine to pivot further until a highly privileged domain account is compromised. It is noted, however, that credentials are no longer cached in memory from Windows 8.1/2012 R2 onwards due to the implementation of protected processes.

This technique has been widely observed in use by both malicious penetration testers, advanced persistent threats, and ransomware operators, using a tool known as Mimikatz. To prevent the success of these attacks, additional Local Security Authority configurations should be implemented to prevent code injection that could compromise credentials.[9]

The final technique observed was gaining access to passwords stored in network share drives.[10] This can be as a result of poor security governance or because credentials within group policy settings in SYSVOL are encrypted using a key shared publicly by Microsoft in

[5] https://web.mit.edu/Kerberos/

[6] https://datatracker.ietf.org/doc/html/rfc4795

[7] https://attack.mitre.org/techniques/T1557/

[8] https://attack.mitre.org/techniques/T1003/001/

[9] https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection

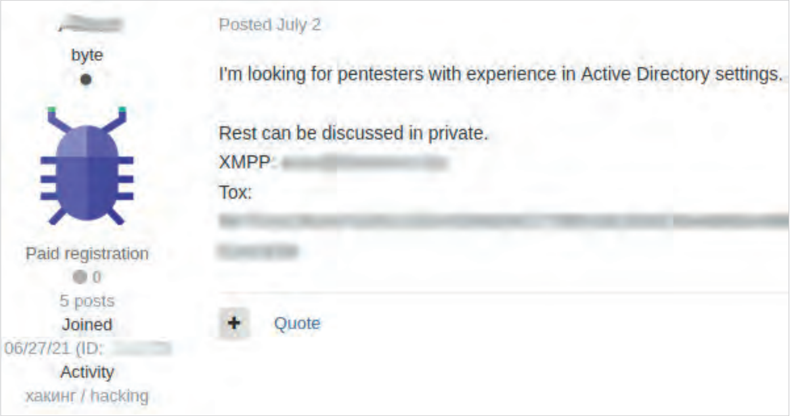
[10] https://attack.mitre.org/techniques/T1555/

2019.[11] Organisations should ensure that credentials are not placed in locations that are accessible by users or within group policy preference files. Network shares should be regularly searched for credentials that might be hardcoded in scripts or stored in documents for business efficiency.

Phase 3: exfiltration and encryption

In recent times, ransomware operators have moved to a 'double extortion' model, by both exfiltrating sensitive files, and encrypting all workstations, servers and backup infrastructure with ransomware.[12] The impacts and devastation that ransomware can cause are widely known, and every organisation will question whether or not they are susceptible to it.

Avos ransomware was first observed in July 2021 actively targeting Australian organisations, as seen in Figure 5. Malicious penetration testers, as observed in Phase 2, will either work with ransomware operators like Avos on a pay-per-access basis, or by operating on commission as affiliates.



[redacted]
byte
●
Paid registration
● 0
5 posts
Joined
06/27/21 (ID: [redacted]
Activity
хакинг / hacking

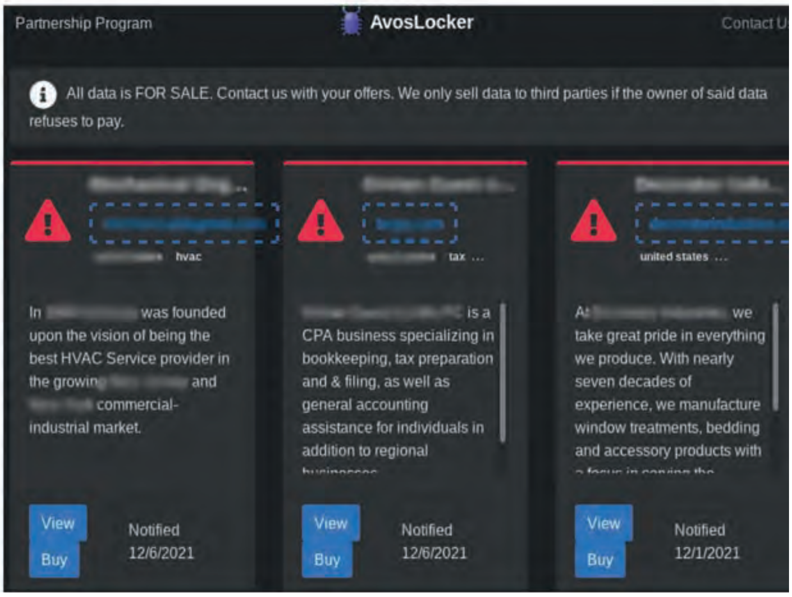
Posted July 2

I'm looking for pentesters with experience in Active Directory settings.

