

AUSTRALIAN CYBERSECURITY MAGAZINE

THE MAGAZINE FOR AUSTRALIAN INFORMATION SECURITY PROFESSIONALS | www.australiacybersecuritamagazine.com.au

@AustCyberSecMag
Issue 10, 2021

**Organised Cyber Criminal
Syndicates A Growing
Threat: AusCERT 2021**

**Reimagining
Cybersecurity in
Government**

**Police Accessing COVID
Tracing App Data**

**Australia's "corporate
soft underbelly"**

**NSW Audit Office Report
Exposes Cybersecurity
Vulnerabilities**

**Where autism
offers a competitive
advantage**

**Ransomware Attack
Impacts Major
Brisbane Hospitals**

**The Cyber
Patient's Dilemma**



ATTACK ON **BITCOIN** ERODES PAYMENT STATUS



Cyber security weekly
podcasts highlights

PLUS

MySec
TV

MySmartTech.tv



CYBERSECURITY
EXPERTS ON YOUR SIDE

MANAGE YOUR IT SECURITY WITH EASE



**Trusted, multi-layered endpoint protection
against ransomware and zero-day threats.
Fully scalable and customisable.**



Best-in-class endpoint security

Combining the latest machine learning techniques with decades of human expertise.



Unique behavior and reputation-based detection

Get easy access to real-time feedback from over 100 million endpoints in ESET® LiveGrid.



Powerful, cloud-based sandboxing technology

Improved protection against ransomware and zero-day threats.



Outstandingly low false positives rate

Free up your resources to focus on what really matters.

**Ready to take your business security to the next level?
Find out more.**



Cyber
Outstanding Security
Performance Awards

**Recognising and rewarding
outstanding performance across
the cyber security sector globally**

Inaugural awards coming soon

**The Cyber OSPAs are supported by leading cyber
security associations around the world**

www.thecyberospas.com



@theOSPAs



**The Outstanding Security
Performance Awards**



New workspaces + new tools = new risks

Work securely from anywhere
with modern authentication

Keep your workforce working securely from anywhere with modern, risk-based multi-factor authentication – including biometrics, passwordless and other methods that deliver the flexibility you need and the convenience your users want. SecurID™ gives you control across all access points, including supported and unsupported BYOD devices, wherever people work.

Contact us for a trial or demo today
dickerdata.com.au/rsa-trial



An RSA Business

SECURITY
EXHIBITION + CONFERENCE

Elevated Intelligence

For a Smarter, Changed World

The world and the security industry have changed forever. Integrating physical security controls with advanced technology is top of mind worldwide.

Increased demand for video analytics, augmented reality, cyber security and robotics highlights just how important digital transformation and innovation is to the growth of the industry. Public safety is at the forefront and security is more critical than ever.

The Security Exhibition & Conference showcases the development of new solutions to essential hardware and security needs; witness firsthand the technologies that are changing how we respond to and analyse future information.

Security 2021 – Empowering industry for a smarter, changed world.

17-19 NOV 2021

ICC Sydney
Darling Harbour

REGISTER NOW
securityexpo.com.au

Lead Industry Partner



Co-located with

INTEGRATE
In partnership with
infocomm



Q1 2021 Internet Security Insights

WatchGuard Threat Lab

The Firebox Feed recorded threat data from

37,409

participating Fireboxes
A **21%** decrease from the previous quarter

Our GAV service blocked

8,599,420

malware variants
55% decrease in basic malware

APT Blocker detected

8,434,602

additional threats
16% increase in zero day hit

Intelligent AV blocked

203,895

malware hits **30%** QoQ decrease in IAV hits



26.4% OF MALWARE WAS KNOWN MALWARE

73.6% OF MALWARE WAS ZERO DAY

High-Level Threat Trends for Q1 of 2021

Zero day malware reached an **all-time high of 74%** in Q1. DNSWatch blocked over five million malicious domains during Q1, **a whopping 281% increase QoQ.**

New and Notable Threats

XML.JSLoader

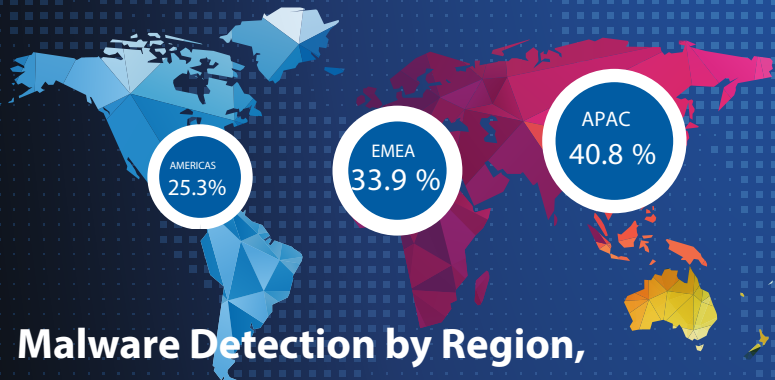
The character data (CDATA) found in the malicious XML sample contained a script that exploits an input validation flaw to ultimately launch PowerShell. The PowerShell command, hidden from the local victim, leveraged fileless techniques to download additional malware, which could take screenshots of your computer or install a trojan.

Zmutzy (Nibiru ransomware)

We found Zmutzy in the top encrypted malware. It can arrive either as an email or something downloaded from a website. Like many malware samples we receive by email, the message contains a supposed shipping notification asking you to review an attachment about your shipment. If a user interacts with this attachment, the malware compromises your computer and could install ransomware.

Linux.Ngioweb.B

We looked deeper into the top malware list, beyond the top 10, and found an interesting sample that recently targeted IoT devices, similar to the New Moon sample from last quarter. The first version of this sample targeted Linux servers running WordPress.



Malware Detection by Region,

Win32/Heim.D took the number one spot with **2,140,536** detections this quarter.

COUNT	THREAT NAME	CATEGORY	LAST SEEN
2,140,536	Win32/Heim.D	Win Code Injection	Q4 2020

Keen to learn about our end to end cybersecurity solution that won't let you down?

Book a non-obligatory virtual appointment with us and get a FREE Plantronics headset, while stocks last.



Read the full Internet Security Report at www.watchguard.com/security-report



CYBER WARS COLLECTION

An exclusive collection created
for cybersecurity awareness

SHOP
NOW



www.mysectv.shop

Contents



Director & Executive Editor
Chris Cabbage

Director
David Matrai

Art Director
Stefan Babij

MARKETING AND ADVERTISING

promoteme@mysecuritymedia.com

Copyright © 2020 - My Security Media Pty Ltd
GPO Box 930 SYDNEY N.S.W 2001, AUSTRALIA
E: promoteme@mysecuritymedia.com

All Material appearing in Australian Cyber Security Magazine is copyright. Reproduction in whole or part is not permitted without permission in writing from the publisher. The views of contributors are not necessarily those of the publisher. Professional advice should be sought before applying the information to particular circumstances.

CONNECT WITH US

- www.facebook.com/MySecMarketplace/
- @MSM_Marketplace
- www.linkedin.com/company/my-security-media-pty-ltd/
- www.youtube.com/user/MySecurityAustralia

OUR CHANNELS



Organised cyber criminal syndicates a growing threat for businesses: AusCERT 2021



Police chief defends accessing COVID tracing app data



How 5G and video surveillance create safer, smarter Australian cities



Where autism offers a competitive advantage



Attack on Bitcoin erodes payment status



e-Waste - The security blind spot

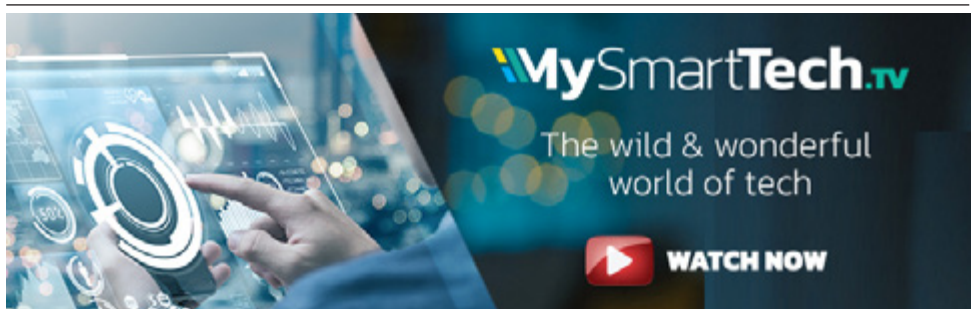
Editor's Desk	9
Feedback loop - have your say!	10
Organised cyber criminal ayndicates A growing threat For businesses: AusCERT 2021	12
Police chief defends accessing COVID Tracing app data	14
UnitingCare Queensland ransomware attack impacts major Brisbane hospitals	16
NSW audit office report exposes significant cybersecurity vulnerabilities at TfNSW & Sydney trains	17
Reimagining cybersecurity in Government through zero trust	22
Australia's "corporate soft underbelly" the first point of attack	26
How 5G and video surveillance create safer, smarter Australian cities	28
Where autism offers a competitive advantage	38
Attack on Bitcoin erodes payment status	30
Podcast episode highlights	35
The Cyber Patient's Dilemma	42
e-Waste - The security blind spot	44



Like us on Facebook and follow us on Twitter and LinkedIn. We post about new issue releases, feature interviews, events and other topical discussions.

Correspondents* & Contributors

- | | |
|----------------------|---------------|
| Andrew Curran* | Dr David Cook |
| Stuart Dahlenburg | Rob Joyce |
| Elliot Dellys | Steve Cropper |
| Mohiuddin Ahmed | Mikala Fanto |
| Paul Haskell-Dowland | Nick Savvides |



"The vicious accusations made by Washington have almost destroyed any trust between China and the US in the field of cyberspace. Their mutual suspicion is bound to significantly increase. There will be a higher probability that both sides could misjudge that the other side is launching cyber attacks."

- Editorial, *The Global Times*, Published 20 July 2021

Welcome back to the *Australian Cyber Security Magazine*. We're returning for Issue 10 from a 2020 hiatus.

Coincidentally, just as we took a broader, global view, in our launch of the *Cyber Risk Leaders Magazine*, COVID19 emerged and spread across the world. The pandemic subsequently triggered a massive rise in cyberattacks and misinformation campaigns. Let's not unpack the five issues of the *Cyber Risk Leaders Magazine* since that time, but just like our health professionals need to have a global perspective as they battle the pandemic, we as security professionals also need to maintain a global perspective, whilst still locally applying the appropriate controls and standards.

