CYBER RISK LEADERS

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

Issue 4, 2021

Education is Essential for ICS Cyber Security Preparedness

Trump's final day executive cybersecurity order – what does it mean?

WhatsApp data sharing policy

Biden's new US defense secretary and impact on the space race

Container Forensics

Zero Trust in a SASE architecture

The New Face of Money

Make digital risk part of the board discussion

Embracing digital identity

Security versus agility

WHY 5G MATTERS

IN A WORLD OF IOT, VR, AR, AI & EDGE

PLUS

Cyber Security Weekly Podcast

MySec.TV

Cyber security weekly highlights

INDO-PACIFIC INTERVIEW SERIES

GEOFF RABY AO | PROF. JOHN BLAXLAND | ZACK COOPER

Is your network security strong enough to combat the added risk of the remote workforce?

For more information on these and other best-in-class solutions
1300 HILLS1 (445 571) or **hills.com.au**

Follow us on | Hills Limited

YOU CAN RELY ON HILLS

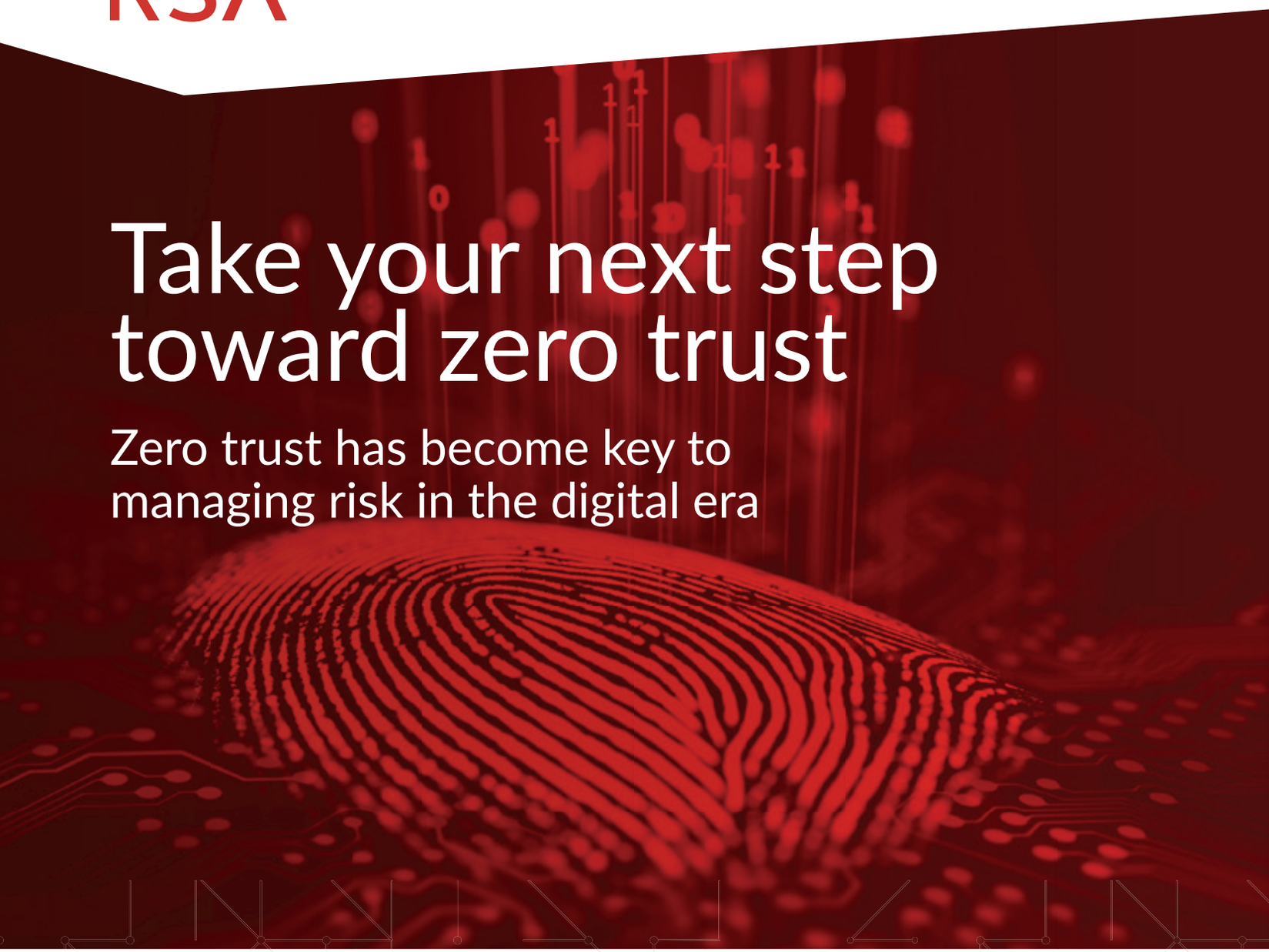
SONICWALL™ | HILLS™

SASE Security With True Data Protection

Make SASE real for your organisation.