Rest can be discussed in private.
XMPP: [redacted]
Tox:
[redacted]

Figure 5. Ransomware operator buying access

If an organisation doesn't make a ransomware payment, their files are leaked on a data leak site maintained by Avos, which can be seen in Figure 6. The ransomware payload is typically delivered by either creating a group policy to distribute the package in the network or being remotely invoked as a process using PowerShell on all hosts.



All data is FOR SALE. Contact us with your offers. We only sell data to third parties if the owner of said data refuses to pay.

[redacted]
[redacted]
[redacted] hvac

In [redacted] was founded upon the vision of being the best HVAC Service provider in the growin[redacted] and [redacted] commercial-industrial market.

Notified 12/6/2021

[redacted]
[redacted]
[redacted] tax ...

[redacted] is a CPA business specializing in bookkeeping, tax preparation and & filing, as well as general accounting assistance for individuals in addition to regional businesses

Notified 12/6/2021

[redacted]
[redacted]
united states ...

At [redacted] we take great pride in everything we produce. With nearly seven decades of experience, we manufacture window treatments, bedding and accessory products with a focus in serving the

Notified 12/1/2021

Figure 6. Ransomware data leak site

There are various methods that ransomware operators can use for exfiltrating data, and if they have already obtained privileged domain access, it may be too late to prevent data leakage. Organisations should perform automated network traffic analysis to identify inconsistencies of outbound traffic, and regularly audit firewall rules and categorisation.[13]

Performing regular backups is critical, but organisations must not forget to implement a robust IT disaster recovery plan and incident response plan that contains procedures for regularly taking and testing backups.[14] It is important that not only the backups are tested, but the plan itself is tested by conducting simulation exercises regularly so that personnel are aware of their roles and responsibilities.

Conclusion

Protecting your organisation from cyber threats is like being involved in a game of 'cat and mouse', and it should be known there is no silver bullet or product that will provide the level of assurance the business needs in its resilience to cyber attacks. A layered approach of controls related to people, process and technology will truly apply the 'Defence in Depth' strategy to impede and disrupt a threat from achieving its objective. The review completed was not exhaustive, and there will always be other recommendations that can be made to improve cyber resilience. A shift in mindset is ultimately required by working on the assumptions that a threat actor already has an initial foothold, and further controls are required to identify, detect and isolate them from the network. ●

[11] https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-gppref/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be

[12] https://attack.mitre.org/techniques/T1486/

[13] https://attack.mitre.org/tactics/TA0010/

[14] https://attack.mitre.org/mitigations/M1053/

Maintaining the spark to make a dent in the cyber universe

BY IAN YIP, FOUNDER AND CEO, AVERTRO

Looking back on my exit from a corporate cyber security role, I now realise I was on the verge of burning out. Being in an industry where you sometimes feel like you've been slamming your head against a brick wall for most of it and unable to change anything wears you down.

I'd planned to take a sabbatical in mid 2020, but the opportunity to start Avertro – a cyber security software company – became the antidote. This mission has recharged my passion for cyber security and the conviction that we can all make a difference.

Ian Yip

Purpose

Cyber security is a challenging discipline, and it can be very rewarding, both for the wallet and for the soul. There are very few industries where one can tie their work to a real sense of purpose. The profession provides a direct link from one's day-to-day to making the world a better place, one keystroke at a time.

This is what attracts many to the industry. The days of the 'hoodie hacker in a bunker' image are not completely gone, but things have changed. There is a level of glamour associated with being a cyber security professional now.

Unfortunately, the more we think things are getting better, the more we are reminded that the same foundational challenges still exist. While cyber attacks are universally acknowledged as a top risk for all organisations, we continue to fight the systemic apathy that exists in boardrooms and at senior leadership levels.

This leaves many wondering if we're making our dent in the universe through cyber. In today's purpose-led society, why do we keep going if we aren't appreciated for it and cannot make the impact we desire?

Culture

Maintaining your spark starts with the culture of your organisation. A bad one will snuff it out, and the right culture will turn your spark into a flame that fuels your soul.