We return for the second half of 2021. So far, it has been a significant year for cybersecurity in Australia and set to escalate in intensity. All indications are we are in a declared cyber war with China. This sits amongst a much wider and deepening dispute with the soon to be largest economy in the world.

In July, Australia's Minister for Foreign Affairs, Senator Marise Payne said in a statement, "The Australian Government joins international partners in expressing serious concerns about malicious cyber activities by China's Ministry of State Security." In response, Chinese state media outlet The Global Times rebutted the allegations. "The Western world is unfamiliar with China's system, and cyberattacks are difficult to trace. Washington is exploiting them to frame China," the editorial said. "The US cannot exploit these smears to substantively attack China. If the US takes aggressive measures, carries out national-level cyberattacks on China, or imposes so-called sanctions on China, we will retaliate."

In the shadow of the pandemic and disputes with China, you would have increasingly heard the word 'sovereignty' being promoted as either a solution or an advantage. As an island nation this is understandable. However, Australia is far from isolated and has limited sovereignty in terms of its security and defence. Much of our defence is reliant on the US and the Five-Eyes nations for intelligence sharing. Even more so in

a cyber-context, where borders don't prohibit or inhibit adversary behaviour across a worldwide web. Cybersecurity companies may espouse Australian sovereignty, whilst also opening offices in Washington and London. Much is said on maintaining sovereign storage and control over our data, but much of the infrastructure remains foreign in ownership and innovation.

Though the nation remains void of a dedicated Federal Government Minister for Cybersecurity, the Australian Government is definitely trying to improve. It understands the critical nature of cyber warfare and the protection of critical infrastructure. The vulnerability of our critical networks is understood, even though many in the general public remain unaware or distracted by the pandemic, set to continue into its third consecutive year.

In a response to the Joint Committee of Public Accounts and Audit's inquiry into an Auditor-General's report on cyber resilience, the Attorney General's Department advised it is receptive to mandating the Essential Eight cyber mitigation strategies. The Australian Government has also just released the Defence Data Strategy 2021-2023. With a degree of transparency, Defence acknowledged it faces challenges upgrading its data maturity. The department says low data literacy, an inability to search across the organisation for data assets, data workforce imbalances across their public service, defence force and industry personnel, and not being aligned with Australian Government, Five Eyes and best practice standards are making lifting data maturity harder.

Three data maturity surveys provided responses from nearly 4,000 Defence Department personnel. Despite some pockets of excellence, the survey confirmed that Defence has an overall low level of data maturity. The strategy includes creating a new data division at Defence and the appointment of a chief data integration officer. That person will lead Defence in rolling out 27 data initiatives across five strategic pillars.

The Chairperson of Australia's Cyber Security Industry Advisory Committee, Andy Penn, has also warned the country needs to stay the

course, investing money and resources along the way. In a recent speech to the National Press Club, marking the first Cyber Security Industry Advisory Committee annual report, Mr Penn confirmed more abundant and better-resourced cybercriminals, cyber activists, and increasingly emboldened nation-states have Australia under constant cyber-attack. "Defences have to be strong, adaptive, and built around a framework that is coordinated, integrated and highly capable."

The Cyber Security Industry Advisory Committee is but just one cog in the \$1.67 billion Federal Government investment to protect Australia from cybersecurity threats via its 2020 Cyber Security Strategy.

"The Australian Cyber Security Centre receives a cybercrime report every 10 minutes. Some 62 percent of small businesses have reported a cybersecurity incident. The World Economic Forum predicts cybercrime could cost the global economy US\$6 trillion in 2021," Andy Penn said.

In this edition, as a partner to Issue 5 of the *Cyber Risk Leaders Magazine*, we provide you the opportunity to consider Australia's cybersecurity posture. In particular, in the wake of a number of recent cyber-attacks and ransomware events, including on Australian education and healthcare sector organisations. We cover a broad set of the trends, from ransomware, organised cyber-crime and the cover feature on how cyber-attacks are undermining confidence in the crypto-currency Bitcoin. We also include links through to our Tech & Sec Weekly Series and the latest Cyber Security Weekly podcasts.

As always, there is so much more to touch on and we trust you will enjoy this edition of



Australian Cyber Security Magazine. Enjoy the reading, listening and viewing!

Chris Cabbage
CPP, CISA, GAICD
Executive Editor

WRITE FOR US!

The Australian Cyber Security Magazine is seeking enthusiastic cyber security professionals who are keen on writing for our magazine on any of the following topics:

- Digital forensics in Australia
- Workforce development
- Security in the development lifecycle
- Threat management and threat hunting
- Incident management
- Operational security
- Security book reviews
- Risk management
- True crime (cybercrime)

If you are interested in writing for us, please send your article pitches (**no more than 200 words**) to the editors' desk at:

editor@australiancybersecuritymagazine.com.au



Interested in Blogging?

You may or may not be familiar with our website, which also provides daily infosec news reviews, as well as our weekly newsletters. We'd like to hear from anyone who'd be interested in contributing blog posts for our platform that reaches out over 10,000 industry

professionals per month, where you can express your opinions, preferences, or simply rant about the state of the cyber security world. If you stay on topic and stick to the facts, we'll be happy to publish you. If interested, email the editors at : editor@australiancybersecuritymagazine.com.au

AUSTRALIAN
CYBERSECURITY
MAGAZINE



**App now
available
on iTunes &
Google Play**

**DOWNLOAD
NOW!**



Organised cyber criminal syndicates a growing threat for businesses: AusCERT 2021

By
Andrew Curran
Staff Writer
MySecurity Media

Organised syndicates of cyber criminals are emerging as a significant risk for large and small businesses worldwide. That is the takeout from a presentation by Professor Ciaran Martin at the AusCERT 2021 Cyber Security Conference on the Gold Coast in May.

Cataloguing the various players in the cybercrime business, the founding CEO of the National Cyber Security Centre and now Professor at the University of Oxford's Blavatnik School of Government said organised cybercrime was a security threat that all businesses needed to learn to counter. He says most cybercriminals are not very sophisticated technically, but they're tenacious and well organized.

"Any organization, however big or small, whatever it does, has got a bunch of risks that it needs to manage," Professor Martin said. "We need to demystify cybersecurity. We have to treat it as an ordinary business risk."

Citing the recent Colonial Pipelines ransomware attack in the United States, Professor Martin said a "bunch of hackers" out of Russia exploited basic weaknesses in corporate security to make some money. Professor Martin said the way many businesses failed to protect themselves against profit-orientated cyberattacks is a serious structural flaw with potentially widespread social and economic ramifications.

"The good news is when we look at the details of this and other cases, there are things we can do about it."

Professor Martin told the AusCERT Conference many businesses still needed to learn about cybersecurity and have an informed discussion about it. Senior management up to the boardroom level needed to increase their awareness and knowledge of cyber risks.

"We wouldn't have a board member sitting out a discussion on pension liability saying, 'Well I don't really understand that.' The same has to be true for cybersecurity.

"You don't need nation-state nation state defences. No one is asking small organizations, universities, local government... no one's asking them to be able to take on a hostile nation-state on their own," says Professor Martin.

But the man who now advises NATO on cybersecurity said many business and business leaders have to get smarter regarding cyber risks and cyber-attacks. At the outset, that includes asking some searching business-wide questions. How does the business propose to defend itself against any cyber-attacks? How does the business control use of privileged IT accounts? How does the business ensure software and hardware is up to date? How does the business ensure partners and suppliers protect any information the business provides to them? What authentication methods does the business use to control systems and data.

Professor Martin argues these are simple questions any business should be asking itself if it is serious about protecting itself against cyberattacks.

According to Professor Martin, cyberattacks, especially from organised criminals, are a growing but manageable threat. He argues cyber risks are rarely catastrophic. Instead, most cyber threats are the aggregation of small harms.

"Hype, fear, and uncertainty - that is our enemy," Professor Martin said on Thursday. But he also says the publicity surrounding recent cyberattacks is drawing more attention to the threat. If the publicity gets more businesses to pay attention to their own cyber vulnerabilities, Professor Martin contends that is a significant positive outcome.

UNDERSTANDING DATA LITERACY
Importance of Data Literacy - Insights of a Chief Data Officer
WHAT IS DATA LITERACY AND WHY ITS IMPORTANT

Kshira Saagar
Chief Data Officer

WATCH HERE

Watch on YouTube

Latitude
Financial Services

CYBER CRIME GOLD MINES IN AUSTRALIAN UNIVERSITIES
With 1.5 million students and 130,000 full time staff, Australian Universities are prime targets for cybercriminals

LINDSAY BROWN
VICE PRESIDENT, APJ

LogMeIn

WATCH HERE

NEW ENTRY TO AUSTRALIA & NZ CYBERSECURITY MARKET
Expands with application-aware workload protection offering

Rob Noble
REGIONAL SALES DIRECTOR - ANZ

WATCH HERE

minsec

THE NEED FOR SECURITY AND AWARENESS TRAINING
Cybersecurity professionals - Australia invests \$8 billion
FEDERAL GOVERNMENT ANNOUNCES \$8M INVESTMENT IN CYBER SECURITY PROFESSIONALS

Phil Rodrigues
Head of Security, APJ Commercial
Amazon Web Services

WATCH HERE

aws

CREATING A COMPLEX CASE
Using a Narrative Visualisation Tool for Crime Fighters
RESEARCHERS DEVELOP A NARRATIVE VISUALISATION TOOL FOR CRIME FIGHTERS

Dr. James Walsh
Research Fellow, Australian Research Centre for Interactive and Virtual Environments

WATCH HERE

University of South Australia

SECURE INTERNET GATEWAY
Cynterra wins major DTA contract for Secure Internet Gateway
DTA TO DEPLOY NEW SIG
CYNTERRA WINS CONTRACT

DRAGO GOZDANOVIC
Chief Executive Officer
CYNTERRA

WATCH HERE

CYNTERRA

ARTIFICIAL INTELLIGENCE
Call for funded National AI Strategy
Australia's National AI Strategy

Ron Gauci
Chief Executive Officer
AUSTRALIAN INFORMATION INDUSTRY ASSOCIATION (AIIA)

WATCH HERE

aiaa
australian information industry association

3G Why it matters?
Why 5G Matters

Chris Althaus
Chief Executive Officer
Australian Mobile Telecommunications Association (AMTA)

WATCH HERE

AMTA

Police chief defends accessing COVID tracing app data

By
Andrew Curran
Staff Writer
MySecurity Media

The Western Australian Government hurriedly introduced new legislation to strengthen the protection of information following a high-profile instance of police using data taken from the State's SafeWA app to assist in a murder investigation.