forcepoint.com

RSA



Take your next step toward zero trust

Zero trust has become key to managing risk in the digital era

One of the critical factors in adopting a zero trust architecture like NIST is to have a mature and comprehensive identity and access management program. Establish and enforce zero trust access policies, manage user identities and access, and implement modern, risk-based multi-factor authentication with RSA SecurID® Suite.

Contact us to learn more about how we are enabling our customers in their journey toward a zero trust environment.

rsa.com/contactus

RSA SECURID® SUITE

AUSCERT2021
Cyber Security Conference
20 YEARS

20th Annual AusCERT Cyber Security Conference

SOARing with Cyber

11th - 14th May 2021 // The Star Hotel, Gold Coast, Australia

4 DAYS

50+ SPEAKERS

IN PERSON & VIRTUAL

Keynote Speakers

Ciaran Martin
UNIVERSITY OF OXFORD

Maddie Stone
GOOGLE PROJECT ZERO

REGISTER NOW >> conference.auscert.org.au

MYSECURITY MARKETPLACE

CYBER WARS

COLLECTION

An exclusive collection created for cybersecurity awareness

SHOP NOW

www.mysectv.shop

Learn to defend and understand your critical infrastructure.

MYSECURITY MARKETPLACE

SCADA & ICS CYBER SECURITY COURSE

5th April – 30th April, 2021

REGISTER INTEREST HERE

COURSE COST

ALL SESSIONS $625.00 ex GST*

**Prices ex GST*

FULL COURSE MATERIALS TO BE PROVIDED

Contents

CYBER RISK LEADERS

Director & Executive Editor
Chris Cubbage

Director
David Matrai

Art Director
Stefan Babij

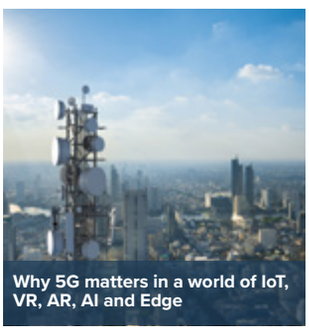
MARKETING AND ADVERTISING
promoteme@mysecuritymedia.com

CONNECT WITH US

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

OUR CHANNELS

MYSECURITY MARKETPLACE
SPACE & DEFENCE
AUSTRALIAN CYBERSECURITY MAGAZINE
AUSTRALIAN SECURITY MAGAZINE
MySec.TV
ASEAN Tech&Sec www.aseantechsec.com
APSM ASIA PACIFIC SECURITY MAGAZINE
Drones & Robotics DRASTIC news.com
CHIEF IT TECHNOLOGY CHANNEL PARTNERS www.chiefIT.me
CCTV BUYERS GUIDE VIDEO | SURVEILLANCE | ANALYTICS
SMART CITIES TECH



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

Daniel **Ehrenreich**

David **Chadwick**

Jane **Lo**
ACSM Correspondent

David **Nicol**

Thomas **Fikentscher**

Garrett **O'Hara**

John **Hines**

Jonathan **Dyble**

George **Moawad**

Daniel **Lai,**

Also with:
Guy **Matthews**
Tom **Wadlow**
Rick **Vanover**
Nathan **Godsall**
Anthony **Spiteri**
Pushkar **Tiwari**
Nick **Savvides**
Gerald **Pang**
Rob **Van Es**

Editor's Desk

"Recent events show all too clearly that many of the biggest threats we face respect no borders or walls, and must be met with collective action. Pandemics and other biological risks, the escalating climate crisis, cyber and digital threats, international economic disruptions, protracted humanitarian crises, violent extremism and terrorism, and the proliferation of nuclear weapons and other weapons of mass destruction all pose profound and, in some cases, existential dangers.

- The White House, Interim National Security Strategic Guidance, March 2021

The world is amidst an 'inflection point'. Mega-trends circling technology and geo-politics have accelerated. In some domains the environment is in flux. The January 6 insurrection of the US Capitol was a low point. So too was the passing of the "patriots governing Hong Kong" resolution at the National People's Congress on March 11. This will reduce democratic representation and allow a pro-Beijing panel to vet and elect candidates. Hong Kong's democratic erosion is practically complete.