At Avertro, we have two key lenses when it comes to culture: company and security. Even before day one, we had our 'why', mission, vision and values defined. They remain to this day, and we've ensured that our team members are not just able to say what they are, but that we live by them.

From a security standpoint, it is critical that we do the right things and that our culture of maintaining our cyber resilience starts with our leaders. We even use our own platform to manage, measure and report on our cyber security performance.

The pandemic has thrown additional challenges at all organisations. As a result, we must be more empathetic, transparent,

flexible and fun. Everyone must actively and consistently check in with team members and listen when they share how they're feeling.

Cyber security is a tough profession given the ups and downs we encounter daily. Team members must rely on each other to get through some of the more difficult times, and there must be scope for vulnerability so people can feel safe knowing there will only be support, not judgement.

Reality

If you believe what you see on social media, then there is an abundance of mental health awareness in the cyber security industry; however, the reality is not quite as virtuous. Much of what happens isn't shared in public.

Stress levels are high, and many professionals, regardless of their seniority or tenure, burn out or leave for other reasons.

There is still a significant amount of toxicity, which drives people away. On top of this, we are struggling with a lack of understanding and accountability for cyber security at the most senior levels of organisations.

While it might sound obvious to say it's the chief information security officer's role to be responsible for improving and maintaining mental wellness in their teams, the truth is that many senior cyber security leaders don't have the required support from their board and executive teams to sustain their own mental health needs or a right-sized cyber program.

Making your dent

Whether you work in a startup or a corporate environment, being able to maintain the right state of mind is key. An organisation cannot be cyber resilient if it does not ensure its people are in the right headspace to defend it, and that they have the requisite support at senior leadership levels.

The cyber team is today's frontline against digital threats. It's therefore time that boards and executives stopped pretending to care and start taking cyber risk seriously. Simply doing so will significantly improve everyone's mental state.

To paraphrase Marie Kondo, we should all ask ourselves if the organisation we work in sparks joy, particularly in relation to cyber security. If not, we need to shake things up. Either make the change from within or vote with your feet so you can find your spark at a place that values you and has the right culture.

Leaders must actively work towards cultivating an environment where people have that glint in their eye and feel empowered by their spark to make a positive dent in the world. There is nothing more powerful than a group of people driven by real purpose. ●

About the author

Ian Yip *is the Founder and CEO of Avertro, the cyber-why company. Avertro is a venture-backed cyber security software company based out of Sydney, Australia. Yip has two decades of cyber security experience in a variety of leadership, advisory, strategy, sales, marketing, product management and technical roles, across Asia Pacific and Europe, in some of the world's leading companies, including McAfee, Ernst & Young, and IBM.*