Western Australia introduced the SafeWA contact tracing app in 2020. It has since been used 245 million times to check in at venues around the state. When introduced, it was clearly stated the app's data was to be used solely for contact tracing purposes and should only be accessed by Western Australia health officials.

However, buried in the fine print was the ability for police to issue notices to hand over data. Western Australia Police used this power twice, serving warrants on the Western Australia Health Department, including when investigating the murder of a OMCG member.

Controversy now surrounds the privacy provisions of the mandatory app. As a result, the Western Australia Government introduced legislation in June to limit the use of the app and its data to infectious disease contact-tracing purposes only.

The new legislation is The Protection of Information (Entry Registration Information Relating to COVID-19 and Other Infectious Diseases) Bill 2021.

"The system was introduced in the middle of the global pandemic, and while access to this information was lawful, the WA Government's intention was for contact registers to only be used for contact tracing purposes," a media statement issued by the Western Australia Premier, Mark McGowan reads.

"This new legislation strengthens this commitment

and guarantees individuals' information collected through contact tracing tools to be used for one reason and one reason only - contact tracing."

The Western Australia Police have defended accessing data from the SafeWA app. Western Australia's Police Commissioner Chris Dawson said police would use all available means to investigate serious crimes.

"Don't expect me to do my job half baked," he told a Perth radio station this week. Nonetheless, the police actions have caused concern in Western Australia, leading to the legislative response from the Government.

Perth QC Tom Percy says police accessing data from the SafeWA app is no different from accessing bank, phone, or CCTV data. The QC said anyone who believed their privacy was sacrosanct was living in a "dream world."

"The fact that they could track people through the SafeWA app is no surprise to me whatsoever," the QC told radio station 6PR.

"I think it's unfortunate that he (the Premier) really coerced everyone into using the app on the basis that your privacy was never going to be infringed."

Premier Mark McGowan reportedly asked the Police Commissioner to desist from using the SafeWA app in criminal investigations. However, the police declined to do so.

"We attempted to negotiate an agreement with the police. They advised that it was lawful, and they couldn't not do things that are lawful," Mr McGowan said this week.

Agreeing the new legislation was important, the Western Australia Opposition criticised the rushed process and said the loophole should not have existed in the first place.

Forcepoint



SASE Security With True Data Protection

Make SASE real for your organisation.

forcepoint.com



UnitingCare Queensland ransomware attack impacts major Brisbane hospitals

By
Andrew Curran
Staff Writer
MySecurity Media

Hospital and aged care provider UnitingCare Queensland experienced a major cyber incident on Sunday, April 25. Ransomware software targeted UnitingCare's internal IT systems. That forced one of Brisbane's biggest hospitals to resort to manual back up processes.

The following Monday, UnitingCare Queensland confirmed the attack. In a statement, they said external technical and forensic advisors were working to restore systems, but a resolution timeframe was not yet in place. In addition, the Australia Cyber Security Centre (ACSC) was notified and is now involved.

UnitingCare Queensland runs two big Brisbane hospitals, St Andrew's War Memorial and Wesley Hospitals. They also operate several smaller hospitals in and are active across the aged care, disability support, and crisis response sectors.

The attack affected the UnitingCare's operational systems, including internal email and patient management systems. The incident was the latest in a series of attacks that have targeted healthcare providers in Australia. Aged care specialist Regis was impacted by a Windows Maze ransomware attack last August.

In September, Anglicare Sydney lost around 17GB of client data during a ransomware attack. Last month, Eastern Health in Melbourne experienced a cyber-attack resulting in IT systems going offline and some surgeries been cancelled.

Jacqueline Jayne, a security awareness advocate at cybersecurity consultancy, KnowBe4, said aged care and health care facilities are attractive targets for cyber-attacks because of the amount of personal data they have.

"This is not only health-related data, but personally identifiable information (PII) is also there for the taking.

"When you consider the completeness of information available on an individual, it is clear as to why it is so popular to cyber-attacks as the dollar value of the data increases significantly."

Following the cyber incidents against Regis and Anglicare Sydney in 2020, the ACSC flagged the vulnerability of the aged and healthcare sectors by financially motivated cybercriminals. The ACSC also said this was because of the sensitive personal and medical information they hold.

In addition to using personal data for identity theft and selling it on the dark web, functioning IT systems are critical for patient care. Attacks on aged and healthcare providers offer cybercriminals the chance to profit from selling personal data and restoring the provider's IT systems.

In the six months to December 31, 2020, the Office of the Australian Information Commissioner (OAIC) received 539 data breach notifications, up 5% on the previous six months. Of those 539 breaches, 23% (or 124 incidents) came from the health and aged care sectors. Malicious or criminal cyber-attacks accounted for 58% of all notifications.

Traditionally vulnerable to cyber-attacks, aged and health care providers like UnitingCare Queensland are now having to fortify their IT systems. But that takes time and money. In the meantime, it is a game of cat and mouse for profit-orientated cybercriminals. ▀



NSW Audit office report exposes significant Cybersecurity vulnerabilities at TfNSW & Sydney trains

By
Andrew Curran
Staff Writer
MySecurity Media

The New South Wales Government Audit Office has found two major government agencies, Transport for NSW (TfNSW) and Sydney Trains, are failing to manage their cybersecurity risks effectively. A critical audit report released on July 13 contained the findings.

The audit was undertaken to assess how well TfNSW and Sydney Trains identified and managed their cybersecurity risks. TfNSW is the lead agency for the NSW Government's transport agencies cluster and provides a number of IT services to the entire cluster, including Sydney Trains.

Sydney Trains is Australia's biggest urban rail operator, operating over 3,200 daily services and carrying 400 million passengers annually. It is a critical piece of infrastructure in Australia's biggest city.

The audit looked at how well the two agencies identified, planned for, and managed cybersecurity risks.

"Significant weaknesses exist in their cybersecurity controls," the audit concluded. "Neither agency has reached its Essential 8 or Cyber Security Policy target levels. This low Essential 8 maturity exposes both agencies to significant risk."

Cyber Security NSW manages the NSW Cyber Security Policy (CSP). The CSP sets out 25 mandatory requirements for agencies like TfNSW and Sydney Trains. This includes making it mandatory that agencies implement the Australian Cyber Security Centre Essential 8 Strategies to mitigate cybersecurity incidents. The Essential 8 are key controls that serve as a baseline set of protections that agencies can put in place to make it more difficult for attackers to compromise a system.

Other findings included low numbers of employees receiving basic cybersecurity awareness training. Only 7.2% of employees across NSW Transport agencies had

completed introductory cybersecurity awareness training by January 2021.

Further, executives were not receiving regular briefings regarding cybersecurity risks and how that risk was managed. The audit found neither agency had developed a culture where cyber risk management was an important part of the management process.

As part of the audit, a team conducted a simulated cybersecurity exercise on TfNSW and Sydney Trains. The team simulated a determined external cyber threat actor seeking to gain access to TfNSW's systems. Following the authorised exercise, both TfNSW and Sydney Trains requested the significant vulnerabilities detected during the audit were not released in the report, citing ongoing vulnerabilities.

The NSW Audit Office made seven recommendations in the report. They include developing and implementing a plan to meet Essential 8 targets, addressing the vulnerabilities identified, implementing appropriate cybersecurity risk reporting to executives, collecting supporting information for the CSP self-assessments, classifying and integrating all information and systems according to importance, undertaking rigorous analysis to re-prioritise CDP funding, and increasing levels of cybersecurity training.

TfNSW first received funding to implement its cybersecurity plan in 2017. Sydney Trains began received funding in early 2020. Combined funding has totalled \$42 million since 2017. Despite the funding and existence of cybersecurity plans, neither agency has mitigated its cybersecurity risks. The NSW Audit Office made both agencies aware of its findings late in 2020. In the following six months, neither TfNSW nor Sydney Trains remediated all the vulnerabilities identified. ▲



MySec TV
NEWS & INTERVIEWS

TECH & SEC WEEKLY

WATCH NOW
SUBSCRIBE

TIM JONES & STEFAN PRANDL
— MANAGING DIRECTOR & CTO

MYSECURITY MARKETPLACE

Introducing Hyprfire and the Firebug intrusion detection system

Interview with **Tim Jones**

Managing Director

And

Stefan Prandl

Chief Technology Officer

Hyprfire is an Australian cybersecurity start-up which has innovated the application of Power Law Statistical Distributions and Behavioural Analytics to achieve effective, real-time network anomaly detection.

In this interview we speak with Tim Jones, Managing Director and Stefan Prandl, Chief Technology Officer.



MySec.TV
NEWS & INTERVIEWS

TECH & SEC WEEKLY

WATCH NOW
SUBSCRIBE

IoT Security Vulnerabilities & Exploits

2:05 / 26:35

IOT security vulnerabilities

Interview with **Lani Refiti**

Regional Director of Claroty

We speak with Lani Refiti, Regional Director of Claroty and cover IoT Security Vulnerabilities & Exploits including some recent research by Claroty on:

- Schneider Electric Smart Meter
- Rockwell's FactoryTalk Asset Centre
- Ovarro's TBox remote terminal units (RTUs)
- OPC Attack Surface



Endpoint of singularity – Sentinelone disrupting the top right quadrant for endpoint protection

Interview with

Evan Davidson

Vice-President, Asia Pacific & Japan

And

Kelvin Wee

Director for Security Engineering, APJ
for SentinelOne

We speak with Evan Davidson, Vice-President, Asia Pacific & Japan and Kelvin Wee, Director for Security Engineering, APJ for SentinelOne and discuss how AI-driven innovations are disrupting the Top Right Quadrant for Endpoint Protection.

We also discuss what the Mitre Att&ck evaluation is, their methodology and why it has become one of the best sources for CISOs to choose their cybersecurity solutions. SentinelOne scored 100% for visibility in the evaluation and we cover the critical importance visibility has in providing extended detection and response capability.





The MySecurity Marketplace gives you the tools you need to grow as a security professional. Join our growing member base today.



EVENTS

Access to events, locally and globally



EDUCATION

Access certified courses, webinars and labs



SOLUTIONS

Access an eco-system of security and technology services, software, trials and demos



PROFESSIONAL DEVELOPMENT

Join a growing hub of security professionals.