Tensions in the Indo-Pacific region have continued to escalate. On March 12 the first ever leaders' meeting of the Quadrilateral Security Dialogue, or Quad, took place virtually. The Dialogue was only upgraded to the level of foreign ministers in September 2019, so given this first meeting of the leaders of India, Japan, Australia and the United States, so recent after President Biden has taken office, is a significant development. Prime Minister Scott Morrison said, "For us, this meeting is about how we keep Australia and the Indo-Pacific region we live in safe, stable and secure." Along with a common cause of a post-Covid-19 recovery, the overwhelming challenge the Quad is seeking to address, is an assertive, and in the South China Sea and Taiwan Strait, an increasingly aggressive China.

On March 5, in Beijing, China's 2021 defense budget, was set at 1.36 trillion yuan, a 6.8 percent increase, or $209.16 billion, from the 1.27 trillion yuan budget set last year. This growth rate stands out as only the third yearly increase during the last decade. China's military spending is understood to now be the second highest in the world after the United States, far exceeding that of its neighbours and greater than the combined expenditure of India, Russia, Japan, South Korea, and Taiwan in 2019. Source

In this issue, we include our recent Indo-Pacific interview series with Australia's former Ambassador to China, Geoff Raby AO, Australian National University's Professor John Blaxland and the American Enterprise Institute's Research Fellow, Zack Cooper.

Covid-19 is at least now under a degree of control, with vaccines being distributed and administered just 12 months following the announcement of the novel pandemic. In our last edition (October 2020), I noted forecasts calculating that over 500,000 Americans will die from the pandemic by the end of February 2021. As of the first week of March 2021, the figure was indeed 521,000, peaking in mid February with around 5,500 deaths in a single day. As of 12 March, over 2.6 million have died globally. Despite the loss of life and the economic impacts, in a cyber context, the pandemic significantly accelerated global digital transformation and has further intensified the weaponization of information. Hence, we're now also seeing governments start to take more proactive action against big technology companies, counter foreign interference and attempt to retain public trust.

The cyber threat landscape remains a significant challenge. Cyber threats are intertwined with the geo-political landscape. Cyber warfare is on display. Nation-states and state-sponsored actors, alongside cyber-organised crime, present an extreme and recurring risk to enterprise, government and populations alike. Recently, in our MySec.TV and podcast series, we covered the Solarwinds supply chain breaches, the Microsoft Exchange hack, attacks on critical infrastructure, such as water treatment plants and the use of the Darknet for facilitating ransomware and major illicit markets reached a peak in 2020, with cryptocurrencies used to launder billions of dollars in related criminal proceeds.

With this 'threatscape' as the backdrop to accelerated technology innovation, or "multiplied innovation", it is why we have selected 5G as this issue's cover feature. With 5G, something far more profound is going on. IDC's research puts some numbers on this: "We see 50% growth in the typical application portfolio," says Patrick Filkins, an IDC Senior Research Analyst. "We see massive interdependencies being built, where each business application has four to eight other app dependencies. We see 58% of all resources at the remote edge needing a network backbone. How does the network help solve that problem? Plus we see 47% of applications being built using modular developed net frameworks. Networking needs to evolve to write the story, and I think 5G helps make that story happen."

As we discussed recently with Algirde Pipikaite of the Centre for Cybersecurity at the World Economic Forum, the challenge remaining with us for some time is managing legacy systems, while ensuring new platforms are built on the principle of security, safety and privacy by design. I'm not confident this is going to be achievable. Besides, we are contending also with a protracted US-China technology divide.

In this edition, we provide you the opportunity to deep dive into the cybersecurity domain, corporate risk management and we cover a broad set of the trends, from space to SASE and plenty in between. We also include links through to our Tech & Sec Weekly Series and the latest Cyber Security Weekly podcasts. There is a lot here to unpack.

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 Magazine. Enjoy the reading, listening and viewing!

Chris Cubbage
CPP, CISA, GAICD
Executive Editor

The New Face of Money - Highlights from the Singapore FinTech Festival 2020

By
Jane **Lo**
SINGAPORE
CORRESPONDENT

During the tumultuous early days of the 2020 Covid19 news cycle, panic abounded.

Besides the immediate health worries, the global trade and economy shut down unleashed waves of manic selloffs and flights-to-safety.

In the financial markets, the Dow Jones suffered its worst day on 16th March 2020 since the 1987 "Black Monday" crash. The benchmark fear index ("VIX") surpassed that of the 2008 Global Financial Crisis. Oil prices plunged into the negative territory for the first time in history.

Stimulus policies, interest rates cuts and lenient reserve rules sparked concerns of inflationary money printing. Confidence tanked and gold's reputation as "safe" powered it past the psychologically key $2,000 level.

2020 is reminiscent of the 2009 Global Financial Crisis.