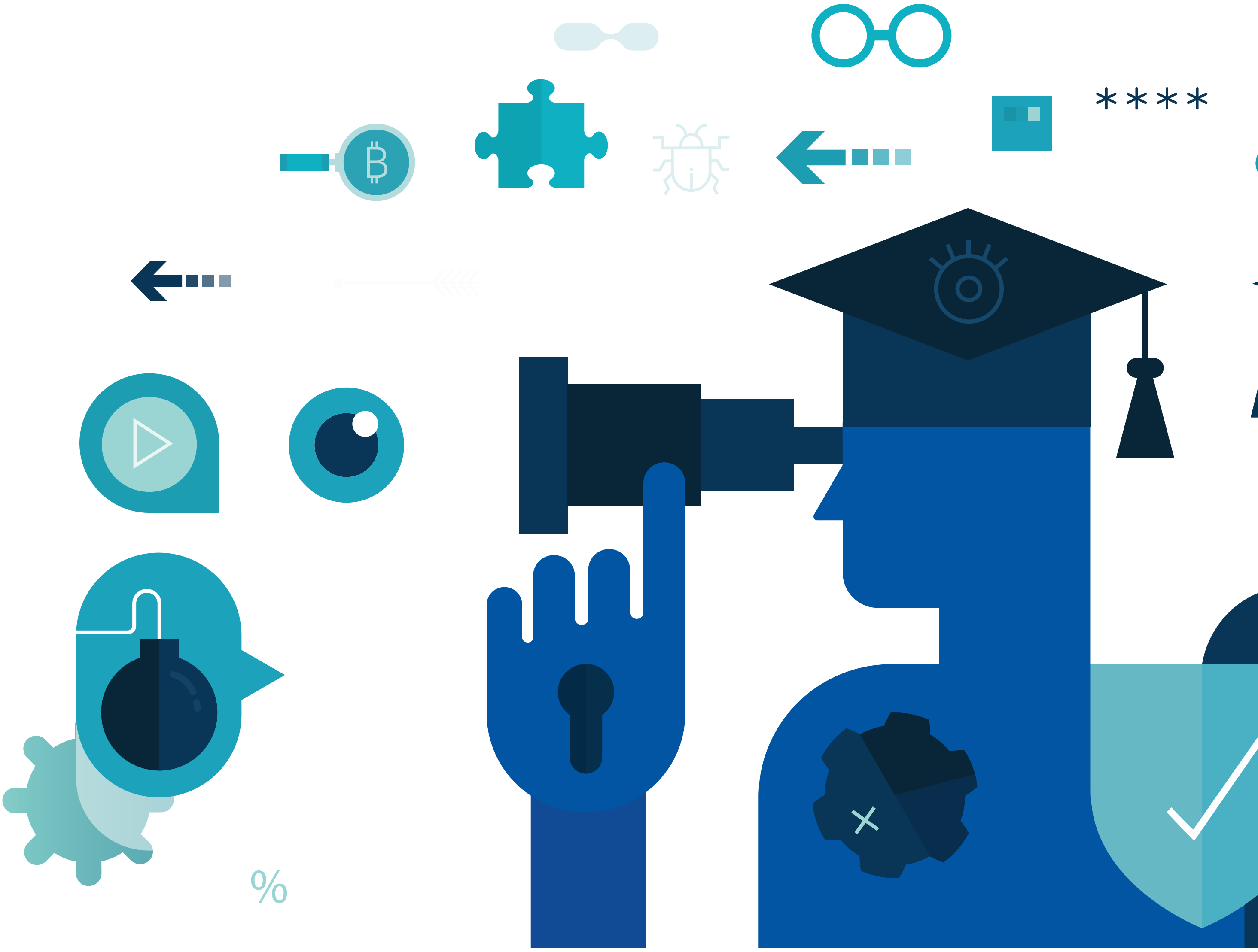
Cyber security education: reinvention required

BY PAUL C. VAN OORSCHOT, PROFESSOR OF COMPUTER SCIENCE, CARLETON UNIVERSITY, OTTAWA, CANADA

Industry and government must prepare for tomorrow's computer and internet security challenges.

To do so, what is necessary is nothing short of entirely new undergraduate degree programs focused on security – reinventing how we deliver security courses in higher education – and this requires direction and support from industry and government. The issue is how to educate tomorrow's security leaders – senior technical managers, policymakers, system architects, software developers and security experts – who will keep businesses, economies, and societies running in a world critically dependent on computer and communication systems.

We begin by clarifying that our primary scope is computer and internet security, although, like everyone else, we will default to the poorly defined catch-all term 'cyber security'. Our main focus is undergraduate programs (especially computer science and engineering departments) and core security knowledge as suitable for use across application domains – e.g., from infrastructure security to autonomous vehicles, smart cities, the Internet of Things, and others yet to emerge. Specialised advanced research – e.g., as carried out by research faculties with grad students and postdoctoral fellows –