OUR CHANNELS





Reimagining cybersecurity in government through zero trust



By
Nick Savvides
Senior director of
strategic business
FORCEPOINT

As the seriousness of the coronavirus pandemic became increasingly apparent early last year, the primary objective for the Federal government was to transfer work processes online, to ensure the public service could carry on with critical work without disruption. This presented a unique challenge, due to the sheer size of the Federal workforce and the amount of sensitive data those workers require – everything from personally identifiable data to sensitive national security information.

While remote working isn't new for many Federal and State government departments and agencies, the sheer scale and inversion of on-site and remote traffic volumes is. Large scale remote working and connectivity is the starting line for the Federal government – though not the finish line. Agencies must continue to evolve from a cybersecurity perspective in order to meet both emerging and future demands created by the pandemic. The most immediate need, however, is ensuring the safety of critical data which has now been spread across a wide network as a result of teleworking. A worker's laptop may be secure, for example, but it's likely linked to a personal printer that's not, and comingled with horribly insecure devices on a home

network. With the realisation that insecure home networks are now a primary access mechanism, it must be assumed that employees are connected via hostile networks, rather than just a subset.

Securing the tele-workforce in a new cyber world using Zero Trust

In the midst of the pandemic, the Australia Cyber Security Centre (ACSC) realised the need for improved cybersecurity practices and created an educational document titled "COVID-19 – Remote access to Operational Technology Environments" to help secure the imminent digital upheaval while flagging the potential risks of cyber attacks (COVID-19 malicious cyber activity). While the ACSC did a commendable job bringing to light many of the pressing cybersecurity issues in the COVID-changed world, like much of the guidance across the world at the time, the focus was on security for network and technical controls, with consideration for the people and human threats left to others.

As reported by the Office of the Australian Information



automated decisioning that works in all scenarios.

This means it's not enough to make periodic, or binary, trust decisions – such as say a successful authentication, or allowed access, or rule – but instead, observe activity and add real time decisions based on the observations. For example, in a traditional binary trust decision, a user is guaranteed access to certain data based on a successful authentication and access rules. Whereas in a true Zero Trust model, these are not guaranteed. Instead a user may authenticate successfully, but then be denied access to data they would normally be allowed because observed behaviour and risk are taken into account, in addition to the access rules.

For this to work effectively, agencies must be adept at identifying real time risk in order for Zero Trust to be both robust and friction appropriate, rather than frictionless.

In this new era, they should be continuously evaluating a user's base activity, behaviour, and sentiment using a wide variety of signals. This means not only understanding what normal behaviour looks like, but also what looks normal but is likely to lead higher risks. Armed with this information, real-time decisions can be made to prevent dangerous actions or escalate oversight even more. Behavioural analytics, which tracks how a user interacts with data and systems has evolved significantly. Growing from a simple pattern, file access and network activity analysis, and fixed rule triggers, today's tools provide high efficacy, high accuracy understanding of user risk. This is made possible not just through modern data-science based analysis techniques, but the sheer abundance of signals.

This provides agencies with science fiction-like understanding which can dynamically adjust and enforce policy based on individual users at each event, access and action as opposed to taking a one-size-fits-all approach that hurts workers' ability to do their jobs.

This additional continuous oversight and real-time decision-making address two of the key challenges described earlier, the human error factor and the loss of control in a remote work world. In fact, these should not be seen just as compensating controls, but actually security enhancing.

The role of the private sector

The current shift in the Federal workforce may seem daunting to some, but it represents a huge opportunity for the government and private sector alike. Over in the US, a commission into the government's structure and organisation for cyberspace recently highlighted the importance of public-private partnerships: partnerships that can help make modernised, dynamic Zero Trust solutions the new normal if they can overcome the unique scaling challenge that Federal IT presents. This model can also be adopted here in Australia. The government must not just embrace commercial providers, but work closely with them to enable such scale, reimagine its workplace, and drive innovation.

Shifting to a Zero Trust model means improved flexibility and continuity, which can help expand the talent pool that agencies and departments attract. Most government jobs were previously limited to one location, with no option for

Commissioner, there were 539 data breaches reported in the period between July and December 2020, a rise of 5% when compared to the previous six months. Furthermore, while malicious activity still remained the primary cause, it was revealed that 38% of these breaches were caused by internal human error. Perhaps even more concerning given the nature of its data, is the fact that the Australian government became one of the top 5 most breached industry sectors for the first time, with human error being the leading cause.

Considering the inversion of access, human error, and that many of the existing assumptions on which security architectures were built are now broken, Federal agencies face unprecedented and amplified security concerns. Federal IT professionals need to be asking questions about their existing programs, structures and security fundamentals to see if they still provide the expected efficacy in this new way of working.

Some of the key considerations are the principles of Zero Trust. While many view Zero Trust through a product lens, it is far better to look at it from a principle perspective, in particular continuous oversight, with continuous and

"Over in the US, a commission into the government's structure and organisation for cyberspace recently highlighted the importance of public-private partnerships: partnerships that can help make modernised, dynamic Zero Trust solutions the new normal if they can overcome the unique scaling challenge that Federal IT presents. This model can also be adopted here in Australia."

remote work. Thus, agencies lost out on great talent that was simply in a different part of the country.

Additionally, more flexible work schedules may also boost employees' productivity. A two-year Stanford study showed a productivity boost for work-from-home employees that was equal to a full day's work. In recent months, the government has seen first-hand that flexible and secure remote work can happen through the novel application of existing technologies – including Zero Trust architecture.

Harnessing the cloud with SASE

As the government embraces working-from-home as a near-future reality, they are also, by necessity, embracing the greater reliance on cloud technology. The ability to conduct day to day operations from remote locations, while advantageous, does not offset the wider security risks. The use of cloud technology mandates the ability to access secure information stored in a singular location through multiple endpoints, thus creating a broader attack surface.

An elegant solution presents itself in the form of the Secure Access Service Edge, SASE, which utilises a converged architecture - making it possible to simultaneously secure information in the cloud via a converged security and network stack. While Gartner in their initial definition of SASE included Zero Trust Network Access, a software defined perimeter that abstracts connectivity between an endpoint or user to a resource, there is significant scope add more Zero Trust principles into SASE.

The principles of continuous monitoring, continuous assessment and real-time decision making are ideally implemented in a SASE security model, as it converges both the signalling and control channels. In this risk-aware/ risk-adaptive SASE model, agencies will be able to monitor for irregular behaviour in real-time and respond in real-time, significantly minimising potential data breaches and security issues. Fundamentally SASE provides the ability not just to have visibility, but when combined with Zero Trust, also to have automated action.


In addition to the security benefits of SASE it also allows for reduction of complexity in environments bringing

benefits of simplified management, increased productivity and reduced operational costs.

The Bottom Line

Federal departments and agencies must evolve cybersecurity in a way that allows them to embrace remote work without being vulnerable to attack. It's not enough to get government employees online; users and data must be consistently secure as well. The mass shift to telework represents a huge opportunity for the public sector – which is growing both its remote work capabilities and its potential pool for recruitment – and for those in the private sector who can be responsive to this need.

In an ideal world, IT leaders would frequently overhaul and rebuild their network security from scratch to suit the ever-changing operating environment, rather than retrofitting legacy systems to suit a broadened network perimeter. In that ideal world, it's likely that Zero Trust principles built into a SASE architecture would be at the core of all solutions, due to its fit-for-purpose design that addresses the modern, distributed workforce.

The key to security in this new era of remote work, cloud and converged network and security is behavioural analytics combined with real-time responses. 



COURSES

Search and find all upcoming featured courses



Fri, Jun 18 10% Discount

Presilience®, Leadership and High Performance



Tue, Jun 01 \$800

SCADA & ICS Cyber Security Course



Tue, Apr 13

Bachelor of Cyber Security

Plus many more!

Australia's "corporate soft underbelly" the first point of attack

Security, Military and Cyber experts are alarmed by corporate Australia's lack of awareness or preparedness

By
Steve Cropper

In December last year, the then Home Affairs Minister Peter Dutton raised cyber security as a critical issue when he introduced the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and told parliament it was "a significant step in the protection of the critical infrastructure and essential services which all Australians rely upon".

He might have appeared like a prophet of doom back then when he told Parliament, "Australia has not suffered a catastrophic attack on our critical infrastructure, but we are not immune...Malicious cyber activity has been identified as one of the most significant threats affecting Australians".

While the original Bill dealt mostly with threats ranging from natural hazards such as weather events, it also considered human-induced threats such as cyber attacks, espionage, chemical or oil spills, and from trusted insiders.

Dutton said that Australia is facing increasing cyber security threats to essential services, businesses and all levels of government.

Since then, Dutton has moved to the Defence Ministry and we have seen cyberattacks on federal parliamentary networks, logistics, Channel Nine, banking ATM networks, the medical sector and universities, just to name a few.

Elsewhere, the Russian-linked SolarWinds attack and the China-linked attack on Microsoft Exchange have stunned governments and observers worldwide.

And yet, cyber security budgets in Australia's corporate sector have remained stagnant and executive teams continue to underestimate the level of damage cyber threats can do to organisations according to the Sophos survey report, The Future of Cybersecurity in Asia Pacific and Japan.

The survey found that 52 per cent of Australian organisations suffered a data breach in 2020, up from 36 per cent in 2019 – this is despite 61 per cent of Australian organisations claiming to have a proactive or better security capability in place today.

This is still considerably better than the average across Asia Pacific and Japan, where 70 per cent of surveyed organisations reported a breach in 2020, which is a two-fold increase since 2019.

At present, the new legislation is being reviewed by the Parliamentary Joint Committee on Intelligence and Security, but according to a leading academic in the field, all the new amendment does is announce the build-up of our already near non-existent cyber mitigation capability.

Former chief executive officer of the ANU's Cyber Institute Lesley Seebeck says the problem faced by the government is the demand curve in terms of the depth, breadth and level of cyberattacks on critical infrastructure is increasing.

"There are also a lot more nation states getting involved

The recent Australian Security Confidence Index (ASCI) showed that Australians feel most unsafe online (41%), especially people over 40, who fear cybercrime

in attacks and the supply chain in terms of people and cyber capability is pretty flat,” Seebeck said.

Vice-President of the Australian Security Industry Association Rachael Saunders said the key word in Cyber Security is the word “Security”.

