

CYBER RISK

LEADERS

THE MAGAZINE FOR SECURITY & TECHNOLOGY PROFESSIONALS | www.cyberriskleaders.com

Issue 2, 2020

Top trends that should inform your COVID-19 security posture

Does COVID-19 signal the end for fingerprint recognition?

Invest in intelligence now to prepare Australia's utilities for the future

Coronavirus victims of a different nature: The targets of COVID-19 cyberthreats

Critical-infrastructure attack attempted against Israeli water supply

The law on cyber bullying and trolling

RESPONSE & RECOVERY

CYBER + COVID-19



**Cyber Security
Weekly Podcast
highlights**

PLUS

**NEW BOOK
REVIEW**

WE'RE BRINGING THE BEST IN CYBERSECURITY RIGHT TO YOU.



This year, RSA Conference Asia Pacific & Japan will be a free virtual learning experience. This is an incredible opportunity to engage with a global cybersecurity community right from your home or wherever you might be.

RSAC 2020 APJ will be packed with sessions and interactive activities designed to expand your knowledge, including:

- Over 60 timely sessions, streamed live during Singapore business hours, or available later on demand.
- Inspiring and forward-looking keynotes from RSA's Rohit Ghai, Microsoft's Ann Johnson, and author, performer and activist George Takei, who will be a special guest on The Hugh Thompson Show.
- Three different Capture the Flag experiences.
- Engaging networking opportunities including Ask the Expert Roundtables.

Secure your spot today—for free—and join thousands of your peers for three days of learning and networking.

Register today at

www.rsaconference.com/mysecuritymedia-apj20

#RSAC



FOLLOW US



EVENTS

Search and find all upcoming featured security events



India's Reach Series
Aerospace, Defence & Security Market Trends
Opportunities for Australia and ASEAN region

Tue, Jun 23 **Free Online Event**

India's Security Sector Market Trends – Opportunities for Australia & ASEAN Region



Fri, Jun 26 **Online Event**

Cyber Risk Meetup AUSTRALIA Capture the Flag 'Cyber Range'



Wed, Jul 01 **Free Online Event**

Australia & Israel Counterpart Series - National Cybersecurity Strategy Insights



Fri, Jul 10 **Online Event**

Mega C-Suite Series Episode 7: Meet the World's 1st CISO



INDIA'S REACH SERIES

Aerospace, Defence & Security Market Trends & Opportunities for the Australia and ASEAN region.



Plus many more!
www.mysecuritymarketplace.com

Contents

CYBER RISK LEADERS

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 Cyber Risk Leaders 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

AUSTRALIAN
CYBERSECURITY
MAGAZINE

www.australiancybersecuritymagazine.com.au


www.mysecuritymarketplace.com

AUSTRALIAN
SECURITY
MAGAZINE
www.australiansecuritymagazine.com.au


www.aseantechsec.com


www.asiapacificsecuritymagazine.com


www.drasticnews.com


www.chiefit.me


Entertain | Engage | Educate
www.youtube.com/user/MySecurityAustralia

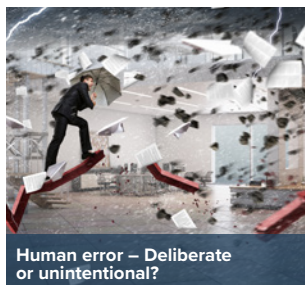

www.cctvbuyersguide.com



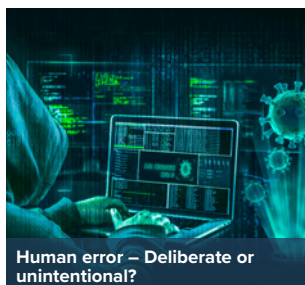
Energy security: Keeping the electrons flowing



The golden tax department and the emergence of GoldenSpy malware.



Human error – Deliberate or unintentional?



Human error – Deliberate or unintentional?



Why domestic violence is a workplace issue.

Editor's Desk

Shaping the future of data centres	5
Submarine Cable Network: The Global Sovereign Asset	8
Energy security: Keeping the electrons flowing	10
Critical-infrastructure attack attempted against Israeli water supply.	12
The golden tax department and the emergence of GoldenSpy malware	16
Getting serious about security assurance	18
Invest in intelligence now to prepare Australia's utilities for the future.	20
Siloed response to cyber threats failing to protect Australian organisations.	24
Human error – Deliberate or unintentional?	28
Top trends that should inform your COVID-19 security posture	30
How to reduce work from home risks in a post-COVID world	36
Does COVID-19 signal the end for fingerprint recognition?	38
Coronavirus victims of a different nature: The targets of COVID-19 cyberthreats	40
The law on cyber bullying and trolling	42
Why domestic violence is a workplace issue.	46
Editor's Book review	48
	50



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



John Young



Dave Weinstein



Geoff Schomburgk



Nick de Bont



Brenda van Rensburg

Also with:
Iain **Strutt**
Brian **Hussey**
Codee **Ludbey**
Ray **Griffiths**,
Mark **Sayer**,
Visahl **Samson**
David **Selvam**,
Michael **Warnock**

“The prospect of high-intensity military conflict in the Indo-Pacific is less remote...including high-intensity military conflict between the United States and China.”

AUSTRALIAN 2020 DEFENCE STRATEGIC UPDATE – July 1, 2020

In June, the cybersecurity ‘situation’ observed across western liberal democracies was thrust forward in Australia to be on the national centre stage. Much like Australia’s early call for an independent international inquiry into the origin and cause of the COVID-19 pandemic, on June 19, Australian Prime Minister Scott Morrison openly declared Australia was being targeted by a sophisticated, state-based, cyber actor across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers, and operators of other critical infrastructure. Coinciding with these attacks, other countries were also reporting significant cyber-attack activity. Naturally, China is implicated. China is acting widely belligerent, whilst enacting further control over Hong Kong – taking one big step closer to Taiwan. Releasing a massive, asymmetric cyber-attack against Australia and other countries sits alongside China’s trade and diplomatic disputes with the US, UK, Canada and India.

It is well accepted that major power competition has intensified and accelerated as a result of the COVID-19 pandemic and the prospect of ‘high-intensity conflict’ in the Indo-Pacific is increasingly likely. For historical context and what the status of the region was as the pandemic unfolded, we include in this edition my book review and podcast interview with Professor Rory Medcalf, author of *‘Contest for the Indo-Pacific – Why China Won’t Map the Future’*. China is certainly influencing it!

On June 30 Australia announced the country’s largest ever investment in cyber security, with \$1.35 billion over the next decade, referred to as the Cyber Enhanced Situational Awareness and Response (CESAR) package to enhance the cyber security capabilities of the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre. The next day, Australia went further and released the *2020 Defence*

Strategic Update and *2020 Force Structure Plan*, acknowledging while the long-term impacts of the pandemic are not yet clear, it has deeply altered the economic trajectory of the world, with implications for national security. Stating “the conduct of ‘grey-zone’ activities are broadly being applied with military and non-military forms of assertiveness and coercion being used to achieve national strategic goals but without provoking conflict. In the Indo-Pacific, these activities have ranged from militarisation of the South China Sea to active interference, disinformation campaigns and economic coercion.”

As a middle-power, Australia is at the centre of a dynamic strategic environment and expanding cyber capabilities, and the willingness of countries like China and non-state actors to use them, make for a complex strategic ‘situation’. At our partnered Webinar on July 1 this was eloquently summed up by Mr. Yigal Unna, Director General of the Israel National Cyber Directorate - “the attack surface is on steroids.”

In this edition, we cover all aspects of security technology and critical infrastructure protection, starting with what is the central element of the internet - data centres. The world’s data is set to grow to 175 zettabytes by 2025 and John Young examines how data centre engineers need to keep pace with an ongoing data evolution. Connecting data centres is the cables and we get insights into the global submarine cable networks, a timely article with the recent completion of the Japan-Guam-Australia North Cable System, approximately 2,700 kilometres in length and a design capacity of 30 terabits per second. Then next, we have Iain Strutt’s consideration to the power source and related energy security issues. These three articles represented the fundamental infrastructure of the Internet and we thank these contributors for providing an excellent base for the remainder of this edition.

We maintain coverage of the COVID-19 pandemic. Adapting your respective security posture is essential in a rapidly changing and unpredictable environment and there has been immediate impacts on security technology, including the potential disruption of fingerprint biometrics. With COVID-19 there was, and continues to be, an influx of adapted cyber-attacks, with some reports that coronavirus-related phishing attacks went up 667%, and every single country around the globe has now been hit with at least one phishing attack related to the pandemic. Longer term, we will also see an increased focus on contactless biometrics as part of multifactor authentication and other security systems such as entry management. AI technologies and drone surveillance is being developed and rapidly deployed to help monitor the spread of the virus. Thermal cameras are being installed in facilities and workplaces and facial recognition will still work even when a person is wearing a mask. Contactless fingerprint recognition, iris scanning and face detection will become the norm for biometrics.

So, when you finally get to leave your home and head to work or enter a public place, likely it will be best to smile, beneath the mask – because you’ll be on camera – thermal included and may even have a drone or robot pass you by with a public health announcement – because this is 2020! And we’re just half way through it.

On that note, as always, there is so much more to touch on and we trust you will enjoy

this edition of *Cyber Risk Leaders*. Enjoy the read!



Chris Cubbage CPP, CISA, GAICD
Executive Editor

CYBER RISK

LEADERS



**App now
available
on iTunes &**

**DOWNLOAD
NOW!**





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. COMING SOON

OUR CHANNELS





Shaping the future of data centres

A survey of data centres by Forbes Insights and Vertiv indicates that not all companies are prepared for our evolving data ecosystem. Just 29 per cent of the 150 business leaders and data centre engineers surveyed say that their facilities are meeting current needs, with only six per cent feeling that data centres were updated in time to meet future demands. The deluge of data that businesses rely on isn't going to hold its floodgates any time soon, so how can we futureproof our data centres? Here John Young, APAC director at industrial equipment supplier EU Automation, investigates.



By
John Young

With the world's data set to grow to 175 zettabytes by 2025, data centres will continue to play a central role in the ingestion, computing, storage and management of our information. In the context of this growth, Forbes Insights' and Vertiv's survey data is worrying — how can data centre engineers keep pace with our data evolution?

Leaner and greener

Current data centres aren't renowned for their energy efficiency. Electricity consumption from China's data centre industry is on track to jump by two thirds over the next five years. By 2023, the sector is projected to consume 267 terawatt hours (TWh) of electricity — more than Australia's total 2018 electricity consumption.

Much of the energy data centres require comes from the need to keep their processors cool, which often uses ambient air-cooling with cold water-recirculation coolers. If data centres are cooled inefficiently, it can lead to high

operational costs and unnecessary spending.

Adopting improved cooling methods is therefore central to securing a bright future for data centres. For example, engineers can consider water cooling methods, which typically cost less and require fewer parts, to remove heat from the computer room air handler (CRAH). Glycol is another effective cooling option that uses a mixture of water and ethylene glycol, similar to anti-freeze for cars, to collect heat from the refrigerant and transport it away from the IT environment. Glycol pipes can run much longer distances than refrigerant lines and can service several CRAC units from one dry cooler and pump package.

Another cooling option is an indirect air evaporative cooling system. This method uses outdoor air to indirectly cool data centre air when the temperature outside the centre is lower than the temperature set point of the IT inlet air. While this significantly improves energy savings, it may be difficult to retrofit this option onto an existing data centre. When selecting the most suitable cooling method, engineers must consider the location and current state of



Almost a quarter of executives surveyed for Vertiv's report revealed that over 50 per cent or more of their data centres will be self-configuring by 2025 — and about one third say that more than half of their data centres will be self-healing by then.

workload to a different cloud provider.

Inside data centres, artificial intelligence (AI) technologies such as deep learning, statistical learning and optimisation algorithms model complex components and operational models. Combined with sensing technologies and automation systems, the goal is to achieve more efficient and reliable data centre infrastructure that operates at a lower cost.

So, it could be that, by collecting data on failure rates in normal operations, self-healing infrastructure can report on failing components such as hard drives or solid state drives (SSDs), or low probability events such as battery defects. This data allows the centre's operator to inform and prepare customers in advance of potential risks. The ability to recognise and report on current and potential failures could also alert operators to any hardware faults, allowing them to order automation parts from a reliable supplier without causing disruption to the data centre's ordinary operations.

On the edge

Preparing our data centres for the future involves looking at the locations of the data centres, as well as at technology. To meet growing demands for data storage and management, small distributed data centres — or edge data centres — are being deployed to enable hyper-local storage and processing capacity at the edge of the network.

Edge computing technology involves placing resources closer to the origins of data — such as motors, pumps or generators — to reduce the need to transfer data back and forth between centralised computing systems, or the cloud. Edge computing is already taking the strain from data centres for a number of consumer applications. Tesla cars have onboard computers that allow for almost real-time processing for data collected by the vehicle's dozens of peripheral sensors, providing the ability to make timely, autonomous driving decisions.

As an industry, we need far more than six per cent of data centre engineers to feel that their facilities are future proof. By looking to new approaches in cooling, configuration and location, data centre engineers can better prepare for the ever increasing flood of data the future will bring. ▲

their centre, as well as their plans for future growth and development.

Self-care

Almost a quarter of executives surveyed for Vertiv's report revealed that over 50 per cent or more of their data centres will be self-configuring by 2025 — and about one third say that more than half of their data centres will be self-healing by then.

Self-configuring or self-healing devices incorporate infrastructure that allows for real-time maintenance, configuration and issue resolution, enabling an adaptable and dynamic working process. Much like the autonomic nervous system of the human body, a self-healing computing infrastructure is capable of constantly optimising its status and automatically adapting itself to changing conditions. While self-healing systems can detect and resolve problems automatically, self-optimisation improves performance or reduces costs by, for example, routing a

Submarine Cable Network: The Global Sovereign Asset

By
Abhilash Halappanavar
Visvesvaraya
Technological University, India

The world in the last few years has come out of age with external policies impacting the domestic functioning of any major country. Similarly, since the days of the U.S-Russia cold war securing strategic assets across the world has been the utmost priority for countries wanting to gain advantage or showcase their prowess in consolidating their strengths. Be it establishing of overseas military and air force bases by the U.S or China's efforts to secure operational ownership of water ports in foreign countries, all deal with holding leverage in negotiating foreign relations to their advantage in economic and military interests. Similarly, the Submarine Communication Cables are the new strategic assets in the oceans that could be the flashpoint for geopolitical tensions. The submarine cables are laid on the sea and ocean bed between land terminals to carry telecommunication signals across the lengths of ocean and sea.

The global digital connectivity relies upon many fibre optic cables lying beneath the Atlantic, Pacific, and Indian Oceans. People generally believe that their international communications are carried via satellite links. The truth is that more than 99% of transcontinental Internet traffic goes through these connecting cables; these are the lifelines of any country's communication grid empowering its business and economic operations. The submarine cables are critical

technology infrastructure and any easy access to govern and manipulate these will virtually put a country in a driver's seat of technological superiority.

The entire submarine cable network is a state-of-the-art arrangement for faster communication under the Global Undersea Communications Cable Infrastructure. But this network has its weak points when they converge at specific zones. These are critical as any damage happening to these convergence points will have a huge outage and connectivity crisis across the globe. There are mainly three cable chokepoints, the first is in the Luzon Strait, the second in the Suez Canal-Red Sea-Mandab Strait passage, and the third is in the Strait of Malacca.

There are 18 international cables running east-west in the Strait of Luzon between Taiwan and the Philippines, communication lines between South-East Asia and the rest of the world rely on this path. Around 13 cables run through the Suez Canal-Red Sea-Mandab Strait passage between Yemen on the Arabian Peninsula, and Djibouti and Eritrea in the Horn of Africa thereby serving as a channel of a communication network between South Asia-East Africa & Europe. Lastly, numerous cables run through the Strait of Malacca between Singapore, Indonesia, and Malaysia into the South China Sea linking communication lines up to Japan.