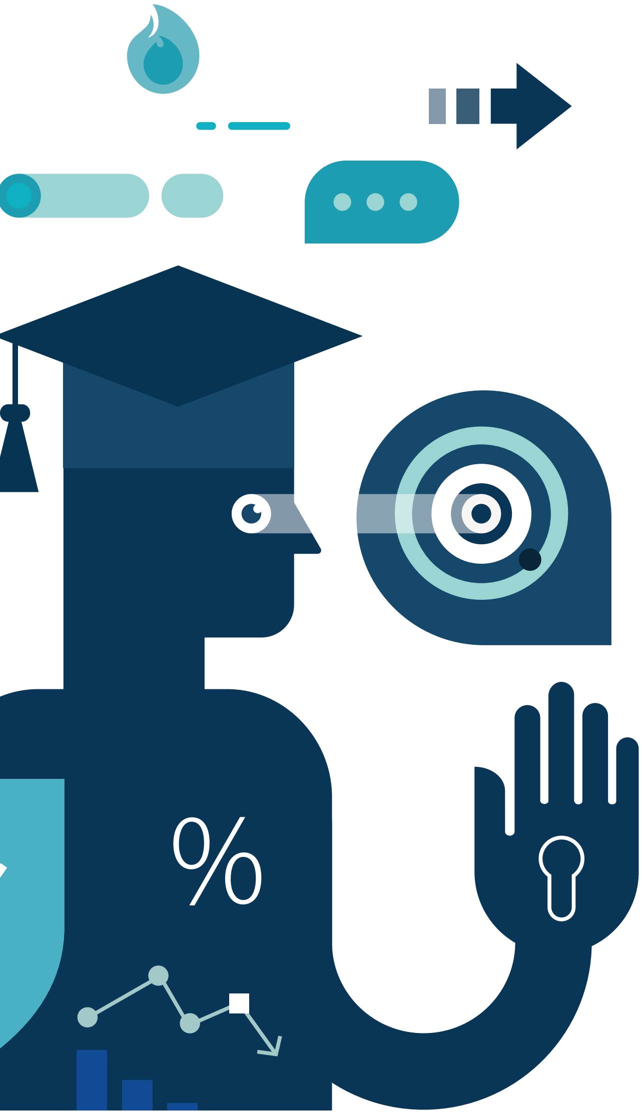


supports this effort but is not our main focus, and appears to be in better shape than undergrad security education.

Delivering effective higher education in cyber security requires many choices. Well beyond cursory mention or simple awareness within general computer science and engineering courses, we suggest that we need entirely new degree programs in security. These will provide knowledge far beyond that possible in the currently typical one or two available undergraduate courses in network or operating system security or applied cryptography.

As networked communication grew into wide use in the 1980s, courses in cryptography appeared, and network security meant security algorithms and protocols to protect data exchanges with remote systems. The early 1990s emergence of the web popularised client-server technologies and electronic commerce, along with antivirus software, firewalls, intrusion detection systems, and secure sockets layer (now TLS), aside from cryptography.

The parade of security technologies has continued to grow, and with it the complexity of networked hardware-software systems, cloud computing and network storage. As a result, a much wider knowledge base is required today for effective security leadership and to understand not only a vast volume of wired and wireless communications technologies and security mechanisms (e.g., for authentication and access control, and encryption and integrity), but also programming language-based software security; security testing and engineering for products and systems; IT security operations related to incident response and recovery; and broad interdisciplinary



knowledge related to security usability, social engineering, privacy, ethics, regulations and laws.

Current university programs are not generally organised, nor sufficiently staffed, to deliver this knowledge. They have existing priorities. Among the greatest challenges is the volume of material. If the baseline assumption is that security knowledge must be squeezed into existing computer science or engineering programs after the mandatory core material these programs already specify for degree requirements, there will never be room for more than one or, at best, a few security courses, typically as technical electives.

The problems with this approach are evident. First, in most current computer science and engineering programs, security is an add-on topic as a consequence of history – it arrived after the curriculum was well-established and packed tightly with existing priorities. Moreover, existing security courses typically require prerequisites that are often themselves second- or third-year courses – for instance, to do network security, students must first take courses in communication networks; before operating systems security, you must first take courses in operating systems and machine architecture; and so on. This then positions security courses as advanced, optional topics.

In addition, the first year or two of many computer science and engineering undergrad programs are largely filled with 'essential background courses', such as algebra, calculus, statistics and probability, and discrete mathematics – not to mention introductory basic programming and systems programming. And if in computer science, then also data structures and algorithms courses; perhaps also databases and software engineering; and so on.

This once again generally positions security courses late in the curriculum (third or fourth year), after several years of core computer science or engineering courses – or as a graduate-level topic. By the senior undergrad level, many students have already chosen specialisations in other areas, or are ready to start their careers, rather than to begin learning about systems security and cryptography. We repeat: Houston, we have a problem.[1]

There are actually several problems. First, how to find room to fit these topics and courses into existing programs. Second, finding instructors with the right expertise to deliver a given security course effectively. A related problem is securing funding to hire or retain such instructors, who are also in high demand in industry.