“There are plenty of IT consultancies who advise their customers on fortifying their computer systems, but that is not enough. Cyber Security is about a lot more than just computer systems and organisations have to examine their operations from a broader security standpoint.”

Ms Saunders said corporates need to be better educated about how cyber incursions are done. “Cyber attacks include gaining access to codes via email phishing, people impersonating banks or other so-called trusted sources to gain critical data about people to help them break into companies’ systems. Cyber intruders get inside companies by taking jobs – even as cleaners, and sometimes, they just break in and steal critical information.

“So it’s important that companies stop thinking about cyber as just something that happens in computers and see it as a major security challenge, she said.”

Last year, the Australian Strategy Policy Institute’s researched Australia’s Cyber vulnerabilities and found: “Our approach to national security planning should now include key companies and their supply chains: it’s time to rethink our national security approach in a more complex, dynamic

and interconnected world.

Their Report, “From Board Room to Situation Room” described the corporate sector as Australia’s soft underbelly and the most likely point of first strike by a hostile nation state.

The authors recommended closer integration between Australia’s government security agencies and the Australian Defence Force with the private sector. “Our corporate sector is now a key component of our deterrent posture against a range of threats.”

Concerns about cyber vulnerabilities are not limited to the Government, Defence and the Security Industry. The recent Australian Security Confidence Index (ASCI) showed that Australians feel most unsafe online (41%), especially people over 40, who fear cybercrime, identity theft and other cyber attacks while using online banking, chatting in social media or online shopping.

In the final analysis, Australia’s characteristic “She’ll be right” attitude will have to give way to a strong dose of reality. The country as a whole will have to wake up and get cyber-ready before it’s too late. ▶

About the Author

Steve Cropper is Industry Affairs Officer for the Australian Security Industry Association Ltd.

How 5G and video surveillance create safer, smarter Australian cities

By
Rob Joyce
Chief Technology Officer, Nokia
Oceania

The rapid ascendancy of technology, coupled with a rising urbanization rate, has made governments around the world accelerate their plans to build smart cities that are safe, sustainable and prosperous. In Australia, the government has outlined a Smart Cities Plan to achieve this goal. The plan features Smart Technology as a core pillar, underlining its commitment to leveraging disruptive technologies to improve sustainability and drive innovation in the Australian cities of the future.

5G-based Internet-of-Things (IoT) solutions are a fundamental aspect of smart cities. This is especially pertinent for the enhancement of video surveillance cameras, which are already a fixture in modern cities. Over the next two years, they will be the largest market for 5G IoT solutions worldwide as the enhanced mobile broadband capabilities of 5G networks support higher image resolution and faster transmission speed. This greatly expands the capacity of these cameras to contribute to critical areas such as security, city planning, industrial automation and more.

Unlocking the potential of video through 5G

Current iterations of the standard closed-circuit television (CCTV) camera are usually dependent on cable or fiber-based networks, which means they can only be deployed in limited numbers at fixed locations.

5G mobile networks eliminate these limitations as they enable CCTVs to operate wirelessly and can support multiple cameras operating at once. This facilitates the creation of wireless multi-camera networks and gives rise to new implementations, such as having cameras attached to human bodies, vehicles, and drones to record footage and transmit data.

Transmitting high-resolution video in real time generates a high amount of data traffic, which is multiplied manifold when more cameras are introduced. This is a challenge for the previous generations of networks, but 5G's drastically increased bandwidth capacity enables network slicing to create channels exclusively for CCTV needs, ensuring high-quality results at the lowest possible latencies.

Transforming Australian cities through smart video surveillance

Where smart cities are concerned, the main advantage that 5G brings to video surveillance cameras is that it enables large-scale CCTV deployment in dense urban environments. Real-time, high-definition video transmission from multiple angles is a crucial element of building efficient, secure cities that make data-driven decisions. Unsurprisingly, CCTV deployment already features prominently in many approved smart city projects around Australia.



While CCTVs are best known for being used in a security context, 5G effectively transforms them into ‘multi-purpose sensors’ because the high quality of the video feed enables more accurate data analysis. The capacity for simultaneous real-time feedback also makes CCTVs valuable sources of information for other systems, such as traffic controls, as they can instantly execute certain actions or processes based on recommendations derived from the transmitted data.

As an example, the City of Darwin installed an additional 138 CCTVs with smart analytics in the city center as part of the ‘Switching on Darwin’ project in 2018 to understand pedestrian flow and traffic statistics for better city planning. Meanwhile, under the AU\$50 million Smart Cities and Suburbs Program, Kapunda – one of Australia’s oldest mining towns – launched the Smart Tourist Town project to increase the city’s liveability and tourism potential. CCTVs were installed around the Town Square and video analytics and movement tracking were used to provide quantifiable data and concrete evidence of how the space was being utilized.

Tackling the privacy question

The increasing commodification of data and its huge potential for exploitation means people are more guarded

over how their data is captured and stored, as well as what they are consenting to it being used for. There is a growing desire for greater data privacy, but less data freedom may limit the effectiveness of many modern security controls, which rely on large and detailed information databases to identify threats and authenticate access.

Video analytics at the edge may be a solution to navigate the dichotomy between security and privacy. For instance, the Australian city of Liverpool was used as a test bed for a sensor that could track objects of interest in a live video feed but would only transmit relevant indicators and metadata. Since no live images were sent and the local database was emptied at intervals, the device was compliant with privacy standards but still enabled data gathering for citywide traffic monitoring in real time.

This experiment suggests that the combination of smart CCTVs and video analytics at the edge could be a powerful combination for addressing privacy concerns without jeopardizing the benefits of data-driven planning. This is made possible because aggregating, processing and analyzing video streams locally on 5G edge clouds do not produce a centralized storage of video data. Thus, 5G infrastructure is an important enabler of this solution as it supports a distributed cloud architecture, in which edge computing is an essential element.

Surveillance, 5G and the future

Cities all over Australia are demonstrating a progressively greater commitment to tackle the economic and societal challenges of urbanization by investing in future technologies and digital infrastructure. Smart, wireless CCTV networks are an integral part of many of these initiatives as they can provide real-time, high-resolution video feeds for rapid yet effective contextual actions – and this is made possible by 5G.

The full potential of video surveillance in the future lies within the convergence of 5G technology and the sophistication of cameras and video analytics. CCTV systems are already being trained to prevent terror attacks by identifying people carrying weapons in real time, as well as being paired with air quality and noise sensors to evaluate the impact of traffic on air quality and noise pollution. Together, 5G and video surveillance can create smarter, safer and better cities for Australians as we enter a digital future. ▲



Attack on Bitcoin erodes payment status

By
Mohiuddin Ahmed
and
Paul Haskell-Dowland



With all the talk about bitcoin becoming mainstream, and some experts' predicting it could replace gold as a reserve asset, it is timely to consider how secure and anonymous Bitcoin transactions really are. Recent events in China and the US have eroded the value of Bitcoin and the idea of 'anonymous' payment transactions.

Unlike normal money, which is backed and valued by the government that prints it, bitcoin is run independently and has nothing backing it, meaning that its value is determined by the number of its users, that is, demand. This means that bitcoin can be worth anything from a few hundred dollars (as it was back in 2017) to over US\$60,000 in April 2021, before falling back to around US\$30,000.

China's ban on bitcoin mining in recent times has limited its broader acceptance as a payment form. Bitcoin in June fell below \$30,000 for the first time in more than five months, hit by China's crackdown on the world's most used cryptocurrency. Bitcoin has lost more than 50% of its value since its April high (subsequently partially rebounding). China has told banks and payments platforms to stop supporting Bitcoin transactions. That follows a recent government order to stop Bitcoin mining in Sichuan province. That takes out a huge level of demand for the

currency, now and in the future, given China is the world's second largest economy, set to become the biggest in coming years.

It is also a myth that bitcoin payment processes are infallible, secure and can't be compromised. This was highlighted recently when the US Justice Department traced and seized a large proportion of the bitcoin ransom that a major U.S. pipeline operator paid to a Russian hacking collective (DarkSide) after it shut down the Colonial Pipeline. An FBI taskforce in essence scammed the criminals, and gained access to about 63.7 bitcoins, worth around US\$2.3 million. That drove down the price of bitcoin and its status as being anonymous and secure was undermined.

Bitcoin itself is secure. It is encrypted and backed by the blockchain system; blockchain is basically a chain of multiple "blocks" which are an anonymous transaction history (a distributed ledger). In simple terms, the blockchain starts with an initial block and transactions are added through new blocks, creating a blockchain. But the infrastructure which enables transactions isn't necessarily secure.

If you hold bitcoin yourself, it is as fallible as the computer on which you hold your software wallet, containing the digital currency. Bitcoin 'miners' or owners hold private keys which are used to access their bitcoin,



similar to the passwords on our bank accounts. Generally, wallets will also contain a public key that is used to receive bitcoins (similar to a bank account number). If hackers can access our bank accounts, they can steal money from these software wallets by discovering these keys.

Digital currency owners may have the option to use multi-factor authentication for transaction verification; hence these accounts are attached to either an e-mail address or mobile phone number. Cyber-criminals can potentially compromise these – with many instances of digital currency owners having their coins stolen or obtained through fraud. Even the alleged creator of bitcoin, Dr Craig Wright, under the pseudonym Satoshi Nakamoto, apparently had his PC hacked in 2020, with encrypted private keys to two addresses stolen, enabling the criminals to steal substantial quantities of Wright's bitcoin.

Many bitcoin exchanges and online wallets have also suffered from security breaches in the past and such services generally still do not provide enough security to store bitcoin or other cryptocurrencies. If you own bitcoin, you should choose your bitcoin exchange and wallet software very carefully, because it is susceptible to hacking depending on the security of the software and exchange platform. Of course, making it too secure can be problematic

too as Stefan Thomas discovered when he locked himself out of his hardware wallet (a highly secure storage device) – holding bitcoin worth \$328m at today's value! .

This highlights the fallibility of the bitcoin system. Bitcoin is based on a proof-of-work mechanism and any party with malicious intent (and sufficient resource) can put together enough computing power to hamper the integrity of the transactions or cause network disruption. Bitcoin uses blockchain for keeping track of the transactions and if cyber criminals can control more than 50% of computing power in the blockchain network, then bitcoin transactions can be manipulated. This is called a 51% attack, a well-known potential risk that could destroy the bitcoin system.