Social media traffic, critical banking settlement networks



***'on 11th June 2020,
announced that it is connecting
the Philippines, China (Hong
Kong and Guangdong Province),
Japan, Singapore, Thailand, and
Vietnam via a 9,400-kilometer
submarine cable through the
South China Sea.'***

like SWIFT services and cloud server farms for data retrieval, etc all are made possible through these submarine cables. With enabling transactions and operations worth Trillions these are invaluable assets for the greater good of the world and development of countries. But with changing dynamics of geopolitics these assets can make or break an arrangement conducive to a country's economy and security. Especially in case of physical conflicts involving the military and also in situations like full out war any damage or cutting off this cable infrastructure could lead to near-total communications blackout that could adversely impact the involved parties of the conflict as well as the rest of the world. Hence the national security and digital safety of nations become sacrosanct towards securing the cables passing through the territorial waters of countries making use of the underwater cable services.


The vulnerability of major powers to cyber-attack makes the monitoring of the huge network of water cables a humongous task and also trust deficit between them only contributes to more tensions. For instance, the United States is concerned about Russia's proliferation capabilities in interrupting global internet traffic communication by cutting undersea cables in the event of a conflict with the West. Also, Russian submarines carrying out espionage activities on the U.S by tapping the cables and spying over

critical information concerning Washington's interest worry the security establishment of the U.S.

In addition to the rise of China in the Asia-Pacific communications arena, Chinese companies have rapidly expanded activity around submarine cables, both on the supplier side and the purchaser side, through Huawei Marine. The Chinese Exim Bank also has been proactive in financing several underwater cable projects in developing countries like Papua New Guinea. Huawei Marine, a collaboration between Huawei and a subsidiary of U.K. firm Global Marine Systems established in 2008, has been active around the world, particularly in Africa in laying of underwater cables. The very fact that China has built a Naval base in Djibouti indicates Chinas' plan to monetise its capability in monitoring internet traffic of North African countries and South Eastern Europe that passes through Suez Canal-Red Sea-Mandab Strait. China's investment in Cyber infrastructure here comes as the region surrounding Djibouti is just starting to come online, including some places that are entirely reliant on Djibouti as a transit point for data transmission and China could leverage this point of connectivity for espionage as well as safeguarding its vested interests in those regions.

Similar to other concerns around the rapidly expanding influence of Chinese firms globally, including Huawei's rise in next-generation 5G wireless networks, there are concerns that Huawei would be subject to pressure from the Chinese government to facilitate espionage or build in security vulnerabilities. The cable infrastructure investment also conveys China's broader strategy to expand its global influence. These factors have troubled U.S and few of its N.A.T.O allies as these put them in vulnerable situations that they have not been used to. It's not immediately clear if Chinese interest in submarine cables are purely for soft-power projections, or installations of powerful tools potentially leveraged for political abuse, undermining cybersecurity, and enabling espionage.

The uncertainty around the intentions and track records of countries like Russia and China give rise to policing of strategic interests in the marina. Asia Direct Cable (ADC) Consortium, on 11th June 2020, announced that it is connecting the Philippines, China (Hong Kong and Guangdong Province), Japan, Singapore, Thailand, and Vietnam via a 9,400-kilometer submarine cable through the South China sea. This would act as an enabler for the Chinese to patrol and justify their territorial claims in the disputed regions on grounds of protecting its vital interests at the same time misuse of this network by China would be a concern in the already troubled waters.

The submarine cables will play a great role as leverage to start or end conflicts. With the fifth-generation warfare gaining more attention from the world the road to supremacy in the cyberspace will go through these cables. Whichever country secures its cable interests will come out as a major power, as continuity and normalcy of the world rely upon these underwater networks. The potential in these cable networks to cripple any given country's operational capability will naturally gain more traction from its adversary. These assets naturally become strategic in nature for all major powers thereby giving the cables a tag of sovereignty. 

Energy security: Keeping the electrons flowing

By
Iain Strutt

About the Author

Iain has been involved in military, police and private security in Australia for over twenty five years, and has significant supervisory experience as a team leader & manager. As a licensed consultant he has acted for a diverse range of clients ranging in areas such as critical infrastructure, private & state facilities & film & television production. He has a particular interest in building management security systems & their operation, Health, Safety & Environment & cyber security

A brief look at energy security issues

The SARS-COV-2 virus (COVID-19) has brought working from home and distance learning into a clearer focus and has shown that certain workplaces can still be effective though the staff can be geographically dispersed. Applications such as Zoom and Microsoft Teams have highlighted that a steady stream of electrons can keep the national economy moving. But what if this flow is compromised? Put bluntly, turning off the lights in another country would reduce living standards to the nineteenth century if successful [1]. There needs to be an understanding of energy security and the need for greater safeguards.

Electricity production is designated critical infrastructure & has become a prime cyber warfare target. Offensive cyber-attacks offer nation states an avenue to augment their power without triggering an armed conflict. An offensive cyber operation is defined as being able to 'deny, disrupt,

degrade or destroy targeted computers, information systems or networks' and this also includes 'attacks that affect critical infrastructure, such as electricity networks'. Such examples include the Russian attack on the Ukrainian electricity grid twice & the high profile Stuxnet attack on the Iranian nuclear facility at Natanz.

Cyber war is a term everyone uses though there is no clear definition with any clear international rules to govern what is a proportional response in the physical world. In instances like those mentioned above, cyberattack is prioritized over cyber defence and with state-on-state 'big battalion' conflict becoming rarer, irregular warfare in this form is set to continue globally. The profile of a typical cyber-attacker falls into two categories; a nation state or its proxy, or a criminal enterprise such as a crime syndicate. Motivation is different for each group, whereas a criminal syndicate is motivated by monetary gain; a nation state may be probing for a future attack or, having done so previously,



launches a significant assault.

There is therefore the belief that an adversary can carry out asymmetric attacks by exploiting coding errors and due to the proliferation of physical systems that are connected to the internet these future attacks are unlikely to cease [1,4]. The risk of asymmetric attacks can be mitigated by understanding potential adversaries and their motives, as this will contribute to good all round defence; it should go without saying that conducting a risk & vulnerability survey to identify defensive weaknesses should be conducted.

Future contingencies

Better long-term security can be achieved with new generation smart metering which is a secure means of sending, receiving and accessing energy information. This does however, pose some interesting problems. Energy utilities want to cut potential energy theft, or to forcibly turn off household solar (PV) systems in an emergency, by

'Given the available information, currently it appears unlikely that baseload power generation can be provided by wind or solar PV as it will not reach significant scale & large amount of PV can

disabling any household system remotely. But an astute nation state might be wary of a facility that could let an attacker potentially turn off the lights. Again, the utility may want to monitor its customers' consumption by the half hour, so it can price discriminate more effectively, though the



competition authorities may find this objectionable. There are at least half-a-dozen different stakeholders with different views on security – which can refer to information, to money, or to the supply of electricity. And it's not even true that more security is always better: some customers may opt for an interruptible supply to save money. It would be prudent to add some type of encryption to the newer types of smart meter as a defensive measure. Encryption can provide confidentiality for data by means of stream or block cyphers & each form has positive and negative traits, which should be considered depending on the application. The amount of secrecy of the encryption system should be appropriate to the degree of confidentiality of the data being preserved. Users of encryption systems should consider the value of the data being encrypted when selecting an encryption system. Options such as the use of elliptical curve cryptography (ECC) or other security strategies for transmission & storage should be explored as options.

Smart metering

Smart meter installations would however, be an improvement to public infrastructure with the investment costs of metering possibly borne by the entity responsible for the metering, the cost recovered over time via distribution network tariffs. Equipment costs are the main driver for stakeholders when investing in metering and sensing equipment with operating costs equally important to those who have to make the choice. Wireless technology can provide a solution but is generally insecure. Poles and wires may be the less expensive option and a smart meter can piggyback on existing infrastructure in built up areas such as a CBD, though for remote communities this remains prohibitive, particularly the construction of more poles and wires. Mobile GSM and GPRS are to be considered though they are expensive due to high power consumption & this defeats the purpose of lowering electricity consumption. If smart metering is to be marketed successfully, incentives must be put in place to get consumers to change the way they use their energy. In contrast, a Northern Ireland introduction of prepaid metering led to a peak demand saving of 10%. This works on the presumption that if energy

costs are tangible, they are more likely to be adopted.

Data security & storage

Storage media and data can be secured against the main points of attack; hardware, software and data. Other points of attacks can be mounted on the network externally, on access controls, or by a disgruntled employee internally. A hierarchical electricity network, one generating large volumes of customer data, will need secure data storage. A potential way forward, the Cloud-Client model, is a combination of distributed computing, artificial intelligence, information and systems theories and programming. This is a highly complex system which has an interoperable capability by creating a smaller cloud inside a larger one with a capacity to process data, such as power supply and load. . Secure data transmission and storage poses an interesting problem; metadata cannot be encrypted inside a network as it needs to remain usable and accessible inside the network. Careful consideration must be given to this issue and the nexus between security & economics is one that needs to be explored, as the collection and storage of this information can lead to privacy issues.

Spare storage capacity should also be calculated as a long-term measure as data levels will increase over time and should theoretically be in the Petabyte range. It is essential for a data facility to store this data as securely as it can, with the ability to handle expanded capacity for the future. To mitigate the risk, the Australian Cyber Security Centres' Essential Eight Maturity Model as this assists in risk mitigation & should be considered as a prudent first step.

Supply & system inertia

There is a plan to have the Northern Territory supplied with 50% renewables by 2030, which is a move from synchronous to non-synchronous energy. The rise of solar energy (PV) has seen costs fall significantly and continuing to decline since 2010. Whilst worthwhile, caution must be exercised. The Australian Energy Regulator (AER) reported that there was an additional 2GW in generation capacity from 2012 to March 2017 of which 92% came from non-synchronous (renewable) sources. Also noted was the decommissioning of coal-based load capacity, leading to a fall of 5.3GW in synchronous generation. This indicates that the recent rise in the National Energy Market (NEM) Rate of Change of Frequency (ROCOF) & decreasing of contingency frequency nadirs is due to the removal of system inertia, caused by the substitution of synchronous to asynchronous generation.

Additionally, the combined report from Energy Australia & the CSIRO discovered that the move to non-synchronous power such as rooftop photo voltaic (PV) leads to significant levels of volatility at the point of connection between the distribution networks and transmission connection point [14,15]. Citing the South Australian (SA) model of frequency instability as a case study, it was observed that the continuous removal of system inertia contributed significantly to the 2016 SA blackout.

As outlined above, aggressively moving to a Renewable Energy Target (RET) with a high proportion of renewable

energy will lead to frequency instability in the grid & may cause unforeseen problems. Furthermore, without reliable & affordable energy output, there is a concern that the post COVID-19 economy will stall, particularly in the manufacturing sector which may be set for revival. This has led to the consideration of new national standards to mitigate the problems with uncontrollable electricity generated by PV causing problems for the energy market.

A proposed solution to the system inertia problem is a rapid acting Battery Energy Storage System (BESS) to deal with any potential drop. The first defence to stabilize a frequency drop is known as the Primary Frequency Response (PFR). The NEM prescribes stability to occur within the range of six to sixty seconds. It is recommended that a faster reaction time can occur earlier than the above-mentioned time frame. A BESS has been put forward as a Fast Frequency Response (FFR) solution to head off system nadir, as it can provide a response in a 10-20ms timeframe, replacing lost system inertia from coal & gas generators. A BESS has a simple setup; a DC battery, a DC-AC power inverter; a controller to measure interactions. The controller is divided into three: Frequency, Charge & PQ power controllers. Only the frequency controller will be discussed. It was noted that a BESS can effectively arrest system frequency drop. As noted, when PV penetration increases, there is a decrease in system inertia. Through experiments and trials it was found that if a faster solution is applied, the earlier a frequency drop is stopped & the BESS contributes to this process. Therefore the observed FFR rate with BESS is 1.77Hz, whilst without BESS the lowest nadir was close to 49.8Hz.

A note on the nuclear option

The energy security debate includes a nuclear energy capability & is being examined in a parliamentary enquiry which is investigating the 'economic, environmental and safety implications of nuclear power'. The nuclear option is part of this steady shift in energy security, which has historically been brought on by acute crises: oil embargoes, pollution, wars and events like COVID-19. Moreover, the nuclear option should also address the feasibility in economic, technological and capability terms and should be carefully considered, putting aside the fights between climate believers & climate sceptics, fossil fuels & renewables.

Globally, nuclear power adoption is mixed, with France adopting nuclear power due to the 1970s' oil shocks. In the past, the catastrophic nuclear disasters in Three Mile Island, Chernobyl & Fukushima have provided cautionary warnings & a failed nuclear system is non-negligible. The Chernobyl disaster made Germany move from nuclear power to solar, creating feed-in tariffs in the late 1990s. However, currently nuclear is not only the safest & cleanest of all energy sources, it produces 11% of the world's electricity and therefore shouldn't be discounted.

The development of Small Modular Reactors, or SMRs, is being examined in the present parliamentary enquiry. Though nothing new, SMRs' one key benefit is cost, with the aim of bringing components together for final assembly. In

an Ikea type scenario, components can be trucked-in and assembled on-site. An SMR can have an output of between 200 Mw and 300 Mw and have been used successfully in India and Pakistan.


The one big difference between renewables and nuclear is that nuclear power is not weather dependent. This advantage is off-set by the necessity for nuclear waste to be stored and managed appropriately as pointed out by the Nuclear Fuel Cycle Royal Commission.

The cost of waste management should be a primary consideration and has been raised in a parliamentary enquiry. At present there are significant waste storage facilities in South Australia and any waste generated by a reactor needs to be stored appropriately.

Another issue that would need to be considered is a reactor's necessity for water to operate effectively as parts of Australia are prone to drought and others arid desert. This may be problematic and an SMR may be better suited further north in the wetter sub-tropical regions or in littoral areas. The proposal for SMRs faces these complications in addition to legislation prohibiting the use of uranium in Australia. Particular sections of the relevant legislation would have to be repealed as currently uranium can be mined and exported but not used onshore.

Conclusion

There is much to consider with energy security; smart meter conversion, installation, storage and privacy, the nuclear option and grid stability and the increasing threat of a cyber attack. There is the future potential for web-based communication between the energy supplier & the customer which may be done by either a server in the meter or at the providers head end. Whilst this is an exciting future possibility, how this is to be secured is unclear. Within this proposed system, an energy supplier will find it easier to cut off supply to a defaulting customer, but stringent security measures must be put in place to prevent this process from being reverse engineered by a malicious actor attacking the entire grid. Issues do present themselves: is the data collection available to government, the energy provider, or both? Will regulators be permitted to forcibly turn off household PV systems? These avenues should be better understood.

Given the available information, currently it appears unlikely that baseload power generation can be provided by wind or solar PV as it will not reach significant scale & large amount of PV can destabilise the grid. Fossil fuels are considerably cheaper and can provide that steady stream of electrons necessary for modern life. Renewables can however, contribute to a cleaner environment if produced economically and businesses have undoubtedly recognised the benefit of lowered energy costs. Renewable energy will not be sidelined, but will increasingly play its part, though the days of governments throwing money at renewable power look to be over or at least being reigned in. Market projections may well be correct that the private consumer will have a significant presence in the market with the installation of household PV though costs of maintaining that connection may rise for new adopters. 

Critical-infrastructure attack attempted against Israeli water supply.



By
Dave Weinstein
Clarity, CSO

Israel appears to have thwarted a large-scale attempt at a critical-infrastructure cyber attack against its national water supply. An internal report from Israel's Water Authority indicates that the incident occurred between Friday, April 24 and Saturday, April 25.