On the positive side, a relatively rich set of resources does already exist to guide the selection of security course topics, including detailed curricular frameworks.[i] One prominent such security curriculum document is from a joint task force involving the Association for Computing Machinery (ACM), the IEEE Computer Society, the International Federation for Information Processing and others, and is called CSEC 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity.[ii] A second source of guidance is the CyBoK effort, sponsored by the UK

[1] For the younger crowd, see: *Apollo 13*

Government; it aims to identify a so-called Cybersecurity Body of Knowledge. [iii, iv]

Another reason to rebuild cyber security curriculums from the ground up is that relying on existing courses as prerequisite background doesn't work well – with course content details controlled by instructors or external departments with different goals, designed to serve different target audiences. It may appear on paper to result in a resource saving, but this is self-delusion. Existing courses are rarely streamlined to focus on (only) the necessary background for a program whose main goal is to produce security experts. Pre-existing courses may also contain prerequisite material for later courses (in non-security programs), or themselves require prerequisites not relevant to security programs.

Why does reinventing the delivery of security education require direction and support from industry and government? Because it is industry and government experts who best understand the current skill set needs and shortfalls, and can hold universities to task. In contrast, many senior university administrators and decision-makers, who are otherwise responsible for development of new programs, have little or no firsthand experience (beyond academia) from which to make suitable curriculum choices. And these choices may result in narrow training programs delivering skill sets with short half-lives, or the pursuit of niche topics more suitable for graduate students of specific research professors. In contrast, what we believe will serve society best is broad-based security knowledge aiming to convey long-serving principles and concepts, and an understanding of the fundamentals and trends in computing and communications technologies, supported by hands-on exercises, labs and case studies that collectively prepare leaders capable of addressing tomorrow's security problems.

What about the many course-based Masters programs in security that have arisen, often being less technical or shorter certificate or non-thesis degree programs, on the order of 12 months? These programs serve a different purpose and audience, struggle to attract sessional instructors with

security expertise (those are snapped up at much higher salaries by industry), and rarely produce tomorrow's security leaders. Their true goal is typically generation of extra revenue, which the institutions then become dependent on, independent of program quality. This inevitably leads to another trap in order to meet revenue targets: admitting students who are part-time or have insufficient technical background to succeed. Such programs create false hopes, and often serve the best interests of neither the students nor regular faculty members. Quality education admits few shortcuts.

In summary, I suggest a need to reinvent how cyber security education is delivered. To do this properly requires building new customised programs from the ground up, with specialised courses designed to develop security experts. Courses designed to be more self-contained, themselves providing just-in-time background (e.g., in networking or operating systems), will allow security courses to begin in first or second year, rather than third or fourth.

The time for standalone programs in security has arrived, and is now supported by the ACM Curricula Recommendations overview report: Computing Curricula 2020 (CC2020).[2] This singles out cyber security as one of six distinct ACM domains: computer engineering, computer science, cyber security, information systems, information technology and software engineering.[3]

Such custom-built undergrad programs in security will succeed only if industry helps drive the desired curriculum, and governments provide incentives or direct support to encourage curriculums of societal benefit. The target is above short-term training, but below niche research areas beyond the expertise of typical instructors. The explicit goal should be to teach not what is easy for non-experts to teach, but what society requires towards developing a knowledgeable and capable workforce of security leaders, security-aware systems and software developers, security architects, system specialists and security experts – who will possess a combination of in-depth and generalist knowledge, as needed to address tomorrow's security challenges. ●

About the author

Paul C. van Oorschot is a Professor of Computer Science at Carleton University, Ottawa, Canada, and a Fellow of the ACM, IEEE and the Royal Society of Canada. Prior to academia, he carried out research and development in telecommunications and the security software industry. His most recent book is Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin *(2021, Springer).*

References

i. PC van Oorschot. Coevolution of security's body of knowledge and curricula. IEEE Security & Privacy 19(5):83-89 Sept-Oct 2021

ii. Burley, DL., Bishop, M., Buck, S., Ekstrom, JJ., Futcher, L., Gibson, D, Hawthorne, EK., Kaza, S., Levy, Y., Mattord, H., Parrish, A., 'Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity'. Joint Task Force on Cybersecurity Education, Version 1 Report, 31 December 2017, https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

iii. Rashid, A., Chivers, H., Danezis, G., Lupu, E., Martin, A,. 'CyBOK: The Cyber Security Body of Knowledge'. Version 1.0, 31 October 2019, https://www.cybok.org

iv. Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., Peersman, C. 'Scoping the cyber security body of knowledge'. IEEE Security & Privacy 16(3):96-102, May-Jun 2018

[2] https://www.acm.org/education/curricula-recommendations

[3] Data science is pending as a seventh domain

ECU recognises top graduates from two decades of cyber security

Twenty years ago, they commenced their studies in Perth in an emerging field known as computer security. Today, they are the innovators, leaders and entrepreneurs in the $250-billion cyber security industry.