Bitcoin is not necessarily safer than cash in a bank account and this will hinder its acceptance as a viable form of payment, something Tesla chief Elon Musk might have realised when it said in May that it wouldn't accept bitcoin for car payments, reversing an earlier decision. He attributed that decision to climate change concerns and the rapidly increasing use of fossil fuels for bitcoin mining and transactions. The huge carbon footprint of bitcoin will also hinder its broader acceptance as a payment form.

Moreover, without proper regulation, digital currencies will create more chaos and could make financial crime easier. There are also on-going challenges for tax officials to determine how to tax payments being made via digital currencies. Financial crimes such as tax avoidance on capital gains held by crypto investors or miners becomes easier due to the relative anonymity of transactions. As it is now, shell companies dealing with crypto currencies are yet to disclose profits or losses incurred, hence governments are being deprived of tax. There are even 'commercial' services to allow bitcoin to be laundered - although they are not as effective as advertised.

While bitcoin can be 'tracked' to various extents, there are other cryptocurrencies that are effectively untraceable. This provides protection for buyers/sellers for legitimate purposes BUT it also provides anonymity for those seeking to misuse, steal or hide activities. All of this will undermine bitcoin's progression to being a common form of payment in the way that cash or credit cards are today. ▲

Paul Haskell-Dowland

Associate Professor Paul Haskell-Dowland is the Associate Dean for Computing and Security in the School of Science at Edith Cowan University, where courses include the accelerated and 100% online Master of Cyber Security. Paul is a regular commentator on cyber issues featuring in local, national and international media (newspaper, radio and tv) and has more than 20 years' experience in cyber security research and education.

Dr. Mohiuddin Ahmed

Dr. Mohiuddin Ahmed is a Lecturer of Computing and Security discipline in the School of Science. Mohiuddin Ahmed has made practical and theoretical contributions in cyber security and big data analytics for several application domains. His research has a high impact on data and security analytics, false data injection attacks, and digital health.



The cyber patient's dilemma

By
Elliot Delys
Founder, Phronesis Security

A Head of IT asked me recently: why bother doing a risk assessment when we already know what's wrong?

It was a fair question – we had spent the better part of a month dealing with a significant security incident and had just concluded a high-level review of the infrastructure landscape. It wasn't good. There were servers running ancient operating systems, legacy equipment with unknown functionality, and poor configurations that had the network constantly at capacity.

The IT estate was a house of cards and it was a matter of when, not if, it led to a serious loss of information availability or confidentiality. This we knew. What we didn't know was how this had come to be, as a lack of network documentation meant we had both inherited an opaque environment. Nor did we know exactly where in the network a data loss or hardware failure incident would result in catastrophic business impact.

So, we faced a dilemma: do we dive in and start patching and replacing hardware, or take the time to conduct a comprehensive risk assessment? Each had their own appeal and challenges.

A comprehensive risk assessment would take time to properly understand the core business processes, user requirements, security control efficacy, and remediation capabilities. Time was something we did not have to spare however, as any day a known infrastructure issue could cause a major incident.

On the other hand, simply diving in was not without significant risk. Patching infrastructure without knowing its functionality could cause unexpected interruption to core business functions, as could any hasty configuration changes. Most concerningly, without understanding the underlying risk, any investment may ultimately be squandered if it came to pass that we were addressing issues which turned out to not be of greatest risk to the business.

Whatever the approach, top management needed an update, the inevitable outlay for infrastructure upgrades would require a solid business case, and the Head of IT's concern had to be addressed. This cocktail of requirements led to me offering the following analogy:

The business is an unconscious patient who has just entered the Emergency Room. We can see injuries that need immediate attention, but we do not know what caused them. If we only patch the wounds without diagnosis, we risk overlooking the underlying illness and need to repeat this all over again next week – or worse still, lose the patient. If we focus solely on diagnosis however, our patient may bleed out before we understand what caused those injuries in the first place.

Our task therefore required a seamless coordination between the doctors (security) and the nursing staff (IT). While the doctors commence root cause analysis to ensure the underlying illness (risks) can be identified and remedied, the nurses jump into action to ensure the visible injuries (infrastructure vulnerabilities) are addressed as quickly and effectively as possible.

Whether in the Security Operations Centre or the Emergency Room, communication is always critical. A high-level risk assessment was drawn up, and business impact assessments were undertaken for the systems in greatest need of treatment. Senior management was engaged to understand the situation, as well as likely expenditure for medium- and long-term remediation. Throughout the process, the two teams were in constant communication with one another: have rollback plans been tested? Have the users been notified? Have the configuration changes modified other risks, and if so, has this impacted the efficacy of other proposed remediation activities?

A balance must always be struck between the tactical and strategic. Neither can be neglected if timely, effective, and cost-efficient risk mitigation is the goal. Sometimes a simple analogy can go a long way in bridging the gap between the business and its technical functions, and in this instance, I am proud to say the patient made a full recovery. Whether in medicine or IT, ongoing monitoring and treatment remains key to the success of any treatment plan. Once the dust has settled, and business as usual resumes, all organisations must keep this in mind when navigating the endless minefield that is enterprise security. ▲



VIRTUAL AND IN-PERSON

INDUSTRY NETWORKING OPPORTUNITIES

Don't miss the chance to hear from industry experts and connect with security and technology professionals around the globe

PROFESSIONALS

BUSINESSES



SEARCH THE MARKETPLACE

ALL EVENTS COURSES WEBINARS REPORTS BOOKS WHITEPAPERS SOLUTIONS

SEARCH BY: NAME, TOPIC, COUNTRY, MONTH, ORGANISER, TYPE

SEARCH

www.mysecuritymarketplace.com





18th June 2021, 7am Singapore/ [-1 day] 7pm Montreal

Episode 270 – WORKING IN PARTNERSHIP WITH LAW ENFORCEMENT – ESET CYBERCRIME INVESTIGATIONS

In this podcast with Jane Lo, Singapore Correspondent, Alexis takes the audience behind the scenes of real cybercrime investigations ESET has been involved in. By going over success stories such as the Andromeda and Operation Windigo busts that brought down multi-million dollar criminal networks, Alexis helps shed some light on how private security companies partnerships with law enforcement agencies work.

Working in partnership with law enforcement – ESET cybercrime investigations

Alexis Dorais-Joncas

Head of R&D ESET
Montreal Branch





Recorded 26th May 2021 Singapore 5.15pm/
Germany 11.15am.

Episode 266 – DISRUPTING DANGEROUS MALWARE – MICROSOFT’S LEGAL ACTION TO DISRUPT TRICKBOT

In this podcast, Mary Jo gave highlights of Microsoft’s legal action in October 2020 to disrupt Trickbot, one of the world’s most pervasive malware families which was behind attacks launched by ransomware groups such as Ryuk. to signal the locations of the Command and Control (C&C) Infrastructure.

Disrupting dangerous malware – Microsoft’s legal action to disrupt trickbot

Mary Jo Schrade

Assistant General Counsel and Regional Lead
for Microsoft’s Digital Crimes Unit (DCU) Asia





The emerging role of bitcoin in spreading malware

Professor Dr. Christian Doerr

Professor of Cyber Security and Enterprise Security, Director of the Cyber Threat Intelligence Lab, Germany

Recorded 26th May 2021 Singapore 5.15pm/
Germany 11.15am.

Episode 268 – THE EMERGING ROLE OF BITCOIN IN SPREADING MALWARE

In this podcast, Professor Doerr discussed the investigation by his team into the emerging role of Bitcoin in powering advance malware, and shared insights into threat actors' use of Bitcoin blockchain to signal the locations of the Command and Control (C&C) Infrastructure.





Streamed May 28, 2021

Episode 264 – STATE OF CYBERSECURITY 2021: GLOBAL UPDATE ON WORKFORCE EFFORTS, RESOURCES AND BUDGETS

We speak with ISACA on their recent annual research report, The State of Cybersecurity. We're joined by Jenai Marinkovic, vCTO/CISO at Tiro Security and advisory board member at Beyond, and member of ISACA's Emerging Trends Working Group and Jonathan Brandt, ISACA Information Security Professional Practices Lead.(C&C) Infrastructure.

State of Cybersecurity 2021: Global update on workforce efforts, resources and budgets

Jenai Marinkovic & Jon Bradt

ISACA





Deepfakes, shallowfakes & cheapfakes – seeing is believing

Dr. Nasir Memon

Vice Dean for Academics and Student Affairs and a Professor of Computer Science and Engineering at the New York University (NYU) Tandon School of Engineering.



Recorded Singapore 17th March 2021 7.15am
/ New York 16th March 2021 7.15pm

Episode 255 – DEEPFAKES, SHALLOWFAKES & CHEAPFAKES – SEEING IS BELIEVING

In this podcast, Dr Lin discussed cyber influence and the modern phenomenon of misinformation, offering historical perspectives and insights into how technological tools are leveraged in today's misinformation campaigns.





The video player shows a split-screen interview. On the left, a graphic for 'MySec TV IRAP Protected' features the text '6clicks for Government' and 'Anthony Stevens Founder & CEO' above the '6clicks' logo. On the right, Anthony Stevens is shown in a video call window. The background of the video player features a blue and white fighter jet flying over a globe. A large white play button is centered over the video. At the bottom of the player, a caption reads 'Anthony Stevens Founder & CEO, 6clicks'. The video progress bar shows 2:24 / 14:31.

Interview with **Anthony Stevens** Founder & CEO of 6clicks



We speak with Anthony Stevens, Founder & CEO of 6clicks.

6clicks is making a big announcement, backed by Microsoft, where the company is launching an IRAP PROTECTED assessed instance of their platform for defence and government market – 6clicks for Government.

Following their recent \$5.5M capital raise, the company also announced this week that Matt Gyde, former CEO of billion-dollar global technology services company NTT Security has joined the team as Non-Executive Director.

Matt's career in IT security spans more than 20 years, with a rich history including high-level roles with Dimension Data and Datacraft-Asia, providing him a deep understanding of how security platforms should be implemented and managed to ensure clients' business outcomes are achieved while ensuring their risk is minimised.

This is our second interview with Anthony and looking forward to following the company's rise. Stay tuned!



NEW ENTRY TO AUST & NZ CYBERSECURITY MARKET

Expands with Application-aware workload protection offering.

Rob Nobile

REGIONAL SALES
DIRECTOR - ANZ



July 12, 2021

Episode 272 – Virsec enters ANZ Cybersecurity Market

Virsec is a San Jose, USA based company which provides an application-aware workload protection platform. Virsec is gearing up for rapid growth in the ANZ region with Rob recently joining the team.