According to a statement from Israel's National Cyber Directorate, the attempted attack targeted the command and control systems of Water Authority's wastewater treatment plants, pumping stations, and sewage infrastructure. A follow-up statement from the Water Authority and National Cyber Directorate reported the incident appeared to be coordinated, but no damage had occurred.

Organisations affected by the attempted attack were ordered to immediately reset the passwords for all of the facility's operational technology (OT) systems—especially those related to chlorine control—and ensure all control software was updated. If it's not possible to change the passwords for certain systems, personnel were advised to disconnect these systems from the internet entirely.

This attempted attack highlights that while water infrastructure often eludes the public's attention as a major source of cyber risk, it remains susceptible to both targeted and non-targeted threats.

A combination of legacy systems, growing connectivity, and federated management—most water utilities are owned and operated at a local level—warrants a high prioritisation of cybersecurity for the water and wastewater sectors on a global level.

As with most OT systems, our water infrastructure

This attempted attack highlights that while water infrastructure often eludes the public's attention as a major source of cyber risk, it remains susceptible to both targeted and non-targeted threats.

demands a granular level of visibility to detect not only latent threats on the network, but also anomalies that might be indicative of a threat or could subject the network to even novice hackers. Misconfigurations and known vulnerabilities effectively lower the barriers to entry for threat actors and increase the risk of exploitation.

Furthermore, as information technology (IT) networks converge with OT networks, owners and operators of water infrastructure should be ever vigilant against account compromises that might grant an attack direct access to industrial control systems. This includes employees and third-party vendors that are accessing the infrastructure remotely.

The security and reliability of critical infrastructure—such as water, power, and telecommunications—is more essential than ever amid the current global pandemic.

WATCH

LISTEN

NATIONAL CYBERSECURITY

Impacts & Realignment of 2020 – Insights from Australia and Israel

*“Has national
cybersecurity awareness
and resiliency improved in
2020 and is a new online
posture necessary to
better combat motivated
and agile attackers?”*

FEATURING



YIGAL UNNA

Director General of the Israel National
Cyber Directorate



DR. TOBIAS FEAKIN

Australian Ambassador for Cyber
Affairs & Critical Technology



The golden tax department and the emergence of GoldenSpy malware

By
Brian Hussey,
VP of Cyber Threat Detection
and Response at Trustwave

Trustwave SpiderLabs has discovered a new malware family, dubbed **GoldenSpy**, embedded in tax payment software that a Chinese bank requires corporations to install to conduct business operations in China.

In April of 2020, the Trustwave SpiderLabs Threat Fusion Team engaged a customer to conduct a Proactive Threat Hunt. The company is a global technology vendor with significant government business in the US, Australia, UK, and recently opened offices in China. Our threat hunt produced several key findings important to the long-term security of their network, however, one key finding stood out as potentially impacting countless other businesses who currently operate in China. A full analysis of our findings is available for download.

Investigation Details

We identified an executable file displaying highly unusual behavior and sending system information to a suspicious Chinese domain. Discussions with our client revealed that this was part of their bank's required tax software. They informed us that upon opening operations in China, their local Chinese bank required that they install a software package called Intelligent Tax produced by the Golden Tax Department of Aisino Corporation, for paying local taxes.

As we continued our investigation into the tax software,

we found that it worked as advertised, but it also installed a hidden backdoor on the system that enabled a remote adversary to execute Windows commands or to upload and execute any binary (to include ransomware, trojans, or other malware). Basically, it was a wide-open door into the network with SYSTEM level privileges and connected to a command and control server completely separate from the tax software's network infrastructure. Based on this, and several other factors (described below) we determined this file to have sufficient characteristics to be malware. We've since fully reverse-engineered the files and named the family GoldenSpy.

GoldenSpy was digitally signed by a company called Chenkuo Network Technology and the signature used identical text for both the product and description fields; 认证软件版本升级服务 – which translates to “certified software version upgrade service”. This name may sound like legitimate software, however, in this situation the tax software already has its own updater service that functions well, and in a way completely unrelated to GoldenSpy.

There were several other unusual aspects of this file, to include:

- GoldenSpy installs two identical versions of itself, both as persistent autostart services. If either stops running, it will respawn its counterpart. Furthermore, it utilizes an exe protector module that monitors for the deletion

of either iteration of itself. If deleted, it will download and execute a new version. Effectively, this triple-layer protection makes it exceedingly difficult to remove this file from an infected system.

- The Intelligent Tax software's uninstall feature will not uninstall GoldenSpy. It leaves GoldenSpy running as an open backdoor into the environment, even after the tax software is fully removed.
- GoldenSpy is not downloaded and installed until a full two hours after the tax software installation process is completed. When it finally downloads and installs, it does so silently, with no notification on the system. This long delay is highly unusual and a method to hide from the victim's notice.
- GoldenSpy does not contact the tax software's network infrastructure (i-xinnuo[.]com), rather it reaches out to ningzhidata[.]com, a domain known to host other variations of GoldenSpy malware. After the first three attempts to contact its command and control server, it randomizes beacon times. This is a known method to avoid network security technologies designed to identify beaconing malware.
- GoldenSpy operates with SYSTEM level privileges, making it highly dangerous and capable of executing any software on the system. This includes additional malware or Windows administrative tools to conduct reconnaissance, create new users, escalate privileges, etc.

These factors have led us to the conclusion that GoldenSpy is a well-hidden and powerful backdoor that surrenders full remote command and control of the victim system to an unknown adversary.

Figure 1 shows the network communication patterns of GoldenSpy installation via Intelligent Tax software.

The scope of this campaign is not currently known. For our client, GoldenSpy was secretly embedded within the Aisino Intelligent tax software, but we cannot determine if this was targeted because of their access to vital data, or if this campaign impacts every company doing business in China. We have identified similar activity at a global financial institution, but do not yet have further telemetry into this campaign.

The current GoldenSpy campaign began in April of 2020, however, our cyber threat intel analysts have discovered variations of GoldenSpy that date back to December of 2016. It is of interest that Chenkuo Technology's website announced a partnership with Aisino in October of 2016, two months prior to the original emergence of the GoldenSpy malware family. Their partnership is for "big data cooperation". GoldenSpy certainly could enable big data access and collection. Trustwave SpiderLabs has no current knowledge if GoldenSpy was active in the wild since 2016, our first identification of usage was April 2020. To be clear, we do not yet know the scope, purpose, or actors behind the threat. We do not know whether Chenkuo Technology or Aisino are active and/or willing participants or the extent of their involvement other than what is presented in the report.

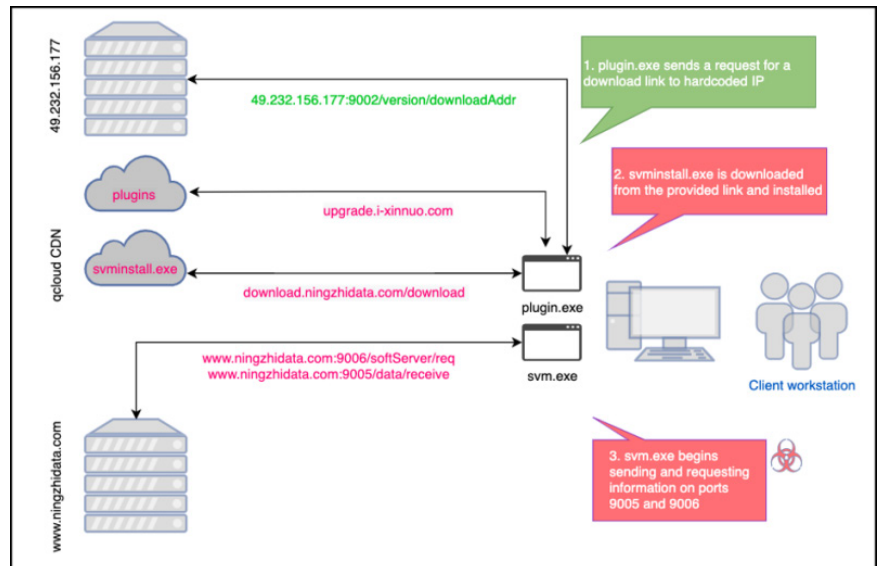


Figure 1

Recommendations

We believe that every corporation operating in China or using the Aisino Intelligent Tax Software should consider this incident a potential threat and should engage in threat hunting, containment, and remediation countermeasures, as outlined in our technical report (download link below).

Trustwave SpiderLabs is still actively investigating and seeking out more telemetry on the GoldenSpy campaign. If you have any information about this activity or feel you may have been victimized by this attack, please reach out to the Trustwave SpiderLabs Threat Fusion Team at GoldenSpy@trustwave.com.

We are available for advice, information exchange, or to engage threat hunting / forensic investigation services.


GoldenSpy Technical Report

Trustwave has prepared a detailed technical report on GoldenSpy that can be downloaded here. The report contains:

- Full incident details, including network and file system indicators of compromise (IOC's)
- Malware reverse engineering analysis reports
- Historical network IOC's and known GoldenSpy variants
- GoldenSpy threat hunting recommendations, including a custom YARA signature designed to identify unknown GoldenSpy variants
- Remediation recommendations

Aisino Corporation and Nanjing Chenkuo Network Technology were contacted and briefed on these findings, as part of Trustwave's documented vulnerability disclosure process. At time of publication of this report, neither have responded.

About the Author

Brian Hussey is Vice President of Cyber Threat Detection & Response at Trustwave. He leads the SpiderLabs Threat Fusion and the Global Threat Operations Teams. Trustwave's Managed Detection & Response (MDR), Managed Detection (MD), Threat Hunting, Intel, and Investigation services fall under his purview. 



Getting serious about security assurance

By
Codee Ludbey CPP
Digital Lead at Norman Disney
and Young, responsible for a
team of security professionals in
New South Wales.

My favourite explanation of the difference between safety and security is succinctly (and humorously) presented by Somerson (2009), who states that security is an approach to protect against the malicious actions of others, where safety is an approach to protect against the duncery of negligence.

Because we can all relate more easily to the the latter, we tend to have more conversations about making designs safe as opposed to secure. In the public consciousness, there is a higher duty to provide safety than security, and this shows in a variety of ways in the engineering industry.

For example, Safety in Design is thoroughly embedded in the typical design processes of any built environment practitioner. Many hours are spent in Safety in Design Workshops, filling in Safety in Design Registers, and developing comprehensive Safety in Design strategies.

On the other hand, Security in Design is still a new and emerging topic that few have actually applied properly outside of Government projects. Even where security in design is applied, the level of thoroughness and completeness from a security assurance perspective is often less developed than the safety in design process. This is probably due to the relative immaturity of security as a science, particularly as applied in the built environment.

Nevertheless, due to some recent observations and experiences with more rigorous security and safety assurance processes, I wanted to present an overview of how the two can be co-managed in the security risk management process. But, before we delve into security

assurance, let's start with a definition of safety assurance from Kelly & Weaver (2004).

"[Safety Assurance is] a qualitative statement expressing the degree of confidence that a safety claim is true."

In the context of design, this definition is basically explaining that safety assurance is a statement or argument that is reinforced by evidence that expresses the level of confidence that a system is safe to operate or rely upon. This is important, as safety, much like security is not certain, and rests on assessments of likelihood and consequence. Subsequently, under the various occupational health and safety laws amongst others, we need to satisfy ourselves, our clients, and the State that we have reduced risks so far as reasonably practicable (SFAIRP). Safety assurance is the process through which we do this.

Security assurance then, is a similar - we need to demonstrate security risk reduction SFAIRP and that a tailored approach to the security of critical assets has been undertaken. Security practitioners have a responsibility for ensuring security is embedded in a project, and that the security objectives are met through a well reasoned argument and risk reduction strategy. This argument should be built upon supporting evidence (or security cases) that can demonstrate to a third party how the identified security risks have been reduced to acceptable levels. To effectively construct this argument, there needs to be a clear definition of the security requirement or objective, a series of security cases (or arguments) that support these objectives, and the subsidiary evidence in design that informs the arguments.



For example, to appropriately assure the reduction of a vehicle borne improvised explosive device risk, a security case could be prepared arguing that the implementation of asset stand off, blast resilience treatments to the building structure and facade, and presence of first aiders on site reduces the risk so far as is reasonably practicable. Each of these risk reduction measures would then be evidenced - through drawings, standard operating procedures, calculations, and blast models, for example.

Importantly, these security elements need to be reflected in any safety arguments that are being prepared as well, as safety and security are intertwined in a number of ways. Many security incidents have a safety component (injury or death of people), and as such need to be tracked by the safety practitioners as part of their assurance activities. Below is an overview of how I have tracked these items on previous projects.

While some of these arguments and discussions do come out in the typical security risk assessment process through workshops and risk analysis, it is rare for a clear concise overview of the security SFAIRP argument to be presented, with strong evidence trails and clear traceability between objectives, identified risk, provided controls, and documentation. This traceability is vitally important for reinforcing the adequacy of the security measures, and also for demonstrating due diligence in design and reducing personal liability exposure under work health safety legislation in Australia.

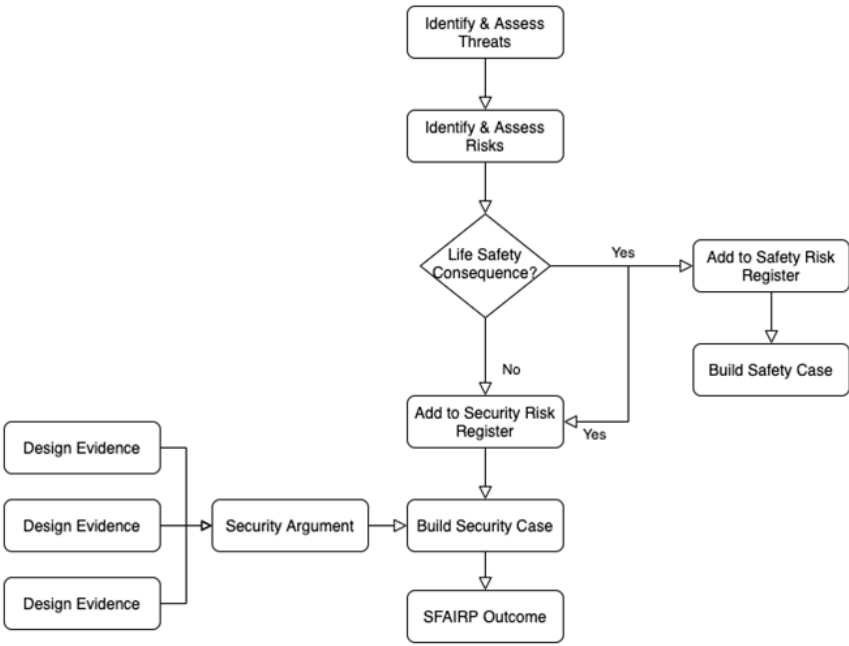
Below is an example of how these elements of the

security assurance approach might be presented and tracked through a design. Each of these identified items (threat, risk, control, design), while described in various different pieces of documentation, should all be brought together in the Security Hazard Log for ease of traceability.