Edith Cowan University (ECU) is celebrating two decades since the launch of its first cyber security courses by inducting 20 of its best and brightest graduates into the ECU Cyber Security Hall of Fame.

Since those first courses were launched in 2001, ECU has emerged as a world leader in cyber security education and research. It now has one of the largest programs of its kind in Australia, with more than 1400 students enrolled across 11 cyber security courses.

It is also the headquarters of the $140-million Cyber Security Cooperative Research Centre, and was recently included as the first Australian university in the International Cyber Security Center of Excellence.

School of Science Executive Dean Professor Andrew Woodward says the professional achievements of ECU's alumni is a testament to the quality of the university's cyber security teaching.

'It's outstanding to see ECU graduates now making a real difference, whether that's protecting our critical infrastructure, or as entrepreneurs finding solutions to big problems that affect us on a daily basis.'

ECU's cyber security programs have grown from humble beginnings with just a handful of students to a globally recognised powerhouse of the sector, producing hundreds of highly sought-after graduates each year.

'Our cyber security courses have grown by 50 per cent year on year over the past four years, which shows just how much this industry is now growing,' he says.

'For example, there are almost as many cyber students enrolled at ECU right now as the total number of those who graduated in the previous 20 years. Even then, we are barely making a dent in the global shortage of skilled cyber professionals – estimated to be more than 1.8 million this year.'

Graduates making a difference around the world

Hall of Fame inductee Christian Frichot founded his own cyber security firm in Perth and has since worked in Silicon Valley for tech giants including LinkedIn.

Frichot has a keen desire to mentor and develop the skills of up-and-coming professionals in the industry.

'My lecturers' drive for expertise had a long-lasting impact on me. I'm fortunate that I have had a great set of people that I have learnt from and collaborated with, and this network really started while at university,' he says.

Frichot believes that increasing diversity in the industry could go a long way towards helping fill the massive skills shortage in cyber security.

'I'd hope that if we continue to amplify under-represented minority voices in the industry, then surely that'll help continue to get younger people interested in the field,' he says.

Championing the push for diversity in STEM

ECU is renowned for widening access to education, and its computing and security discipline is no different.

ECU cyber security student Hannah Rice worked in a hardware store before embarking on her studies. She was recently awarded a prestigious national cyber security scholarship, and will have the

opportunity to work shoulder to shoulder with Department of Defence and Australian Signals Directorate (ASD) experts.

The Leisa Condie Defence Women in STEM Undergraduate Scholarship is worth $10,000 per year for the final two years of Rice's studies. The scholarship also gives her the opportunity to undertake professional placements within the Department and the ASD.

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

Rice is now in her second year of a Bachelor of Science (Cyber Security) degree. She says the scholarship was recognition of her success so far 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.

Rice started her degree in cyber security almost by accident after completing a Bachelor of Arts and spending the first part of her working life at Bunnings.

She says she is happy to be a model that other women pursuing a career in STEM can 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.'

Twenty-five women studying STEM degrees from universities around Australia were given scholarships as part of the program. ●