Where autism offers a competitive advantage

By
Dr David Cook

Cyber-attacks can come from anywhere, and it seems that cyber warriors can also emerge from unexpected quarters. The newest weapon in organisations' defences turns out to be people on the autism spectrum, whose special talents make them ideally suited to the role of cyber warrior.

The characteristics that distinguish people on the spectrum include scrupulous honesty, a passion for problem-solving, superior talent at spotting patterns, and exceptional focus on pursuing anomalies until they are resolved. They are relentless in detecting incongruities and repairing code, refusing to stop until a solution is found.

As a result of their pursuit of logical outcomes, people with high-functioning autism spectrum disorder (ASD) tend to demonstrate outstanding dedication to software objectives and are very unlikely to misrepresent or distort the truth. These gifts also make them highly suited to software testing, another key area of the IT industry.

Neurodiversity is fast becoming a specialised category of ICT employment with a much higher rating in terms of expected benefits and efficiencies, despite past stereotypes that pigeon-holed ASD candidates as too difficult. The

emerging view is now more accepting towards quirks and peculiarities, and those with high functioning ASD are receiving greater attention than before. The new language is not so much about "challenges" and "difficulties". Clever human resources planners now talk about the new "different" in ICT employment opportunities.

Roles connected with IT, assurance and data analytics may appeal to people on the spectrum because they feel more comfortable interacting with machines than dealing with people, especially face to face. This can be a welcome relief for this group of people, who may have difficulties dealing with the unwritten rules of personal discussions and social structures.

As well, interactions within the computing domain usually require logical engagement with systems, programs and platforms, and provide specific work objectives, clear guidelines and relatively rigid protocols for completing tasks, which suit many people on the spectrum.

As Harvard Business Review reports, savvy organisations are catching on to the fact that people with high-functioning ASD offer a competitive advantage. The federal Department of Human Services has found that

According to the Australian Bureau of Statistics, there were 205,200 Australians with ASD in 2018. Yet only about 40 per cent of working-age people with ASD participated in the workforce in 2015.

Statistics, there were 205,200 Australians with ASD in 2018. Yet only about 40 per cent of working-age people with ASD participated in the workforce in 2015.

The reasons for this may have nothing to do with ability. Research by autism advocacy group Amaze has found that about one-third of people on the autism spectrum are unable to attend job interviews due to anxiety. Even if they are able to attend, many struggle in interviews because they don't have the communication skills needed to sell themselves to potential employers.

This is more than a needless waste of human potential. For corporations, it is a missed opportunity with serious – and expensive – consequences. The growing threat of cyberattacks, cyber espionage and even cyberterrorism means that organisations must constantly upgrade their defences and if they are attacked, they may have to spend huge amounts of money to cyber criminals demanding ransoms or upgrading their systems.

This is where people on the spectrum come in to their own. As a result, the IT industry is an exception to the pattern of poor employment outcomes. People with ASD working in IT find jobs more often, enjoy higher levels of job satisfaction and stay in their roles for long periods of time, offering employers a loyal and dependable workforce in a rapidly shifting industry.

The rise of online learning is also proving to be a boon for both workers with ASD and their employers. People on the spectrum engage successfully with this learning mode because it removes the anxiety often associated with face-to-face interactions and provides certainty and clarity around tasks.

As a result, people with ASD are more likely to actively engage with online courses such as a Master of Cyber Security or Master of Computer Science than with in-person alternatives. Such high-level qualifications can be hugely beneficial, as they greatly expand opportunities both for finding and keeping a job and for enjoying the satisfaction and potentially higher salary that come with it.

The message is clear: when organisations hire people on the autism spectrum, the benefits are mutual. The solution is also within easy reach: more and more corporations can share their experiences on how to implement a neurodiversity program. In the current environment of labour shortages and skill deficits, neither employers nor employees can afford to let so much potential go untapped.

Dr David Cook is a lecturer within the School of Science and unit coordinator of the Information Warfare unit for ECU's Accelerated Online Master of Cyber Security, a member of the Australian Centre for Cyber Security Excellence (ACCSE), and a Fellow of the Australian Computer Society. ▲

people with autism in software-testing roles are 30 per cent more productive than their neurotypical colleagues.

Some trailblazers are implementing neurodiversity programs with the specific goal of attracting people with on the spectrum. Both the Department of Foreign Affairs and Trade and the Department of Defence have introduced neurodiversity programs in the technology field. ANZ Bank has a "Spectrum Program", and comparable programs have been established at both the Commonwealth Bank and Westpac.

National Australia Bank too partnered with DXC Technology's Dandelion program in 2019 to establish a program called Neurodiversity at NAB. It reports that the results were "outstanding", with the bank finding that after three months the DXC Dandelion team's productivity was 26 per cent higher than the existing team's output. One ASD trainee at NAB scripted a new program within their first couple of weeks that "effectively saved the bank hundreds of hours".

Yet much more can be done by the corporate world to take advantage of the talents people with autism spectrum disorder have to offer. According to the Australian Bureau of

e-Waste - The security blind spot

By
Stuart Dahlenburg,
VP, General Manager,
Information Management
and Digital Services, Iron
Mountain, ANZ

The emergence of the COVID-19 pandemic last year forced businesses and their employees to radically reimagine their day-to-day life. Unprecedented restrictions on travel, physical interactions, and changes in consumer behaviour forced companies to change the way they operate and consumers the way they engage with businesses.

Businesses and people were forced to adopt digital solutions overnight. In some cases, banks, grocery stores and retail brands were rolling out technology plans that would ordinarily have taken years to complete, in a matter of weeks.

However, new remote working models can bring a number of potential risks from a data protection and privacy perspective. Cloud technology, which allowed workers to be productive by providing access to company documents outside of the office environment, was critical in ensuring businesses could continue to operate.

At the same time, it led employees to leverage unfamiliar tools to share documents, leaving sensitive data sitting on a laptop or mobile device which could then be stolen or damaged, or in the cloud, where it's at risk of being stolen through a cyber attack.

According to the ACSC, there were around 60,000 reports from individuals and businesses reporting instances of cybercrime in 2020, however the actual number of incidents is likely to be much higher.

Similarly, a report by BDO says data breaches caused by malicious hacking increased by 91 percent in 2020, likely caused by IT support challenges during remote working, and the lack of preparedness for increased cyber attacks during the pandemic.

With an increasingly dispersed workforce, security has never been more crucial to keep a business running. Aside from keeping precious intellectual property safe, ultimately security reduces liabilities, insurance, compensation and other social security expenses to be paid by the company to the stakeholders.

COVID-19 has forced the hand of businesses in several sectors by requiring them to confront their digital preparedness in tackling cyber threats head on.

Cybersecurity must no longer just be in the confines of IT – it requires a comprehensive strategy that extends to all aspects of the business, from the customer service call centre to the boardroom.

Organisations need confidence that fundamentals are in place to ensure they remain protected from this increasingly prevalent risk. Businesses must invest in physical security, follow best practice and take a holistic approach.

Cybersecurity depends greatly on physical security

While it's known that the cost of successful digital attacks keeps rising, one element of security that is often overlooked is that of physical items, the loss or breaching of which can be just as harmful if left unchecked.

For example, attackers who gain physical access to a computer can almost always take advantage of that access to further their efforts.

Laptops, USB drives, tablets, flash drives and smartphones all have the ability to store sensitive data that can be lost or stolen. And in a world of hybrid-

working with many employees working remotely and taking equipment from the office to their homes, organisations increasingly have the task of safeguarding data, equipment, people, facilities, systems, and company assets.

Companies spend substantial amounts of dollars on physical security, keeping the public at large out of their headquarters, limiting access to sensitive areas, or workers from mission-critical areas such as the server room. The same concern must be shared when regarding discarded equipment.

Casually discarding an old computer and e-waste in the bin is just as risky as throwing an individual's passport on to the street.

One company that experienced the negative side of unsecured waste destruction was the Idaho Power Company in 2006, which disposed of company hard drives without wiping them clean and later found out that sensitive corporate data had ended up on eBay, where hundreds of its old hard drives were being sold online. Contained on those hard drives were confidential employee information and proprietary memos.

In the information age, every piece of data is valuable. Just because something seems to be no longer of use, it doesn't mean it wouldn't be of use to someone else. Bad actors are going to greater lengths to get their hands on anything and everything that could lead them to a payout, from former customer credit card numbers to 10-year-old trade secrets.

Back to basics: Best practice of destruction

At the same time businesses are facing the need for increased security of physical and digital data, concerns about the damaging effects of climate change are also mounting with businesses across Australia, big and small, innovating to reduce their environmental impact.

Yet few are harnessing the full value or understanding the significant relationship between strategic information lifecycle management and waste reduction, energy efficiency, and environmental responsibility initiatives.

This is particularly crucial for big tech organisations that have a large output of e-waste, as

Australia's e-waste is currently exported offshore, and destroyed in unsafe ways that often don't securely destroy data properly, and is harmful to the environment. This poor management of e-waste disposal can be detrimental to any business in regard to hefty fines, lawsuits or even imprisonment.

However, proactive destruction procedures can benefit businesses in solving issues around security and sustainability, at the same time.

In today's world, hardware recycling and disposition must meet businesses' disposal needs while maximising retired asset value in a safe, efficient and environmentally friendly manner.

Benefits include leaving a positive impact on the environment, which, in turn, maximises good stakeholder management, as well as ensuring that data is being securely and responsibly destroyed, leaving no risk of security threats.

A hybrid working model brings with it a number of potential risks from a data protection and privacy perspective. However, organisations that identify and implement a holistic approach to physical and digital data security will be better placed to react and defend against cyber threats.

Rather than putting the environment and business at risk by irresponsibly discarding e-waste, companies can take the lead by putting into practice more-sustainable methods, including instilling e-cycling within the company culture, setting protective procedures in place, considering the options that work best for their business and partnering with a secure e-waste destructor.

By implementing simple processes, businesses can give themselves the greatest chance of successfully managing the disposal of their digital assets in ways that minimise the threat of e-waste to the environment and to organisational reputation.

A holistic approach

E-waste management will continue to be a challenge for Australian businesses as CEOs continue to embrace digital transformation.

Companies cannot afford to hold on to every file indefinitely, whether it's physical or digital, that takes up valuable resources.

Organisations with aligned cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified security policies across security divisions.

The benefits include an integrated threat management strategy that reflects an in-depth understanding of the impacts to interconnected cyber-physical infrastructure.