Overview of a Traceable Evidence Trail in Design Documentation

To further expound on the traceability of the security arguments, the risk register, and corresponding security reports can be supplemented with a Security Assurance Goal Structure. Goal Structured Notation is increasingly being used in safety science to improve the structure, rigour, and clarity of safety arguments. Due to the complexity inherent in demonstrating risk reduction to acceptable levels, text based arguments can be difficult to follow, and can require dense and lengthy reports to appropriately present. Due to this complexity, Goal Structured Notation has been developed to visualise safety arguments. Visual presentation is easier to follow, and can more readily demonstrate connections and relationships between design elements and risk,

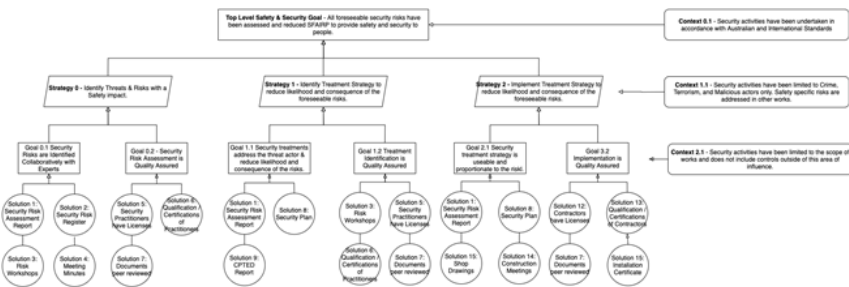
Below is an example of a Security GSN that provides a summary of the security arguments. The top level safety and security goal is presented for the project, which is supported by 3 security strategies (arguments). Each of these strategies have goals that have to be achieved to demonstrate that the strategy is effective. To demonstrate



Overview of the Security/Safety Documentation Flow



Overview of a Traceable Evidence Trail in Design Documentation



Example Goal Structured Notation for Security Arguments

To demonstrate that these goals have been achieved, a number of solutions (or evidence) need to be presented. Each level of the argument should be referenced back to a tangible piece of evidence, such as a report, meeting minutes, or other formal record to provide an easily traceable, and auditable overview of the security strategy.

that these goals have been achieved, a number of solutions (or evidence) need to be presented. Each level of the argument should be referenced back to a tangible piece of evidence, such as a report, meeting minutes, or other formal record to provide an easily traceable, and auditable overview of the security strategy.

Example Goal Structured Notation for Security Arguments

By providing a GSN as a summary of the security approach, we can assure the client, third parties, and if it came down to it, a court, that the process that was undertaken provides a proportionate level of safety. Altogether, the process of assurance and appropriately arguing the security risk management strategy is vital to demonstrate the effectiveness of security controls, and to contextualise how security risks are reduced. The provision of extensive evidence, and providing a trail from this evidence through the process to the original threat identification can be a powerful tool in convincing non-security practitioners that appropriate due diligence has been undertaken.

Much like safety science before it, security is likely to go through a similar process of professionalisation. If we are do not take active steps to assure our methodologies, we are likely to be burned when things go wrong. While a fully evidenced and assured security design is time intensive, the benefits are substantial - both legally and professionally. A proper security assurance process demonstrates the level of thought and detail that goes into an effective security strategy, and removes the shroud of mystery and clarifies the 'dark arts' of security to the non-practitioner. ▶



COURSES

Search and find all upcoming featured courses



ESET
Free Cybersecurity
Training for your
remote workforce

Free Training

**ESET Cybersecurity
Training**



**CYBER
SECURITY
TRAINING**
+ISACA CSX

Cybersecurity Nexus
(CSX) - Linux
Application and
Configuration (CLAC)



**CYBER
SECURITY
TRAINING**
+ISACA CSX

Cybersecurity Nexus
(CSX) - Network
Application and
Configuration (CNAC)



**CYBER
SECURITY
TRAINING**
+ISACA CSX

Cybersecurity Nexus
(CSX) - Penetration
Testing Overview
(CPTO)

Plus many more!



Invest in intelligence now to prepare Australia's utilities for the future.

By
Ray Griffiths,
OT Security Lead, Australia
& New Zealand, Accenture;
Tony Histon, Transmission &
Distribution Lead, Africa, Asia
Pacific and the Middle East,
Accenture.

On Christmas Day 2015, attackers used spear phishing emails and variants of the BlackEnergy 3 malware to gain access to the technology platforms of electricity companies in the Ukraine, knocking power systems offline for six hours.

A similar scenario taking place in Australia is not hard to imagine – a 40-degree summer's day and power fails across major Australian cities sending citizens into chaos. It is not until the payment of extortionate ransoms and many hours before power is restored. Since the attack in the Ukraine, and subsequent power outages in Argentina, Paraguay and Uruguay, hackers have become even more sophisticated at disrupting operations and wreaking havoc across the grid for energy providers and their customers.

As energy generators and network companies are increasingly integrating Operational Technology (OT) systems with IT, their potential attack surface consequently increases, creating vulnerabilities across the network. With this reality, comes recognition among Australian utility

providers for greater protection of our nation's critical infrastructure and assets, a sentiment highlighted in the federal government's 2020 Cyber Security Strategy and Accenture's contribution to the piece.

A survey conducted by Accenture found that despite investment in cyber security rising among three in five utility companies, the detection rate for attack remains low at just 56 per cent. Here's how utilities companies can better prepare and protect their critical assets and infrastructure and ensure digital investments deliver valuable returns now and well into the future.

Identifying and minimising infrastructure risks

As Australian utility providers continue to modernise grids and power plants to enhance reliability and support demand management, OT systems are increasingly being integrated with IT platforms. This converged IT-OT attack surface can

increase vulnerabilities, giving attackers opportunities to wreak havoc if they can penetrate cybersecurity defences anywhere in the system. In the Ukraine, the malware used by the attackers was able to reach the grid's control system from the corporate network as control system interfaces had been connected directly to the Local Area Network (LAN).

Whilst IT platforms tend to receive regular upgrades and maintenance to reduce the risk of such malicious attacks, OT systems and platforms may be replaced less frequently, resulting in out-of-date infrastructure that is easier to infiltrate. Without proper lifecycle management, legacy systems in OT environments may be subject to vulnerabilities patched up years ago in IT.

It is therefore not surprising to see that 54 per cent of utilities executives surveyed by Accenture said one of their biggest security challenges was legacy components. Organisations must know where the risks to their systems and platforms lie and employ proper maintenance to ensure they are not left open to attack.

Employing threat intelligence to understand your adversaries

Nearly three quarters of utility executives admit staying ahead of attackers is a constant battle that is becoming increasingly unsustainable and financially draining. A solution is to utilise shared and actionable threat intelligence to pre-empt malicious attacks and stop them before they have the chance to compromise systems and networks.

Utilising threat intelligence throughout operating environments and among business ecosystem partners is critical, considering 40 per cent of breaches in 2019 originated from indirect attacks through a supply chain or business partner eco-system. Without appropriate controls, a compromise of a utility service provider may result in an impact that impacts the wider energy grid.

Implementing threat intelligence enables utilities organisations to better understand the tactics, techniques and procedures likely to be used against the operating environment. When threat intelligence is deployed, boards receive security reports and analyst briefings on threat context, intent, target and associated business risks. Combined with expert security analysis, these services can track the dark web for indication that threat actors may be targeting a particular utility and gain vital intelligence about their plans.

Bridging the gap to eliminate weaknesses in existing systems

Preventing cyber breaches isn't just about technology and intelligence. Australian utility companies must bridge the gap between IT and OT teams and actively share resources and learnings in order to benefit their entire organisation.

Utilities need visibility of the conversation streams between IT and OT equipment, especially when it comes to control systems and cyber assets. Joint security teams need to map the OT environment to control and monitor interactions with OT components. Interactive dashboards, offer visibility of OT networks and their constituent

Implementing greater digitisation in the grid will offer Australia's utility companies considerable resilience and sustainability benefits, yet will also heighten their risk footprint, leaving many ill-equipped to respond when malicious threats arise.

intelligent electronic devices (including relays, meters, and remote terminal units) to present the attack surface at risk and any alerts to unexpected behaviour.


Additionally, it is vital that OT remains part of the security governance cycle and is included in all of organisation's conversations and solutions. IT and OT security need to come together to deliver a strong security posture. The IT domain brings established controls and procures, OT brings valuable expertise in the physical and virtual environment: integrating capabilities will improve overall utility cyber security maturity.

Implementing greater digitisation in the grid will offer Australia's utility companies considerable resilience and sustainability benefits, yet will also heighten their risk footprint, leaving many ill-equipped to respond when malicious threats arise.

With cyber attacks continuing to hit at an alarmingly frequency, Australia's utility providers must bolster their IT/OT cyber security in a joint effort and drawing on threat intelligence to secure a safer and more sustainable future for themselves and their customers. ▲



Episode 204 Accenture Podcast Series: The IT-OT attack surface and developing Australia's cybersecurity posture



Siloed response to cyber threats failing to protect Australian organisations.

By
Mark Sayer,
APAC Cyber Defence Lead,
Accenture; Joseph Failla,
Security Lead, Accenture
Australia and New Zealand.



Episode 195
Accenture Podcast Series:
Why threat intelligence is
your best defence -
Accenture's new Cyber
Fusion Centre, Sydney

Australian organisations are entering a new era in the fight against cyber crime, typified by deep collaboration between threat actors, the formation of cyber crime syndicates, compromised data sharing and pre-distributed malware designed to quickly knock out company-wide IT systems. This year, targeted and devastating attacks have already caused significant disruption for Australian organisations spanning logistics, healthcare and infrastructure.

Cyber criminals are becoming increasingly sophisticated and relentless in their pursuit of security weaknesses and new vulnerabilities. The cost of ransomware attacks alone increased by 40 percent in Australia from 2017-2018, and companies spent around \$10 million dealing with cyber threats during that same period, according to Accenture's 2019 Cost of Cybercrime Report.

Although conventional cyber crime continues to dominate the threat landscape, Australian organisations are now facing more targeted intrusions, with intricate relationships forming between threat actors and the underground economy allowing cyber criminals to sell access to an organisations' data from dark web marketplaces. These augment traditional attacks and make it challenging for organisations to know their enemies. In fact, some businesses may have already been exposed to malicious software, sitting dormant until activated for the right price.

The disruption for Australian businesses, and their employees, partners and customers caused by

these intrusive attacks highlights inadequacies within organisational cyber security. The traditional 'whack-a-mole' style approach to cyber threats, where successful and attempted attacks are dealt with one-by-one, is clearly no longer effective against the onslaught of these sophisticated and high-profile attacks.

Changing tack with cyber threat intelligence

Fortunately, Australian organisations are now moving towards a smarter and more integrated approach to cybersecurity. Rather than responding to attacks as they occur, organisations are leveraging valuable intelligence to gain a better understanding of the cyber threat landscape.

When analysed correctly, cyber threat intelligence (CTI) allows companies to identify intelligence gaps and develop proactive strategies for responding to cyber threats. However, many continue to take a siloed approach to this information, using the intelligence as an indicator of compromise to shore up areas of previous vulnerability. Whilst useful for closing gaping holes in an organisation's front-end, this will do little to deter sophisticated actors, determined to find a more insidious pathway inside.

For organisations to succeed with CTI, they must recognise what information they need to successfully fight back, develop models for risk-based decision making and provide actionable insights for departments across the organisation.



Fighting back with a strategic approach to cyber security

As a start, organisations should use intelligence to create a better understanding of their individual threat landscape and determine the likelihood of an attack. This requires an inward look at digital assets and third party vendors to analyse how valuable they may be to cyber criminals.

More broadly, determining what types of actors commonly attack an organisation's geography can provide important insight into location-based vulnerabilities. For example, ransomware incursions increased by 58 percent in Australia from 2017-2018, highlighting a trend toward lock-out style attacks which can cause serious disruptions even if data is backed up and secured safely offline.

Beyond this, the modus operandi of threat actors operating in an organisation's industry should be explored. For financial services, an industry traditionally reliant on value chains and vendors, Accenture observed supply chain vulnerabilities advertised on underground marketplaces to be primarily affecting the sector, according to Accenture's 2019 Cyber Threatscape Report. This represents a unique tactic by cyber criminals targeting financial services, who aim to route around strict security protocols. Just this year, an Australian bank suffered a data breach via a third-party vendor with attackers gaining access to its server during a routine upgrade – a time of known vulnerability for servers.

Recognising how sophisticated attacks may be and

what techniques they use will allow organisations to develop models better suited to realistic potential threats. Why set up the cyber equivalent of a full-blown motion sensor and CCTV system when the attacker is simply looking for an open window?

Making the most out of CTI

In addition to useful threat intelligence, optimising an organisation's threat knowledge base and developing a core team equipped to handle any cyber crisis will inform a more responsive and measured strategy based on the intelligence.

In order to make the most out of CTI, Australian organisations must hire the most qualified experts, for example, those from ex-defence or government backgrounds. They may have deeper insight into current cyber threat intelligence techniques and can better foresee attacks before they arise.

Further, information should not come from one source. Rather, organisations should leverage industry-based CTI sharing such as from Information Sharing and Analysis Centres (ISACs.). Collaboration between industry, government and research sectors is key. Often organisations conduct information collection alone, which results in a fragmented industry understanding of the threat landscape. Collaborating with peers, government and law enforcement will broaden industry knowledge and ensure a unified response to potential attacks.

Finally, threat intelligence should be comprehensible by a long list of stakeholders. Painfully detailed diagnostics of an organisation's cyber flaws won't help the c-suite create a compelling case for spending money on security operations. Instead, security chiefs must develop high-level abstracts on critical events, potential threats and vulnerabilities designed to be easily understood by senior executives. For other tech-dependent departments, relevant overviews should be developed. For example, briefings on the latest web application attack techniques for digital developers or details of the latest real-world threats for operations teams.

Know your enemy

As organisations grow their reliance on new technologies, high-profile cyber attacks are set to become even more devastating, disruptive and costly. For Australian organisations to protect themselves and their customers they must know themselves and their enemies.

This means more than simply collecting intelligence. Organisations must also leverage this information for actionable insights about themselves and the broader threat landscape. It is essential that organisations also work together to create a broader ecosystem of awareness and bolster industry-wide cyber protection.

The prevalence of sophisticated and insidious cyber attacks will only grow in Australia and across the globe. However, with more efficient use of intelligence and more strategic approaches to cyber security, Australian organisations can stay protected and will be better equipped to respond effectively when the enemy strikes. ▀



Human error – Deliberate or unintentional?

By
Visahl Samson David **Selvam**,
Singapore

Throughout this technology age, from industrial to business, cyber security plays a critical role everywhere. Maintaining confidentiality of information in an enterprise helps it to work and maintains consistent operations.

The human is the weakest link in the cybersecurity chain from the very beginning (Swinhoe, 2019) in 2019. In the field of information security, human error can be divided into two groups, either deliberate or unintentional. An intentional one may occur due to an insider threat, which has motivations behind it. While an unintentional one has no motivation or pre-planning, which may be due to a number of reasons, such as not knowing how a particular technology works, or lack of awareness.

According to research conducted by Kaspersky (Kaspersky, 2017), in 2017 nearly 49% of malware/virus attacks are consisting of human error as contributing factors. In these attacks 53% are due to careless/uninformed employees, 36% of social engineering/phishing attacks, 38% is accidental hardware loss by the employee. Furthermore, as per Verizon's 2019 data breach investigation report (Verizon, 2019), 34% of the data breaches are due to the threat of human error.