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

Getting started with cloud security

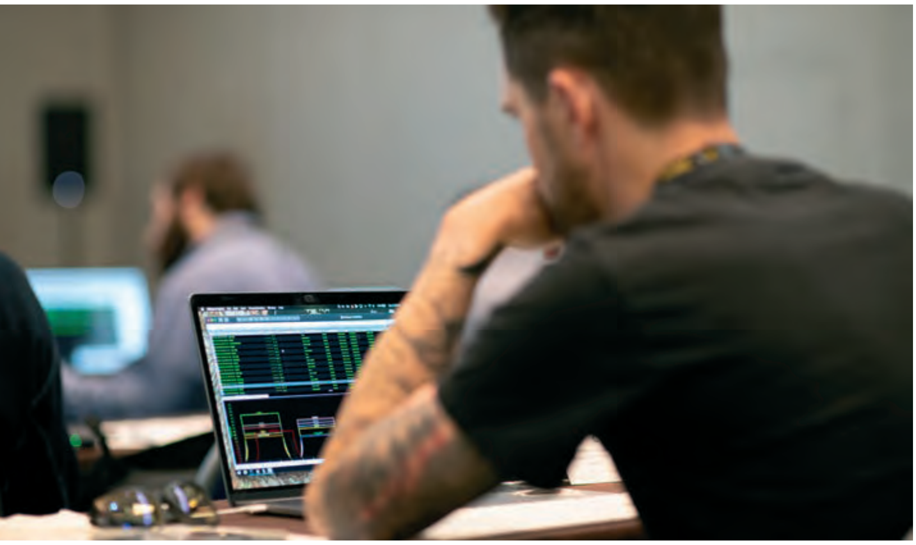
BY FRANK KIM, TECHNICAL DIRECTOR, CLOUD SECURITY CURRICULUM, SANS

Follow the money; where there's value, attackers will follow. Whether it's sensitive data that can be easily monetised, intellectual property that can be stolen, or business proprietary information, the cloud now has it all. The business drivers for moving to the cloud are undeniable, and organised crime, nation-states, and your competitors understand this. They may target your cloud systems and infrastructure directly, or, more often, go for the weakest link in your people, whether they be malicious or negligent insiders.

Common cloud security mistakes

The cloud has magnified seemingly simple security issues. Let's talk about the top three:

1. *Security misconfigurations:* Your engineer or administrator makes a mistake, resulting in a security misconfiguration. This insecure setting results in an entire folder of sensitive data being shared accidentally on the internet for anyone to download. Big mistake.
2. *Improper identity and access management:* It can be even more subtle than a simple misconfiguration. The cloud allows you to easily define who can do what within the cloud; however, it's not as easy as it seems. Overlapping and confusing settings can result in overly broad access, giving insiders and adversaries access to systems and data that they shouldn't have.
3. *Insufficient application security:* Cloud infrastructure is arguably more secure than many traditional on-premises environments; however, just because the cloud infrastructure is more secure, that doesn't mean attackers are going away. They will target the weakest link, which is now often your custom-built business applications. Application security controls and practices are now even more important in the cloud.



Tips for securing cloud environments

It may seem overwhelming at first, but it's also straightforward to get a handle on your cloud security. Learn the cloud provider's services in detail so you can use and secure them properly. This means multiple providers like AWS, Azure, and GCP, because your business will likely be using more than one in a multi-cloud world. Ensure you have appropriate monitoring and visibility to identify anomalous activity. Finally, establish consistent controls and governance processes. Remember, it's easy to make a mistake, but you have to expect that these mistakes will occur. Leveraging automation for consistency, and embedding security into your business and technical processes, will help to ensure you can build correctly from the start.

Is cloud security a shared responsibility?

Yes and no. All the major cloud providers espouse a 'shared responsibility model'. The cloud providers do handle a lot, such as physical security and security of the cloud infrastructure; however, it's up to you, the user of the cloud, to build and deploy secure systems and applications. Remember, if you have a breach, you're the one that is ultimately responsible to your customers, and will be the one in the headlines. ●

SANS

CLOUD SECURITY

Scan the QR code to find out more about SANS Cloud Security Courses!

Cloud Security Courses

FOR509: Cloud Forensics and Incident Response | 4 Days

SEC540: Cloud Security and DevSecOps Automation 50%+ new content and new lab environment | GCSA

SEC522: Application Security: Securing Web Apps, APIs, and Microservices | GWEB

SEC541: Cloud Security Monitoring and Threat Detection | Now 5 Days

SEC557: Continuous Automation for Enterprise and Cloud Compliance | Now 5 Days

SEC488: Cloud Security Essentials | 6 Days | GCLD

SEC510: Public Cloud Security: AWS, Azure, and GCP | GPCS | 5 Days + Extended Lab Hours

SEC541: Cloud Security Monitoring and Threat Detection | 3 Days

SEC557: Continuous Automation for Enterprise and Cloud Compliance | 3 Days

SEC584: Cloud Native Security: Defending Containers and Kubernetes | 3 Days

SEC588: Cloud Penetration Testing | 6 Days | GCPN

MGT516: Managing Security Vulnerabilities: Enterprise & Cloud | 5 Days

MGT520: Leading Cloud Security Design and Implementation | 3 Days

To find out more about Cloud Security Courses, visit www.sans.org/u/1kzc

SANS | GIAC CERTIFICATIONS