A hybrid working model brings with it a number of potential risks from a data protection and privacy perspective. However, organisations that identify and implement a holistic approach to physical and digital data security will be better placed to react and defend against cyber threats.

Where, typically, physical security and digital security were once entirely separate realms, they are slowly becoming more intertwined.

As rapidly evolving technology increasingly links physical and cyber assets, spanning sectors from energy and transportation to agriculture and healthcare, the benefits of converged security functions outweigh the challenges of organisational change efforts and enable a flexible, sustainable strategy anchored by shared security practices and goals. ▲



Graeme Reardon
Managing Director of D-Link Australia
and New Zealand.

D-Link

How to get the most from your Smart Home.

www.mysmarttech.tv

Interview with **Graeme Reardon** Managing Director of D-Link Australia and New Zealand.

D-Link

Join us as we chat to Graeme Reardon from D-Link on how to get the most from your Smart Home.

For over 32 years and in more than 100 countries across the world, D-Link is connecting millions of people in their daily lives. From powering hospital networks so that life-saving operations can be carried out, to simply running your Wi-Fi network at home so you can enjoy streaming the latest movies to your Smart TV or tablet, D-Link solutions are a part of everyday life.

Graeme Reardon is the Managing Director of D-Link Australia and New Zealand and in addition to D-Link, has had over 20 years' experience working with several other major networking brands including Cisco's consumer and SMB businesses.

With a borderline obsessive passion for all things IT-related, he presents a broad spectrum of insights for home consumers and businesses alike.

CYBER RISK LEADERS

“This large and diverse group paints an interesting narrative of the state of play in enterprise cyber risk.”

Foreword by M.K. Palmore, Retired FBI Assistant Special Agent in Charge, FBI San Francisco Cyber Branch



“With experience and insight, Shamane has written a really useful book for existing and aspiring CISOs.

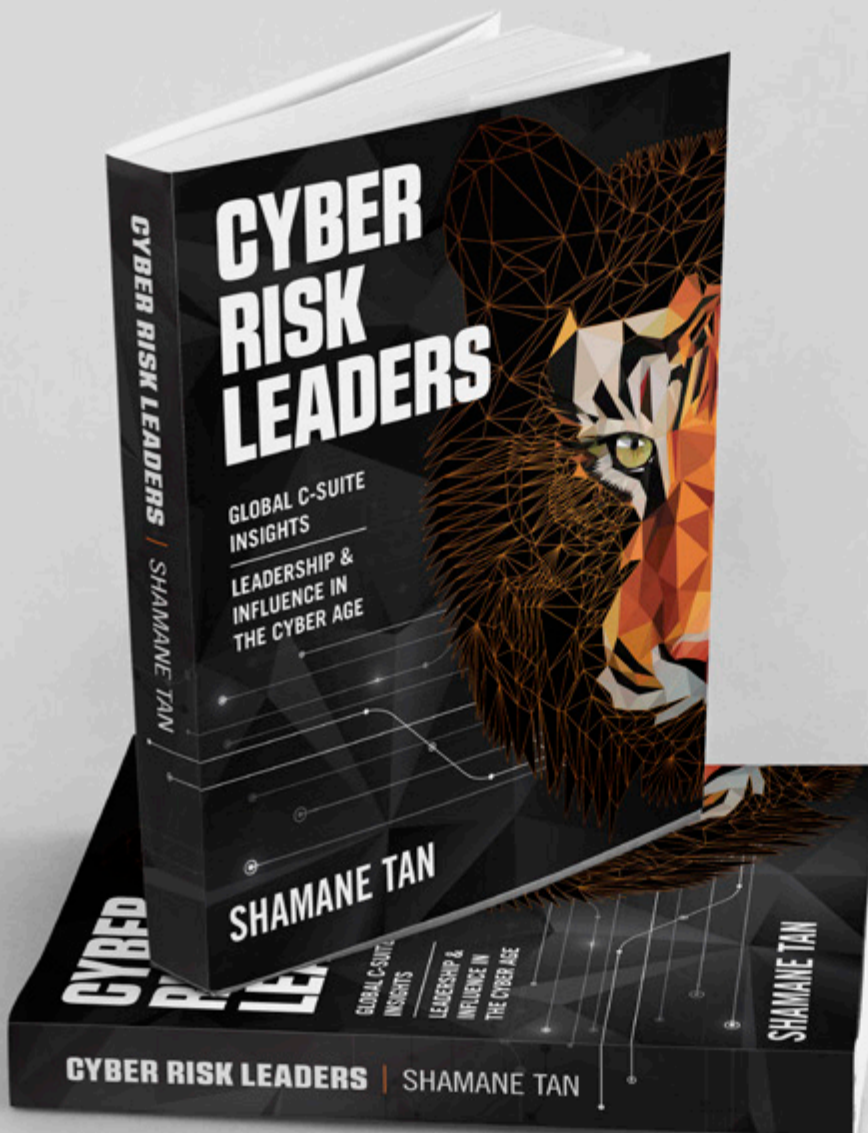
I loved her unique voice, highly readable style, and wholeheartedly recommend this book.”

CEO, Cyber Security Capital (UK)



“She has explored many topics long considered on the fringe of traditional security with great storytelling and insights from industry leaders.”

CISO, Telstra APAC



ABOUT THE AUTHOR

SHAMANE TAN advises C-Suite on uplifting their cyber risk and corporate security posture.

She is an international speaker and Founder of Cyber Risk Meetups, a platform for security executives to share innovative insights and war stories.

GET YOUR COPY HERE!

Proudly Published by



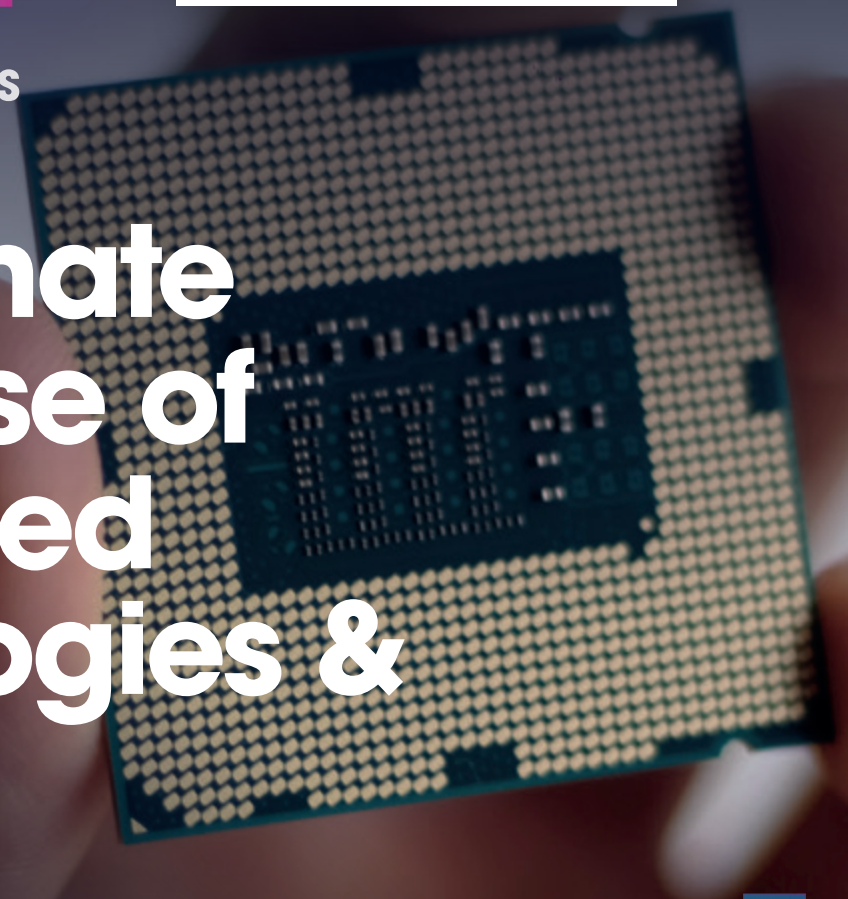


Embedded Technology Convention **2022**

SINGAPORE • LAS VEGAS

**19-20
January
2022**
SINGAPORE EXPO
SINGAPORE

**8-9
June
2022**
LVCC
LAS VEGAS, USA



The Ultimate Showcase of Embedded Technologies & Systems

The Embedded Technology Convention is the central hub to discover the latest technological innovations and trends, expand your industry knowledge and extend your global professional network.

WANT TO KNOW MORE?

For **full information about exhibiting**, a full brochure and costs please contact:

ASIA

Carson Liu

Event Director

Tel US: +1 914 639 6564

Tel UK: +44 203 026 3765

Email: carson.liu@prysmgroup.com

USA

David Miller

Event Director

Tel US: +1 702 707 7627

Tel UK: +44 203 026 3765

Email: david.miller@prysmgroup.com

www.EmbeddedTechConventionAsia.com | www.EmbeddedTechConvention.com



RESOURCES - PRODUCTS - EVENTS

EXCLUSIVE SECURITY & TECHNOLOGY OFFERINGS

Register as an industry professional to gain access to our exclusive content or promote your brand to feature your content to a global market across all our channels.

PROFESSIONALS

BUSINESSES

SEARCH THE MARKETPLACE

ALL EVENTS COURSES WEBINARS REPORTS BOOKS WHITEPAPERS SOLUTIONS

SEARCH BY: NAME, TOPIC, COUNTRY, MONTH, ORGANISER, TYPE

SEARCH

www.mysecuritymarketplace.com

THE HUB

ENGAGE WITH LEADING INDUSTRY BRANDS

Access exclusive and curated content from the startups to the top brands: Products, resources, events, webinars, updates, interviews & podcasts.

PROFESSIONALS

BUSINESSES



THE HUB
Everything about your favorite companies in one convenient place.

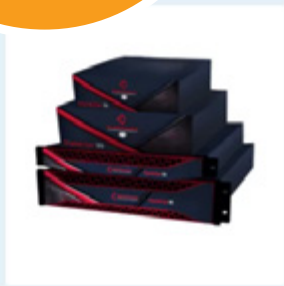
CHECK OUT THE LATEST PRODUCTS



Access Control, Network security
Enable Zero Trust with RSA



Access Control
YubiKey 5C NFC



UTM
10% Discount to Marketplace Users
Crystal Eye UTM Gateway Series 30+



Endpoint Protection
Malwarebytes Endpoint Detection and Response