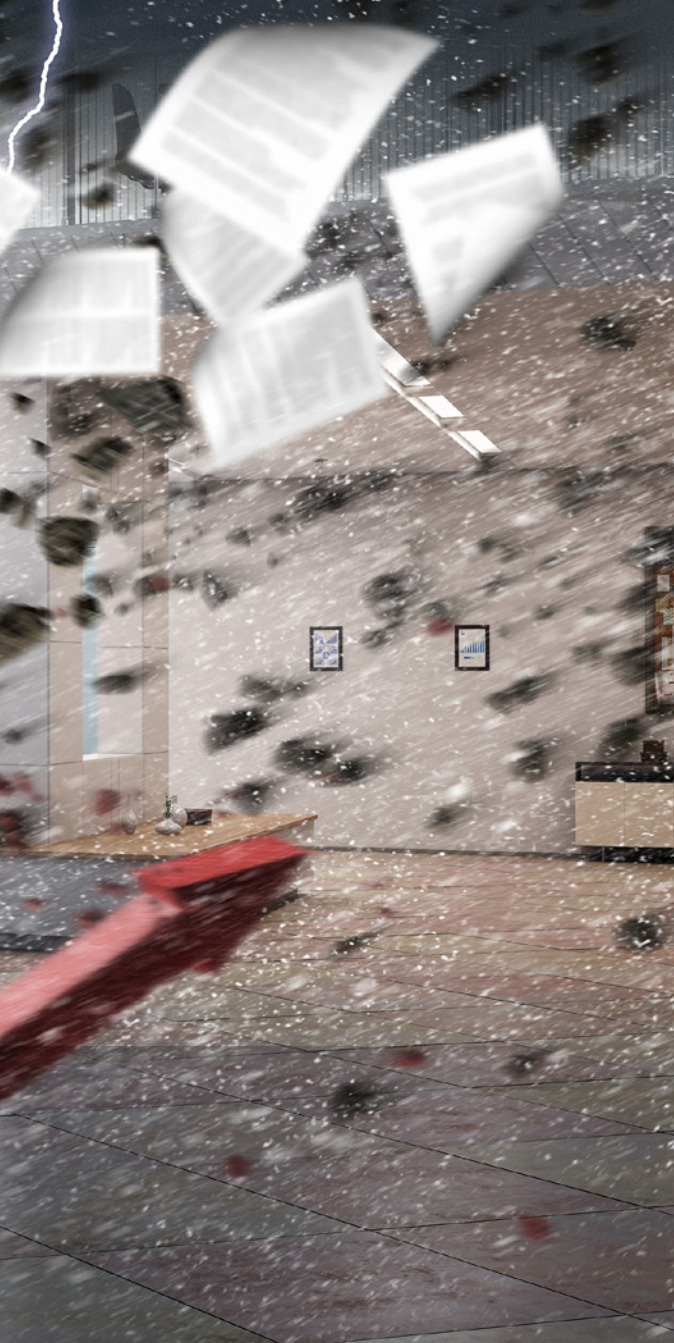
Human error causes and impacts

The research demonstrates that human error contributes to data breaches. Companies need to establish how these issues are going to happen and how it can impact them. There are several causes of human error.

The primary one is ignoring the workplace policies and/or not being aware of them. Under this case, the employee is presumably not aware of the organization's information security policies and the employee has breached the policy which has resulted in a security incident.

Another reason is that common information security practices are not known. Awareness of information security includes classification of phishing / spear-phishing emails, malicious email attachments, poor passwords etc ... Without that basic awareness of information security, the employee becomes vulnerable to the attacker / hacker. Currently attackers are not targeting the company's executive/board members but rather they're targeting low-level employees. Recently in the USA, it is reported (Lindsey, 2020) that hackers are targeting the potential employees to spread malware on the organization's system.

The third primary reason is negligence. This could



include failing to do the work properly. This factor would mostly be unintentional, but it does have a significant impact on the organization.

Data breaches occurred due to human error

Several data breaches have occurred due to human error. The well-known and famous data breach that occurred as a result of human error was Target Data Breach in 2013. Data breach studies (Xiaokui, Danfeng, Ke & Andrew, 2017) indicate that the data breach consists of several human error facts. In the first place, the malware has been planted into the systems in a sophisticated phishing attempt. Second, security warnings have been ignored and no action has been taken against the warnings generated by the monitoring software. According to reports, the total cost of this data breach is nearly US\$300 million.

McCumber cube

McCumber cube methodology can be used in organizations to reduce the risk and impact caused by human error.

Education - SETA programs

SETA stands for Security Education and Awareness. SETA is a training program (Solms, S.H. & Solms, Rossouw, 2009) aimed at educating employees to reduce human error-related data breaches and to increase awareness of information security among them. Implementing SETA programs is one of the recommended (M.G. Lee, 2012) methods and is followed by many organizations at this moment. According to ISO27001 Clause A.8.2 (Calder & Watkins, 2015), The organization should enable this SETA program not only to its employees, but also to its respective contractors and third-party users. Measures to conduct SETA programs at least once a year are recommended.

Simulated attacks

Simulated attacks designed by the organizations help in testing the knowledge and practices of employees. These are similar to the exercises of a fire drill. In simulated attacks, the organization sends the employees phishing / malicious email / email attachments to see how well they are identified and responded to by the employees. This is widely used and one of the recommended methods to follow (Rapid7, 2018).

Policy

Policies play a vital role in controlling/preventing the impact of human errors. The most recommended and important policies are password policy and information disclosure policy.

Password policy

The primary purpose of the password policy is to create a strong password standard, to protect those passwords, and to enable frequently changing passwords. The password policy (Sans, n.d.) applies to all personnel responsible for any account, any system used within the organization, the network, and the facility to store any information. The following is an example of a password policy according to NIST 800-63 (NIST, 2020) guidelines.

- Password should be a minimum of 8 characters when it being set-upped by people
- Password should be a minimum of 6 characters when it being set-upped by a service/system.
- The password should support all the ASCII characters including space.
- Chosen passwords should be checked with a password dictionary.
- Password should support at least 64 characters of maximum length.
- Minimum of 10 attempts before the logout.

Apart from those NIST framework guidelines, there are some more options which can be added to the password policy,

- Passwords must be changed every 90 days.
- The password should contain at least one upper case letter, one lower case letter, one symbol, and one

number. This will help to increase the complexity of the password.

Information disclosure policy

According to ISO27001 Annex A.7.2 (Humphreys, 2016), organizations should conclude agreements whenever new staff join the organization. Also referred to as a Non-Disclosure Agreement, this sets out what information can be disclosed to the public and what information cannot be disclosed. The agreement should clearly set out the actions to be taken in the event of a breach of the Non-Disclosure Agreement. In addition, it is important that the organization take appropriate measures to make its employees aware of the agreement.

In addition, the organization can use the data classification policy to make this work easier. Data classification helps the organization to classify in terms of confidentiality. A typical data classification has four levels (Irwin, 2019); confidential (only higher management must access); Restricted (only particular job roles can access); internal (all the employees can access); and public (everyone can access). Classifying the information allows an employee to be aware of the information that they can disclose.

Apart from these two policies, organizations can consider another policy for BYOD (Bring Your Own Device). Organizations are also advised to run periodic internal audits/reviews to ensure security measures.

Technology

The use of proper technology will significantly reduce the occurrence of human error. Technology measures that can be implemented to prevent human errors include;

Employee Monitoring software

Use of Employee monitoring software is a basic mechanism that can be used by the organization to reduce the occurrence of human error. This facility allows every activity of the employee to be monitored so that, if any security incidents occur, information from the monitoring system can be used to identify the root cause / where it begins. There are several ethical issues associated with this but using this with acceptable policies such as what data can be collected will be beneficial.

Cryptography and Encryption

Encryption is the most recommended technology to counteract threats, particularly human error. Organizations should use encryption while resting data (Robb, 2017). Also, the algorithm that is going to be in place should be secure enough, and in general, instead of creating a new algorithm, it's wise to choose one that already exists. Currently, in the industry, there are several vendors like IBM, Dell, McAfee providing their cryptography and encryption products.

Identity and access management

Allowing employees to have access only to what they need for their job roles would be an appropriate strategy. Identity and Access Management (IAM) deployment in place would also help to reduce the risk.

Two-factor authentications (2FA)

Currently, usage of two factor/multi-factor authentication is emerging among the organizations to provide an additional layer of support. According to research reports (Sans & Preston, 2014), the intention of adopting to 2FA is significantly increasing.

Upcoming landscape

According to the future cyber-attack landscape predictions of the security organization (Checkpoint, 2019), it is estimated that the phishing-based attacks will remain as a top vector of attack and will rise rapidly. Another prediction (Jason, 2019) estimated that the Phishing vector would go beyond e-mail and launch via cloud. So, when the attack vectors evolve the organizations need to keep their tactics up to date to combat them.

Conclusion

Since this vector of threat is human, it cannot be eliminated, but countermeasures can help to stop human error from turning into security breaches that can cause serious impact to an organization. Technology is not a single solution in cybersecurity to solve all the problems, but rather the shared responsibility of everyone to keep the digital world safe. 

CYBER RISK

LEADERS



COVID19 – PODCAST EPISODES



Episode 199 - National Security implications of COVID-19 - Prof John Blaxland & Jacinta Carroll - Australian National University

In this episode Chris Cabbage speaks with John Blaxland, Professor of International Security & Intelligence Studies, Strategic and Defence Studies Centre and Jacinta Carroll, Senior Research Fellow, Counter Terrorism and Social Cohesion, National Security College, each at the Australian National University. We discuss the immediate national and regional security implications of how 2020 is panning out and open discussion around military, national security and civilian vulnerability, including in a cyber context.

Episode 202 - COVIDsafe Tracing App gets peak tech industry backing - Interview with AIIA CEO Ron Gauci

The Australian Information Industry Association (AIIA) has given strong support for the Australian Government's contact tracing app, COVIDSafe, designed to digitally alert Australians of nearby COVID-19 infections. As the peak industry body for innovation technology in Australia, the AIIA was given an exclusive briefing today by the Minister for Government Services, Stuart Robert MP, CEO of the Digital Transformation Agency and head of Australian Cyber Security Centre on the technology behind the tracing app and the cyber security protections built into it.

Episode 200 - Privacy recommendations for Australia's use of contact tracing mobile apps like TraceTogether

Interview with Professor Dali Kaafar, Executive Director of the Optus Macquarie University Cyber Security Hub, in his role as a co-researcher into making privacy recommendations as the Australian government explores the use of contact tracing mobile apps as a tool for public health officials and communities to fight the spread of the COVID-19 pandemic.

Episode 198 - Early impacts & opportunity of COVID-19 on the Australian Cybersecurity sector - Michelle Price, CEO of AustCyber

Interview with Michelle Price, CEO of AustCyber, the Australian Cyber Security Growth Network. In the wake of a global pandemic, emerging at the time of the RSA Conference, San Francisco what has been the impact on the Australian \$8.5 million project funding round issued in late 2019. Michelle outlines how the Australian cyber security sector and parts of the AustCyber cohort face significant risk as a result of an economic downturn and also some that are responding to an uptake and have a major market and sovereign opportunity should Australia recover strong and fast.

Episode 194 - COVID-19 deals a major blow to Asia's technology sector, Canalys Report

Interview with Sharon Hiu, APAC Channel Analyst with Canalys, based in Singapore. Canalys Report, 'COVID-19 deals a major blow to Asia's technology sector', dated 20 February highlights the COVID-19 outbreak will hurt Q1 sales in APAC, especially of smartphones, PCs and component products. But customer adoption of cloud-based services will increase as more people use videoconferencing and collaborative and online tools to execute business continuity plans and reduce travel.

Episode 206 - COVID-19 impact on Asia's technology sector, Canalys Update #2

Interview with Sharon Hiu, APAC Channel Analyst with Canalys, based in Singapore. This is our second update podcast (recorded 22 May, 2020) to gain current Canalys observations of the APAC Technology Channel sector and the impacts of the COVID-19 pandemic. What has been the overall impact for Asia?

Episode 201 - Securing Remote Workers in the Age of Teleworking with DNS, DHCP and IP address management

Interview with Matt Hanmer, managing director for ANZ and regional director for South Pacific for Infoblox and Jasper Chik, Sales Engineering Manager, ANZ, discussing what Infoblox has observed over the last few months as the workforce has shifted to a remote environment and the common vulnerabilities overlooked by Enterprise in managing a remote workforce. 2019 international Threat Hunting and intelligence conference in Singapore (29th Nov 2019).

PODCAST HIGHLIGHT EPISODES



Episode 208 - Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations - Interview with Morey Haber, CTO & CISO, BeyondTrust

Interview with Morey Haber, CTO & CISO, BeyondTrust on the launch of the 2nd edition of his first book, "Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations". The first edition was a best-seller on Amazon when it was launched 3 years ago. customer adoption of cloud-based services will increase as more people use videoconferencing and collaborative and online tools to execute business continuity plans and reduce travel.

Episode 207 - The 3 C's of Cyber - Crisis, Culture & Compliance – Fortinet Series Ep1

In the first of a three part series with Fortinet, we speak with Cornelius Mare, Director of Security Solutions Fortinet ANZ and Glenn Maiden, Director FortiGuard Threat Intelligence, ANZ and delve into crisis management during a COVID-19 pandemic and its relationship to culture and compliance and how these three critical areas are interdependent.

Episode 192 - Video Management Systems and responsible application of advanced technology - Milestone Systems

Interview with Brett Hansen, South Pacific Country Manager for Milestone Systems. Brett is responsible for driving Milestone Systems across a diverse range of new and existing markets in the region, while facilitating large-scale projects and partnerships, as well as leading the company's local team. Organisations' and 'Just-in-Time (JIT) Privileged Access – Why It Is The Next Big Step In Risk Reduction & How To Implement It'.

Episode 204 - Accenture Podcast Series: The IT-OT attack surface and developing Australia's cybersecurity posture

Interview with Ray Griffiths, ANZ OT Lead, Perth and Zoe Thompson, Manager Accenture Security Practice, Canberra discussing the Australian Security of Critical Infrastructure Act 2018 and how a broad attack surface across Critical Infrastructure also increases the opportunities for malicious actors to wreak havoc if they can penetrate cybersecurity defences anywhere in the system.

Episode 195 - Accenture Podcast Series: Why threat intelligence is your best defence - Accenture's new Cyber Fusion Centre, Sydney

Recorded at Accenture's new Cyber Fusion Centre in Sydney, we interview Joseph Failla, ANZ Security Lead and Managing Director of the Accenture Security practice for Australia and New Zealand and Mark Sayer, APAC Cyber Defence Lead for Accenture.

Episode 205 - Going Passwordless - Interview with Yubico's ANZ Country Manager

We missed timing this with World Password Day (May 7 - First Thursday of May) but took the opportunity to speak with Geoff Schomburgk, Australia and New Zealand Country Manager for Yubico. Geoff discusses the move towards a passwordless future and some of the key benefits and considerations for businesses and services looking to eliminate passwords.

Episode 188 - Hi-Tech Crime Trends of 2019 - Interview with Group-IB CTO & Co-Founder, Moscow

Jane Lo, Singapore Correspondent interviews Mr Dmitry Volkov, CTO and Co-Founder of Group IB on Hi-Tech Crime Trends of 2019.

Group IB, a Singapore-based cybersecurity company that specializes in preventing cyberattacks, has analyzed key recent changes to the global cyberthreat landscape. The report examines attacks conducted for espionage and sabotage purposes. The report contains chapters devoted to the main industries attacked and covers the period from H2 2018 and H1 2019. Group-IB analysts highlight key high-tech crime trends and conclude that 2019 heralds a new era of cyberattacks. The annual report was presented at CyberCrime Con 2019 international Threat Hunting and intelligence conference in Singapore (29th Nov 2019).

CYBER RISK MEETUP 2020

The Cyber Risk Meetup community has been enjoying it's busiest year diving into a high intensity of virtual events. The Mega C-Suite Series is now into Episode 7, meeting the World's First CISO in Steve Katz and this series is further supported with a Global Virtual Book Club and a Capture the Flag 'Cyber Range' event with partner, Security Innovation. Well done to Mimecast for their sponsorship of these core industry events.

Here's a taste of the events to date and to stay tuned for much more...stay tuned via the MySecurity Marketplace or visit www.CyberRiskMeetup.com



THE MEGA C-SUITE VIRTUAL MEETUP EDITION

CYBERRISKMEETUP.COM

What do you need to legally know, when your company is breached - Cyber Risk Meetup (Tokyo Edition)

In this 60 minute edition, Cyber Risk Meetup Tokyo Chapter host, Steven Li, spoke to Scott Warren to share the legal side of dealing with data breaches.

Scott Warren is a Partner in Squire Patton Boggs' Data Privacy & Cybersecurity practice in Asia and the Middle East. Mr. Warren has been working on digital data and data breach issues in the region for over 25 years, with over half of those years working in-house for Sega and Microsoft. He sits on the Executive Board of The Society for the Policing of Cyberspace (www.polcyb.org) and is a Certified International Counter-Cybercrime Professional. In this special virtual episode, we will explore how companies across the globe and in Japan are being impacted by data breaches legally, how trade secrets are at risk, some of the major laws and themes impacting your response, and provide you a strategy to prepare.

<https://anchor.fm/shamanetan>

Mega C-Suite Series, Episode 6: 'Hybrid Warfare: The Next Normal in Business Competition'

In this episode and candid conversation, Casey Fleming, Chairman and CEO of BlackOps Partners shared his views about the asymmetrical Hybrid Warfare where technology makes everyone a target and a weapon in a new kind of war. He also walked through some sensitive and confronting issues where state actors have been behind some of the most sinister and successful cyber-attacks and breaches.

Casey is recognised as a top expert, visionary, and keynote speaker for the leading strategic issue facing all organizations: new era, existential risk created by adversarial nation-states and groups. He regularly advises senior leadership of the private sector, Congress, Department of Justice, The White House, government agencies, the military, and academia on security strategy, cybersecurity, and national security.

Cyber Risk Leaders @ the Global Virtual Book Club

Have you ever wondered what does effective #leadership looks like during #crisis? What are the various ways for leaders to cope and stay calm in high stress situations? Or perhaps how can leaders encourage their team when it comes to learning and #innovation?

What are the important ingredients of building successful teams? In Episode 4, hosts Carmen Marsh, CEO of Inteligenca, and Shamane Tan, author of 'Cyber Risk Leaders' hosted a few very special guests from the US at the global #virtual Cyber Risk Leaders Book club.

Checkout their fireside chat with Theresa Payton, CEO of Fortalice Solutions, and first female #CIO at the #WhiteHouse, overseeing the IT operations for President George W.Bush, together with Jason Elrod, Exec Director at Sutter Health. This episode also enjoyed a sneak preview of Theresa's latest book: "#Manipulated: Inside the #Cyberwar to hijack elections and distort truths". Subscribe here so that you won't miss out on upcoming episodes:

Mega C-Suite Series, Cyber Risk Meetup Capture the Flag 'Cyber Range'

These Virtual Hackathons have been held in Australia and Singapore. Cyber Riskers were given the opportunity to join the leaderboard and test their skills on different challenges, and hundreds of intentionally vulnerable applications. All players receive a certificate of participation plus a swag boxes for the Top 10, and amazon gift vouchers for the Top 3.

CMD+CTRL Cyber Ranges are intentionally vulnerable applications and websites that tempt players to steal money, view their boss's salary, buy expensive items for free, and conduct other nefarious acts. Hundreds of vulnerabilities, common to most business applications, lay waiting.

For each vulnerability found, you'll score points and climb the leaderboard. All players have fun with exciting prizes & giveaways to be won! Worried you won't know what to do? Don't worry. They provide cheat sheets and tips to get you quickly ramped up.

Stay tuned for more!



Top trends that should inform your COVID-19 security posture



By

Linda **Gray Martin**,
Sr. Director & General Manager, RSA
Conference together with cyberse-
curity experts from RSA Conference
2020 APJ:

Paula **Januszkiewicz**,
CEO, Owner, Cybersecurity Expert,
CQUIRE

Magda **Chelly**,
Head of Cyber Consulting, Former
CISO, Entrepreneur, Marsh
Asia

Erich **Kron**,
Security Awareness Advocate,
KnowBe4

Javvad **Malik**,
Security Awareness Advocate,
KnowBe4

Stan **Lowe**,
Global Chief Information Security
Officer, Zscaler, Inc

Only months ago, businesses around the world had to make massive changes. The cause of those changes was so unprecedented that even those with strong incident response plans struggled to maintain their security posture amidst the challenges of an increased remote workforce.

The dust has started to settle, but hindsight tells us that we must do more to prepare for the inevitable: This—or something like this—will happen again. So how do organizations just entering the nascent stages of recovering from COVID-19 prepare for what will be a recurring issue? As we emerge from this first phase of this crisis, experts across the RSA Conference APJ program have weighed in on what's to come so that organizations can better understand the actions they need to take today to be ready for what will come tomorrow.

What's Trending Now?

So far, the biggest trend influenced by the pandemic is remote working and an increased usage of collaborative suite programs, said Paula Januszkiewicz, CEO, Owner, Cybersecurity Expert, CQUIRE. "Some companies had to adjust to the new reality rapidly. Luckily, all tools, which enable more than simple conversations, have become more

efficient in response to users' needs."

Though collaboration tools may have become more efficient, the sudden shift to a remote workforce exacerbated the challenges of defending the disappearing perimeter. Companies have been thrust into conducting business from multiple locations with little or no preparation, which will to continue to be the case post-pandemic, said Magda Chelly, Head of Cyber Consulting, Former CISO, Entrepreneur, Marsh Asia.

As the attack surface expands, companies and security teams will face new challenges, Chelly explained. "Attackers will be using multiple channels of communication with a focus on social media, all targeting end users dispersed across the globe, working from unsecured networks, and on their own devices. They will also be leveraging opportunities for physical attacks in empty offices."

Erich Kron, Security Awareness Advocate, KnowBe4 agreed that attacks have been increasing. Any emotionally charged situation opens the doors for social engineers to leverage different attacks from Phishing, Smishing, and Vishing to social media manipulation. In most cases, attackers are attempting to either get information or stir up chaos. "When people are in the midst of chaos, that impacts their ability to think critically. Getting somebody's emotional



“When people are in the midst of chaos, that impacts their ability to think critically. Getting somebody’s emotional state agitated puts them in a position where it is hard for them to make good decisions,”

state agitated puts them in a position where it is hard for them to make good decisions,” Kron said.

The Results of Cutting Corners

To enable remote work and move businesses online, many companies opted to cut some corners. They tweaked their policies and procedures in order to make things work, said KnowBe4’s Javvad Malik, Security Awareness Advocate.

For some that meant turning off 2FA. For others it meant leaving RDP ports open and exposed to the Internet. “In their efforts to try to keep the show on the road, they took shortcuts. As a result, they have accrued technical debt,” Malik said.

Organizations did what they needed to do to keep the business running. The issues now, Malik said, is that attackers know these weak points and will take advantage of them.

Boost Your Post-COVID Security

The past will repeat itself, so we need to think about architecture and the tools and technology that we put in place and determine what worked and didn’t work in order to adjust, said Stan Lowe, Global Chief Information Security

Officer, Zscaler, Inc.

Companies large and small will continue building out remote work capabilities as they are realizing it is more economical to pay for internet and cell phone services than to pay for square footage. “Companies are looking for ways to offset losses from this period of time, and they are going to be shifting spending, so we need to change the way we deliver IT and security for customers and employees,” Lowe said.

To secure a portion of that spending, security leaders need to ensure a seat at the table. How? Lowe said, “use this opportunity to show that you are a business enabler who can allow your organization to use the tools and technology to drive business revenue. You need to enable the business.”

Steps to Take Now


Organizations need to communicate with their people. “Help them understand how this works,” said Kron. “Make sure your people understand how changes are going to work. Educate people on phishing attacks so that they are on the lookout despite having those emotional triggers. Communication is the anti-disinformation.”

Cybercrime will continue whether businesses are operating remotely on a temporary basis or more permanently in the future. “Businesses need to ensure continuous cyber risk management and a non-traditional approach to perimeter defense,” Chelly said.

Go back and plug the holes. In order to augment their overall security posture for the future, it’s critical that organizations figure out what they did, why they did it, and what will happen if they take this versus that action to try and resolve it. “Companies haven’t thought that through,” said Malik. “Document all the decisions you are making—or go back and document the ones you’ve made—and identify why you did it and how you plan to reverse it.”

Additionally, it is important to ask how to securely collaborate in a remote environment. “The question grows even more difficult because people commonly combine their regular social activities with work-related ones while working from home,” Januszkiewicz said.

Over the past few months, we have all had to come to terms with the new reality. We must continue to rethink how we live, how we work and how we approach security and be able to adjust accordingly.

RSA Conference 2020 APJ will be returning as a 3-Day Virtual Experience designed to help the cybersecurity community move forward by bringing the power of learning to you. Register for the free virtual experience here. 



How to reduce work from home risks in a post-COVID world



By
Geoff Schomburgk
Vice President for Australia &
New Zealand at Yubico



**Episode 205 -
Going Passwordless -
Interview with Yubico's
ANZ Country Manager**

With vast numbers of employees now working from home, we have entered a new normal, and whilst a few people are now going back to their workplaces as restrictions ease, many office workers are likely to continue to work from home for the rest of the year. The technology giants like Google, Microsoft, Facebook, Amazon, Slack and Twitter have all made this move with some saying it has proven to be just as productive as the traditional office. These innovative market leaders often set the standards for best practices, which could influence how other companies develop their secure work from home strategies going forward.

Whilst Australian organisations continue to navigate this difficult time — focusing on maintaining productivity, boosting employee morale, and equipping remote teams with the software and tools they need — many companies are also thinking about how this ‘new’ way of working will change their business for good and accelerate their path to digital transformation. James Calder, the global director of Woods Bagot-owned office design consultancy, Era-co has said that hot-desking, shared kitchens and crowded public

transport are a thing of the pre-COVID era and he said: “It’s the end of activity-based work as we know it.”

One thing is certain; as more core business functions and applications move to the cloud, a strong, yet flexible, security foundation is critical to reducing risk exposure for an organisation. In fact, we’re seeing this now.

Working from home introduces new complexities that aren’t typically present in a secure and trusted office environment. Managing access to essential corporate applications, while also adjusting to rapidly support a remote workforce, has been challenging for many companies and rightfully so. When supporting a remote workforce, there is more ambiguity and uncertainty of an employee’s environment, making it critical for organisations to re-establish trust with their users and the devices they’re using.

Back to the basics with two-factor authentication

How do you ensure individuals accessing your IT systems are really who they say they are? You lock the front door.



It's a simple concept that's often forgotten, but if your organisation has a complex security infrastructure complete with firewalls, end-to-end encryption, virus scanning and more, it's irrelevant if you haven't first safeguarded your access points with strong authentication.

Two-factor authentication (2FA) plays an important role as the first line of defence against phishing scams, credential stuffing, or man-in-the-middle attacks. But not all 2FA is equal. When considering a 2FA method, it's important to understand that there are varying levels of effectiveness.

SMS codes can be compromised by SIM swapping and number porting scams, while one-time passcodes on authenticator apps can be inconvenient and impede productivity. In fact, research proves that SMS and mobile authenticators are not as effective at preventing account takeovers and targeted attacks as other methods like security keys. Security keys leverage open authentication standards, like FIDO2 and WebAuthn, to provide the highest level of security assurance while also providing a seamless user experience.

Regardless of the 2FA method you believe is best

It's a simple concept that's often forgotten, but if your organisation has a complex security infrastructure complete with firewalls, end-to-end encryption, virus scanning and more, it's irrelevant if you haven't first safeguarded your access points with strong authentication.

for your organization, it's important to implement it for all employees, across all systems and applications. It is the single best step you can take to drastically improve your security posture with little effort. For many enterprises, my best recommendation is to turn on 2FA with these three business-critical tools.

1. Identity and access management systems (IAM) and identity providers (IdP)

Access management tools are a good place to start when enforcing 2FA. Most organizations already leverage an Identity and Access Management (IAM) solution or identity provider (IdP) — whether it's Google, RSA, Microsoft, Okta, Ping, Duo, or something similar — to streamline access and reduce the hassle that comes with multiple logins. Combining an IAM service with strong 2FA results in a winning joint solution that can immediately improve an organisation's security posture by protecting all business-critical applications with a single point of sign-on.

2. Virtual Private Network (VPN) solutions

In the age of remote work, it's important for organisations to ensure employees are using a secure network. With a VPN, only permitted users are allowed to access the data being transmitted, which is why accessing a VPN can be risky when relying solely on passwords. Leveraging 2FA will help to secure VPN access from malicious attackers.

3. Computer logins

With the influx of remote work, many users are using their personal devices for work-related functions or work devices for personal use. In a perfect world, users should designate the appropriate devices to either work or personal use only, but that is not as realistic as it sounds. If devices like laptops and desktops are not secured properly, they can be potential entry points for external threats. Protecting computer logins with 2FA is a tactic that can help safeguard devices from unwanted access or misuse.

With the current climate, there are many unknowns, but the security infrastructure doesn't have to be one of them. By taking the necessary precautions, like setting up 2FA wherever possible, an organisation can continue business operations with the majority of its workers at home while also having peace of mind regarding security. ▲

**COVER
FEATURE**

Does COVID-19 signal the end for fingerprint recognition?

By
Michael Warnock,
Head of Growth
APAC at SecureAuth

While COVID-19 has thrown doubt and uncertainty onto almost everything, one thing is for certain – we have never been more conscious of where our hands are going. The incessant reminders to ‘wash your hands’ have highlighted how easily germs are picked up and transferred by touching and there’s been a rapid adoption of contactless...well everything really. Contactless deliveries, contactless medical appointments, even contactless schooling, the list is endless.

At some point, the threat posed by COVID-19 will recede, and people may resume shaking hands and hugging each other. By then, however, the habits we’ve formed and the innovations developed now to build our new contactless economic system will have taken root.

So what does that mean for touch-based technology such as fingerprint recognition security systems commonly used on smart devices, building management systems, border control and the like? In New York City, the NYPD stopped employees from using the fingerprint entry security procedure but does COVID-19 really herald the end of fingerprint recognition?

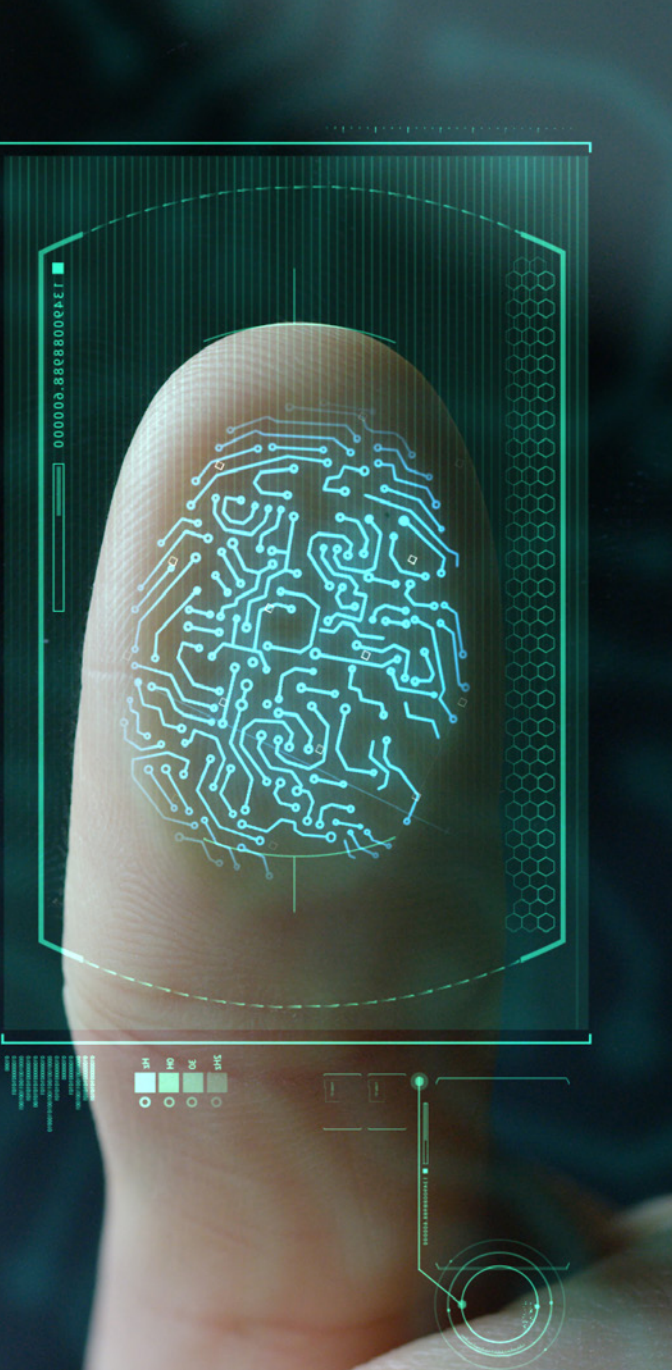
Up the hygiene ante

Fingerprint recognition is a secure and convenient technology that has become common and widespread and in the short-medium term remains a key part of many robust security systems. With that in mind, sensible use of the technology can help to significantly prevent the spread of germs

Contact with fingerprint recognition is different from touching other surfaces in that it involves intended, mindful contacts, as opposed to surfaces such as the poles in buses and trains, elevators, ATMs, door handles, handrails, tables, credit cards and money which come in contact with countless people. This means we can help protect ourselves by keeping hand sanitiser next to fingerprint recognitions sensors and directing people to use it before and after touching the sensor.

Multifactor authentication

The sudden shift to remote working due to COVID-19 has seen many businesses grappling with their existing security



'China (Hong Kong and Guangdong Province), Japan, Singapore, Thailand, and Vietnam via a 9,400-kilometer submarine cable through the South China sea. '

smartphone or laptop is reasonably low given those devices aren't being touched by multiple people.

With COVID-19, has come an influx of new cyber attacks. With recent reports indicated that in the month of March, coronavirus-related phishing attacks went up 667%, and every single country around the globe has now been hit with at least one phishing attack related to the pandemic. So, in the current landscape, the security benefits associated with multi-factor authentication will far outweigh any potential risks associated with fingerprint recognition.

The rise of contactless biometrics

However, longer term, we will see an increased focus on contactless biometrics as part of multifactor authentication and other security systems such as entry management.

As a result of COVID-19, we have seen a surge in biometric and AI technologies being developed to help monitor the spread of the disease. Thermal cameras being installed in airports and facial recognition that works even when a person is wearing a mask have been developed rapidly and these leaps in innovation will be adopted more widely. Contactless fingerprint recognition, iris scanning and face detection will become the biometrics of the future.

There's no doubt COVID-19 has changed the way we live and work irreversibly. Fingerprint recognition technology will be around for a while yet, but we do need to be mindful of how we use it and, as with anything, practice good hygiene.

Longer-term, there will be extra layers of authentication, more security built into the devices we use to access systems, and contactless biometrics will become commonplace. ▲

procedures in an attempt to keep corporate data secure. According to the Australian Cyber Security Centre, "Multi-factor authentication is one of the most effective controls you can implement to prevent unauthorised access to computers, applications and online services. Using multiple layers of authentication makes it much harder to access your systems. Criminals might manage to steal one type of proof of identity (for example, your PIN) but it is very difficult to steal the correct combination of several proofs for any given account."

Traditionally, multi-factor authentication uses a combination of:

- something the user knows (a passphrase, PIN or an answer to a secret question)
- something the user physically possesses (such as a card, token or security key) and
- something the user inherently possesses (such as a fingerprint or retina pattern)

Fingerprint recognition is an integral part of many multi-factor authentication technology and the risk of the spread of disease by using it on a personal device such as a



Coronavirus victims of a different nature: The targets of COVID-19 cyberthreats



By
Leslie F. Sikos, Ph.D.,
Dr. Sikos is a lecturer in
computing and security,
specializing in network
forensics and cybersecurity
applications powered by
artificial intelligence and
data science.

The novel coronavirus disease (COVID-19) outbreak, declared by WHO as a global pandemic on 11 March 2020, resulted in panic, uncertainty, and fear, which are exploited by threat actors for phishing and data exfiltration, and malware distribution. In addition, the massive increase of remote workers, many of whom apply poor security measures on their computing devices, opened new avenues for exploitation. Opportunistic fraudsters distribute misinformation and fake safety advice, often with malware, request personal data for providing allegedly up-to-date information on COVID-19, or try to convince people to perform financial transactions, in particular through purchasing bogus products (fake cures). For example, a purported COVID-19 alert, seemingly sent by the WHO, is actually a spam that distributes a new variant of the HawkEye keylogging malware.

As Interpol warned about financial fraud linked to COVID-19, “criminals are exploiting the fear and uncertainty created by COVID-19 to prey on innocent citizens who are only looking to protect their health and that of their loved ones”. The list of cyberthreat types associated with

coronavirus includes a wide range of fake products and scams, from bogus Starbucks gift cards to vacation scams, and from bogus property rentals to mobile apps, such as CovidLock, which seemingly serves the purpose of tracking the spreading of the coronavirus, but is actually an Android ransomware. ZDNET reported that thousands of COVID-19 scam and malware sites have been created. This is already evidenced by legal actions, such as the restraining order of the US Federal Court against a website offering fraudulent coronavirus vaccine, however, many of such websites are live and their number is still on the rise.

In Australia, Scamwatch of the Australian Competition and Consumer Commission (ACCC) received reports of COVID-19-themed scam texts sent to members of the public. Telstra warned people about fake SMS messages sent on COVID-19 testing, and reported scammers providing fake phone support by pretending to be a staff member of Telstra, NBN, or Microsoft. 9News reported flight cancellation scams, while Moneysmart of the Australian Government warns about superannuation scams. In New Zealand, the Financial Markets Authority (FMA) reported

investment scams related to goods in great demand, such as sanitary products. Fake coronavirus maps are emerging, along with text message scams and phishing emails claiming to have updated COVID-19 information.

In China, online scammers taking advantage of the community fears created a shortage of face masks, while a social engineering attack has been impersonating the Mongolian Ministry of Foreign Affairs in the form of press briefings. In Hong Kong, the police force issued a scam alert due to phone scammers posing as government officials telling “anomalies” in their health, only to try them divulge their bank details. In South Africa, a scam appeared about the Reserve Bank allegedly collecting “contaminated” banknotes and coins. In Europe, rogue traders started advertising and selling products, such as hand sanitisers to consumers, putting the European Commission on high alert. In the US, government-issued relief fund (stimulus package) emails have been circulated, asking for personal information, and scammers try to trick people into reserving a COVID-19 vaccine over the phone. Other types of cyberthreats include fake fundraising and scammers impersonating the WHO for donations, and COVID-19 testing kit scams. According to YouMail, Americans receive 1M+ robocalls daily, some of which offer non-existing at-home coronavirus testing products. In Canada, scam sites selling cleaning products to “super-clean your house or office” appeared along with, according to the Canadian Anti-Fraud Centre, “special” air filters to protect from COVID-19; fake lists of COVID-19-infected people in the vicinity, seemingly from the Centers for Disease Control and Prevention; and fraudsters posing as agents of the Public Health Agency of Canada, tricking victims into confirming health card and credit card numbers for a prescription.

These are just some of the examples of cyberthreats related to COVID-19, the variety of which makes it necessary to be sceptical and vigilant, and never click on suspicious links or open suspicious attachments. Having security protection (antivirus, firewall, frequent updates, multi-factor authentication, regular backups, using company VPN, etc.) for our computing devices is fundamental, but this has to be complemented by user awareness. As a general advice, look carefully to spot signs of scam including, but not limited to, wrong addresses, misspelled domains, and misleading URL names. Even if an email appears to be sent by a legitimate organisation, such as the government or the WHO, keep in mind that logos and branding can be faked, and email headers spoofed (e.g., appears to be sent from donate@who.int). Requesting a payment related to COVID-19 via Bitcoin is always a red flag. Missing the appropriate license required for providing a financial service, whether banking, superannuation, or investment, can indicate fraud, which can be prevented by looking up the relevant government website, such as the ASIC website, and search for the company in question. Taking tough security measures to fight cybercrime related to the novel coronavirus pandemic is particularly important, considering its global presence and potential impact, and the exponentially increased number of people working from home in these hard times. ▲

'In China, online scammers taking advantage of the community fears created a shortage of face masks, while a social engineering attack has been impersonating the Mongolian Ministry of Foreign Affairs in the form of press briefings.'



Listen Now: Episode 189
ECU launches new Security Operations Centre with RSA Security – building renewed tertiary focus on cybersecurity skills training



Bringing all of the MSM channels together on one platform for the latest and greatest in security, technology and events from across the Asia Pacific and the world. Now available on Apple and Android platforms.



A dedicated channel for Boards, C-Suite Executives and Cyber Risk Leaders to highlight cyber threats as a key business issue.



The Australian Cyber Security Magazine was launched in agreement with the Australian Information Security Association (AISA) to be focused on AISA's 3,000 members, nationally and forms part of AISA's national cyber security awareness and membership communication platform.



MySecurity Media can facilitate specialist round-table luncheons or breakfast sessions for up to 20 invited guests for high level discussion on Security & Cybersecurity themes, guided by the Vendor's Leaders and accompanied with published content.



Dedicated channel for all things about Drones, Robotics, Autonomous systems, Technology, Information and Communications



The region's newest government and corporate Technology and Security magazine, with a focus on the Southeast Asia region and the 10 ASEAN member nations



Commenced in November 2017, the Cyber Security Weekly Podcast has surpassed 120 interviews and provides regularly updates, news, trends and events. Available via Apple & Android. Over **55,000** downloads in the first year.



Event opportunities in Sydney, Melbourne, Brisbane & Singapore providing attendees a special experience and additional takeaways, including podcast interviews and print media.



The Australian Security Magazine is the country's leading government and corporate security magazine. It is published bi-monthly and is distributed to many of the biggest decision makers in the security industry. Provoking editorial and up-to-date news, trends and events for all security professionals.



My Security Media rapidly expanded into the Asia Pacific Region with its sister publication – the Asia Pacific Security Magazine. It is published bi-monthly. It is available online to read by all and upon every issue release a direct link is sent to a database of subscribers who are industry decision makers.



Technology channel partner ecosystem platform with a natural focus on Big Data, Internet of Things and fast emerging technologies



The MySecurity TV Channel delivers news and interviews for the Asia Pacific Security Magazine, Australian Security Magazine and Australian Cyber Security Magazine – and from across MySecurity Media channels.

CYBER RISK LEADERS

IMMERSE YOURSELF IN THE WORLD OF A CISO (CHIEF INFORMATION SECURITY OFFICER)

"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."

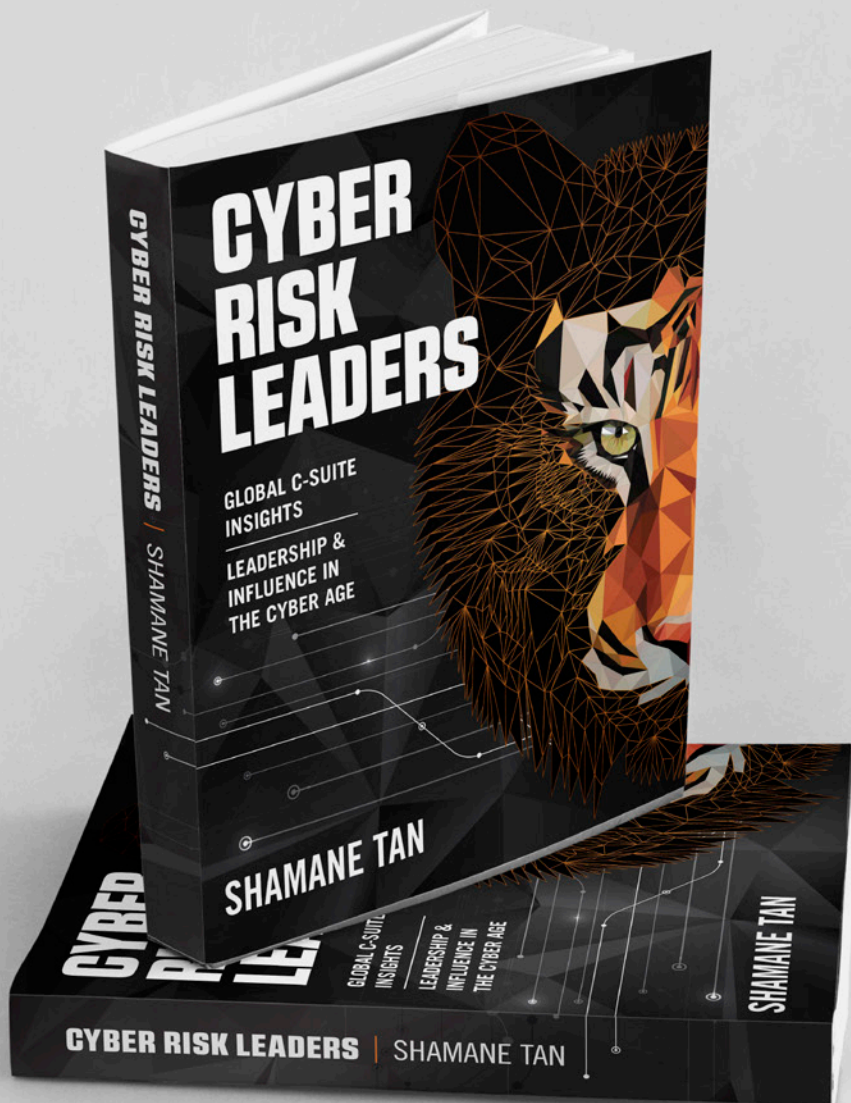
I loved her unique voice, highly readable style, and wholeheartedly recommend this book."

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





The law on cyber bullying and trolling



By
Brenda van Rensburg

Over the past couple years, we have seen a rise in both cyber bullying and trolling. According to 'NIH', cyberbullies are hidden behind a screen and thus have little remorse for their victim. Unfortunately, many of us has been on the receiving end of a person with malicious intent. Is there legal recourse for someone who has been on the receiving end of a troll or cyber bully? This article will compare a Troll to a Cyber Bully and discuss some legal approaches for both.

It is important to recognize a cyberbully from a troll. The reason is that you can quickly identify one from the other and apply some recourse. From a broad view, cyberbullying and trolling have no significant difference. In both cases, the initiator purposely uses an online medium to create a negative response. However, when you apply a narrower interpretation you will find that the cyber bully's goal is focused on intent to create harm whereas the latter has intent to disrupt a community with negative commentary.

Trolls are attention seekers. Their goal is to turn a 'commentary piece' onto themselves by creating provocative comments. The more attention they receive from a site, blog, or post, the happier the troll. In short, they are a nuisance to a community.

Cyberbullies prefer to target a person or persons. Their intent is to intimate, shame, and harm their victim. They prefer to 'hide' in the cyber space and do not like any attention drawn to them. They generally have a 'pseudo-name' and will post photos, videos or extremely 'mean-spirited' messages about an individual. All a cyberbully wants is to distress their victim possibly into suicide. According to Frontiers in Psychology, there is a high

percentage of cyberbullies in schools. However, anyone can become the victim.

LEGISLATION

The term cyberbully is not defined within an Australian statute. However, this does not mean that cyberbullies are not 'dealt with' by the law. Cyberbullies can be convicted under several piece of legislation and many are being convicted.

One of the most asked questions is whether a cyber bully can be convicted? If you think about it, a cyberbully is an 'online assault'. However, can you convict a cyberbully under Assault? The elements to convict under assault (WA Criminal Code Act) is:

1. Force – Applied or Threatened
2. Without Consent
3. Intention
4. Unlawful

Unfortunately, the first element may be challenge as the statue states that "A person who strikes, touches, or moves, or other otherwise applied force of any kind to the person of another, either indirectly or directly..." The argument is challenged on the fact that force was not necessary applied. It is generally the victim that applies a force to themselves. Naturally, you could look at 'Threats' as expressed by the cyberbully. However, the elements of s. 338(a) is 'a threat to kill, injure, endanger or harm any person'. Threatening to expose several videos or photos online does not satisfy any of these elements.



In 2013 a person aged between 19 and 21 (the crime was committed over time) was convicted of cyberbullying under the Criminal Code Act (WA) s. 204: 'Indecent act with intent to offend'. The respondent (the person who committed the crime) was charged for offending five girls aged between 13 and 15 years. The respondent threatened girls, unwillingly, into 'sexual acts.'. Things escalated whereby the respondent threatened to share video footage if they did not do as he said. Notably the federal police were brought in, the perpetrator was convicted, an appeal was made, and the appeal was dismissed.

So how do we legally tackle a cyberbully who believes they are invincible to the law? Cyberbullying, generally, uses mobile phones, emails or even social media sites. To harass or abuse a person, or group of people, could be a criminal offence under the following pieces of legislation.

1. Menace, harass or cause offence using the internet: Criminal Code Act 1995 (Cth) s. 474.17: 'Using a telecommunications network with intention to commit a serious offence'.
2. Intimidating or Threatening Conduct: Criminal Code Act 1995 (Cth) s 474.15: 'Using a carriage service to make a threat'.
3. For Sexual Threats and Intimidation: Criminal Code Act 1995 (Cth) s.474.17(A): 'Aggravated offences involving private sexual material—using a carriage service to menace, harass or cause offence.'
4. To encourage suicide: Criminal Code Act 1995 (Cth) s. 474.29(A): 'Using a carriage service for suicide related material'.

AUSTRALIAN STATES AND BULLIES

Some Australian states are making huge strides when it comes to Cyber Bullying, especially within schools. An argument has been raised on whether schools should be held responsible for the actions of children online as extension to 'Duty of Care'. However, setting the 'precedent' so to speak is New South Wales who have amended their Criminal Code to accommodate suicide.

According the Crimes Act 1900 (NSW) s 60E, Assaults etc at schools: 'A person who by any means... (b) is reckless as to causing actual bodily harm to that student or member of staff or any other person'. The person is 'the student or member of staff is attending a school'. A person can receive up to 12 years imprisonment.

WHAT TO DO

Cyberbullying can be tried under the criminal code. However, by the time it reaches court the effect of the bullying which could have resulted in horrific ending to a victim. Notably, what will follow is a series of discussion within government about online crime. Until formal legislation is introduced, other than sections of legislation which can be applied now, there will be many more victims with many more perpetrators escaping the law.

The first step, however, is to recognize the perpetrator. Is this person a Troll or a Cyber Bully? Remember, a troll is focused on themselves. They will normally post comments on a post to initiate negative action. Things you can do is to not engage with their comment, delete their comments, or notify administration of the site that you are experiencing menacing behaviour.

A Cyber Bully, on the other had is much more sinister. If you feel you are being cyber bullied, you should seek advice either from the police or a lawyer. Being threatened or 'assaulted' online, is not acceptable, no matter the age of the individual. Notably, there are several contentious factors that could come into play which a lawyer could help you navigate through. Arming up with the law is possible one of the best defences against a cyber bully and a troll. However, it is important to know that parents and children should not feel helpless, alienated or intimidated by a cyber bully. There are a number of sites you can turn to for help such as the 'Kids Helpline' (www.kidshelpline.com.au). Alternatively, you can also ask your local police for guidance. Or, you can seek the guidance of a lawyer. But, whatever you do, NEVER deal with a cyberbully by yourself.

About the Author

Brenda is the head of Data Security for Terrene Global and international keynote speaker. Her experience across a spectrum of industries from Legal, Financial to Resources has given her an in-depth knowledge of how to relate corporate governance, enterprise risk management and cyber & data security management to directors, C-level executives, and all employees within organizations. She is currently completing her law degree to compliment her technology skills so that she can add value to current, and future, issues facing our community and legal industry.▲



Why domestic violence is a workplace issue.



By
Nick de Bont

Nick de Bont has worked within security related fields in both private enterprise and government for 20 years and has built domestic and family violence related security programs within private industry. He is a certified protection professional (CPP), holds a Bachelor of Laws, Bachelor of International business and diplomas in postgraduate law, intelligence analysis and security and risk management.

Domestic and family violence is a workplace issue. It has far reaching effects on victims and those they work with, it significantly impacts the productivity of staff and can lead them to prematurely leave their jobs, it affects colleagues and also consumes significant time for managers and human resources professionals. The vast majority of people who suffer from domestic or family violence are in paid employment[9], yet the role of employers in addressing the issue is still not well defined in Australia.

There is no socio-economic limit to domestic and family violence - victims are found in blue collar or white-collar workplaces, and can be young or more mature in age. Since the age of 15, one in six Australian women and one in 16 men have been subjected to physical and/or sexual violence by a current or previous cohabiting partner, and approximately one woman is killed every week and one man every month by a current or former partner often after a history of domestic violence.

Political, societal and culture attitudes are changing - a number of large Australian businesses have now implemented special leave provisions for employees who may require it due to domestic and family violence. This is aimed at facilitating time off to attend court, moving from

their family home, visiting a doctor and engaging with lawyers. These developments indicate a slight but important change – that is, recognition that the domestic and family violence is not only a private issue, and that employers can play an important role in ensuring the safety and security of their staff both at work and at home.

With the increasing trend of working from home and restrictions on travel and business trips there is increased pressure on those facing domestic and family violence who now have less opportunities to escape abuse. As businesses examine more permanent working from home solutions they must consider their ongoing workplace health and safety obligation to provide a safe place to work. The correct desk height and a suitable chair checklist may not seem as critical to an employee where a business is asking an employee to work in a hostile and abusive location. Managers must consider how they can provide those suffering domestic and family violence appropriate support and implement policies where an employee feels safe to raise this sensitive and deeply personal issue.

How can companies support their staff facing domestic and family violence

As companies begin to provide special leave, another way in which employers can provide significant support is

'Australian police deal with 5,000 domestic violence matters on average every week. That's one every two minutes'

often overlooked. Many large companies within Australia employ corporate security professionals, and although their role and remit vary, a substantial part of their role is ensuring employees are safe and feel safe in the workplace. The involvement of corporate security professionals in the area of domestic and family violence can enhance staff safety at home and helps protect colleagues and customers in the workplace. The threat of an active assailant in the Australian workplace is very low, yet many businesses have drafted emergency plans, paid consultants for reviews and even conducted training for staff. But in comparison the threat of a family violence matter spilling into the workplace is significantly more likely for almost every workplace in Australia yet many businesses have limited controls for this more likely threat.

This current disconnect is due to the powerful emotive narrative of terrorism where many people see the likelihood as significantly higher than reality. Employees in the Australian workplace are much more likely to be assaulted, abused or attacked due to being indirectly targeted due to a domestic or family violence matter than any form of terrorism. This powerful narrative for terrorism can be compared with the discomfort of many to even talk about domestic and family violence and a cultural belief this

remains a personal issue.

Whilst some research has been undertaken overseas, there has been little on the threats of family violence to the Australian workplace or the prevalence of employees being targeted whilst at work. Research from the US has showed that 95% of women who are stalked by a violent partner, experience harassment and disruption at their place of work.[12] Conversations with a number of security professionals reveal it is common for partners to attempt to locate the target of their abuse in the Australian workplace. Many cite examples of individuals trying to social engineer information from other staff over the phone, tailgating to pass building security barriers, regular abuse delivered via company email and phones, stalking in foyers and car parks and installing malware on mobile devices to track and listen in. In some cases, corporate professionals reported incidents of significant threats and violence, including assault on other staff. Both the businesses involved and the victims want to avoid any media attention resulting in almost none of these instances being publicly reported.

Employers have an obligation to provide a safe workplace and the threats posed by family violence can have both their likelihood and impact reduced by effective security controls. Involvement of private security professionals and working with law enforcement, will ensure those staff who are affected are better protected as well as ensuring the safety of their colleagues, managers, visitors and customers.

Not just a matter for law enforcement

A line often touted is that domestic and family violence is a police matter. Australian police deal with 5,000 domestic violence matters on average every week. That's one every two minutes. The workload for law enforcement is overwhelming requiring them to prioritise emergency cases and those with clear indicators of a pathway to violence. As with many areas of law enforcement private security professionals can play a role in providing a valuable supporting role to ensure the staff in their workplace are safe and protected.

There is and will continue to be a reluctance from many corporate security professionals to become involved in advice to those affected as it is a high stakes matter – wrong or ineffective advice could place someone in more danger. However, many in these positions are highly trained with diverse backgrounds, and furthermore there are sources of training and advice available for those not so confident to upskill. It is important to ensure security staff involved are appropriately trained and skilled, and avoid assumptions they will be effective based purely on their background or job titles. Domestic and family violence is a very emotional and challenging topic for individuals to talk about, and only highly skilled corporate security professionals can avoid the risk of enhancing trauma and exasperating a situation, assessing the risk to both the individual and the workplace and advising on effective controls. ▲



BOOK REVIEW | BY CHRIS CUBBAGE

CONTEST FOR THE INDO- PACIFIC WHY CHINA WON'T MAP THE FUTURE RORY MEDCALF

'A fast-paced and fascinating guide to this vital strategic concept.' —Gideon Rachman, author of *Easternisation*

CONTEST FOR THE INDO-PACIFIC, WHY CHINA WON'T MAP THE FUTURE

By
Rory Medcalf

Thanks to ANU Media for providing a copy to review.

By
Chris Cubbage,
Executive Editor, MySecurity Media



Check out the
Podcast here

PODCAST

www.blubrry.com/mysecurity

"China and the United States have entered a state of comprehensive struggle, amounting to full-spectrum rivalry. The Pentagon publicly labeled China a strategic competitor, and a series of blunt speeches in 2018 and 2019 by US vice president Mike Pence confirmed that this assessment has permeated America's China Policy. The situation could deteriorate through miscalculation or confrontation." (*Contest for the Indo-Pacific, Why China won't map the future*, page 20)

At the start of 2020, the world was amidst an industrial technology revolution and major power contestation, dealing with significant and rapid change – including to the global climate. The situation has since been exacerbated by a global pandemic, destabilising the world economy. The circumstance is that the deadly novel coronavirus originated in Wuhan, China. There are serious questions over China's governance and transparency in how the virus was identified and managed. In this context, this book has a sharp, indeed, pinpoint focus.

Released at such a unique and 'unprecedented' time in modern human history, Medcalf makes more than mere mention of 'black elephant' events which may arise. COVID-19 is one such black elephant – "a likely event – and a bad one – that everyone sees looming yet still comes as a shock."

Medcalf uses descriptors of China with reference to its; 'perilous momentum', 'global power ambitions'; and being 'excessive and coercive.' Hence, Medcalf's historical context across the opening three chapters is critical to setting the scene of today. In addressing the present geo-political theatre, captured in Chapters 5 – 8, at the time of his writing, the present was absent a global pandemic. In his single, final Chapter outlining the future – appropriately titled, 'Navigating Mistrust' - Medcalf leaves the reader assured the future is to be very different than today. To highlight his insight further in the current context, he makes an appropriate mention of China's links to 'disease outbreaks'.

A former intelligence officer, now based at the Australian National University, Rory Medcalf has displayed himself as a leading Australian intellectual. An esteemed researcher and an immensely talented writer. Though taking enjoyment in reading this work, I'm left wondering if this book was motivated more towards countering China's own propaganda machine and uttering the voices of Australian leaders and policy makers.

Flipping over to the back-cover summary, the book's foray opens with, "The Indo-Pacific is both a place and an idea." Having been the editor and publisher of the *Asia Pacific Security Magazine* since 2011 and in 2012 published a book with CRC Press, *Corporate Security in the Asia Pacific Region*, I have stubbornly resisted the term, 'Indo-Pacific'. The term appears academic and came increasingly applied as Western propaganda against China. Indeed, Medcalf notes this is precisely how it is perceived, confirming at the outset of the book, "Certainly China feels risk

and discomfort in the term."

Despite my personal view and semantics around the term used for the region, this book is deeply important. The title itself is provocative by proclaiming the book's intention. To send a message to the Chinese Communist Party that the change in terminology from Asia-Pacific to Indo-Pacific, was and remains a message to China that it has a group of competitors and faces resistance - arched over by the US and India and muddled together by "middle players" of Australia, Japan, South Korea, Singapore, Vietnam and most conspicuously, Taiwan. He makes the point that "the intention of other countries should be to make China think twice."

I appreciate how Medcalf seeks to establish and explain the foreign policy shift Australia has made and how the term 'Indo-Pacific' has much deeper meaning and intentions, over that of retaining the status quo of 'Asia Pacific'. Despite a series of defence and foreign policy white papers since 2012, the Australian public have been poorly kept informed, or have not appreciated the significance of such a rapid, tectonic policy shift. This book greatly contributes to this education, which frankly, has been severely lacking.

Regrettably, this book may also provide the Chinese Communist Party with the recipe for success. As a worst-case scenario, it provides sufficient basis to allege China may well have been motivated to use a biological weapon like COVID-19 in order to significantly destabilise the West – which is what has been achieved. Medcalf highlights China's failings and weaknesses, as well as the potential strength from a collective alliance of middle players. China is hereby greater informed of how the West is thinking and how itself can use this knowledge to its benefit. Including the use of asymmetric, 'full-spectrum' warfare.

Medcalf develops four key factors which, he notes, "combine to project a shadow of imperial over-stretch. China will face extensive security tests across the vast Indo-Pacific, regardless of whether America sustains full-spectrum strategic rivalry. China will keep provoking anxieties from India and other consequential nations. Sooner or later, Beijing's decision makers - in a moment either of confidence or nervousness – will likely authorise military action in one or more far-off places, with consequences hard to predict or control." With hindsight, COVID-19 fits with this scenario. Has the West underestimated China's intent on global power?

Taking the view with Medcalf's historical lens, military conflict appears inevitable – it will be a matter of how far the conflict extends. With that in mind, Medcalf sends a critical message, supported by a number of national security observers – "it's time for government and business to brace and hedge, to prepare for the risks of multiple plausible futures."

Definitely a recommended read during a time of pandemic isolation and day by day, rapidly increasing tensions and vulnerability in the region. ▲



REPORTS

Search and find all upcoming featured security reports

 <p>Bring Your Own Device. Bitglass' 2020 Personal Device Report</p> <p>Thu, Jul 09 Free Direct Download</p> <p>Bring your own device: Bitglass' 2020 Personal Device Report Bitglass</p>	 <p>eSafetyresearch</p> <p>Covid-19 impact on Australian adults' online activities and attitudes June 2020</p> <p>Wed, Jul 08 Free Direct Download</p> <p>How COVID-19 impact on Australian adults' online activities and attitudes eSafety Commissioner</p>	 <p>FORESCOUT</p> <p>The Enterprise of Things Security Report The State of IoT Security in 2020 by Forescout Research Labs</p> <p>Mon, Jun 29 Free Direct Download</p> <p>The Enterprise of Things Security Report Forescout</p>	 <p>TRUSTWAVE SPIDERLABS INVESTIGATION</p> <p>The Golden Tax Department and Emergence of GoldenSpy Malware HOW REQUIRED TAX SOFTWARE PROVIDES A HIDDEN BACKDOOR INTO VICTIM NETWORKS</p> <p>Fri, Jun 26 Free Direct Download</p> <p>The Golden Tax Department and Emergence of GoldenSpy Malware Trustwave</p>
---	--	---	--

Plus many more!



THE 'GO-TO' TOOL FOR LEADING PROFESSIONALS



- ✓ **WEBINARS**
- ✓ **WHITEPAPERS**
- ✓ **UP COMING EVENTS**
- ✓ **CONFERENCES**

SEARCH THE MARKETPLACE

[ALL](#) [EVENTS](#) [COURSES](#) [WEBINARS](#) [REPORTS](#) [BOOKS](#) [WHITEPAPERS](#) [SOLUTIONS](#)

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

SEARCH



COVID-19 RESOURCES
FOR SECURITY PROFESSIONALS

[SEE MORE](#)

www.mysecuritymarketplace.com