Just like today, the collapse of trust in 2009 prompted much soul-searching for cash alternatives. It was against this backdrop that Bitcoin burst into the scene as "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."

Today's crisis reveals the dramatic gains Bitcoin has made since its creation 12 years ago. What does its rise mean for gold, the tenacious old guard against disruptions? And for cash, the incumbent recognised form of exchange?

From the 2020 crisis, with the pandemic as a testing ground of sorts for these three contenders - Bitcoin, gold, cash – which will emerge as the face of money in the coming decades?

"Follow the Money"

To paraphrase the popular catchphrase by the anonymous source "Deep Throat" in the movie "All the President's Men", trace the funds for the raison d'être.

Tracing the history of money unveils the use of possessions (cattle, shells, salt, and of course gold), the evolution of its function (a method of payment, a unit of account, a store-of-value) and its role in political control (the debate over how the USD influences the geopolitical landscape is an example).

Predicting how money will develop in the coming decades involves drawing on historical events.

Moreover, as technology powers more and more of our daily lives, the view of money is also necessarily through a technological lens.

And where money matters intersect with technology, the Singapore FinTech festival is the ideal forum.

So, what are the views on how Bitcoin, gold and cash

will develop in the coming decades? We look at some discussions.

Does the recent record-breaking run of Bitcoin spell the end of cash and gold?

Undeniably, the recent highs asserted Bitcoin's status as a credible contender.

Having languished at single digit levels for much of the last two years, Bitcoin hit $10,000 in the summer, and smashed the $20,000 barrier during the FinTech festival week.

Is this breakthrough a hype or does it herald the beginnings of Bitcoin as money of the future?

Bitcoin claims to be the "silver bullet" for commonly cited problems.

One is reducing the inefficiencies in cross-border money transfer by replacing the legacy of myriad operating protocols with blockchain-based Bitcoin. Another is reaching the "unbanked", by leveraging their mobile phone connections in the blockchain.

At first glance, Bitcoin without reliance on existing money clearing and settlement arrangements appears to be superior.

However, digging through the discussions at the FinTech

Ravi Menon, Managing Director, Monetary Authority of Singapore, speaking at the Singapore FinTech Festival 2020 on 8 December 2020. Photo Credit: Singapore FinTech Festival

Since its inaugural edition in 2016, the Singapore FinTech Festival, organized by the Monetary Authority of Singapore (MAS), has not disappointed.

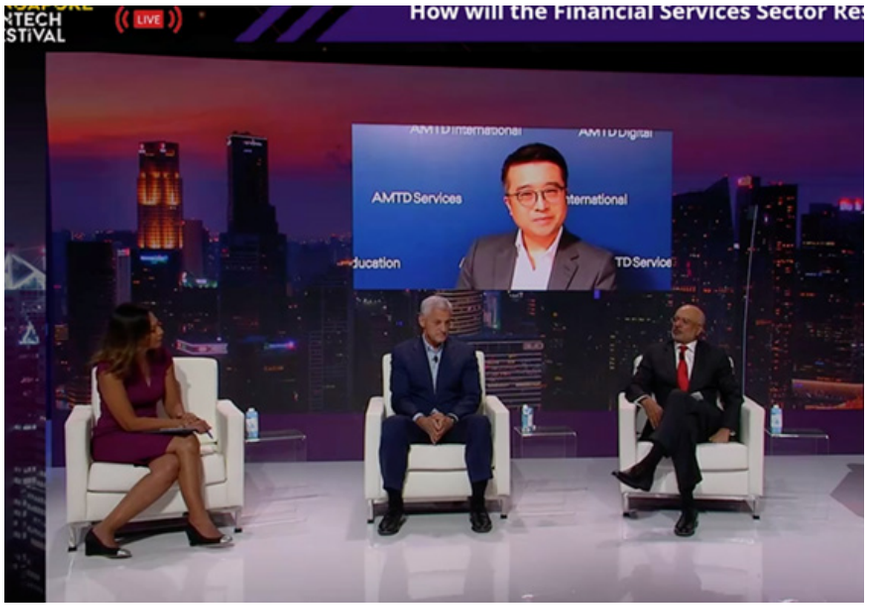
And for the second year in the row, the Singapore FinTech Festival, is co-held with the Singapore Week of Innovation and TeCHnology (SWTICH).

However, with Covid19 restrictions, this year's show featured a hybrid format that combined a 24-hour online event platform with satellite events around the world.

The 5-day festival (7th - 11th December 2020) attracted 60,000 participants from over 160 countries, 27 international pavilions, 1,300 exhibitors, and 45 satellite events across the globe.

More than 2,000 world-renown speakers from the financial sector (banks, regulators, payment service providers), start-ups, "Big Tech", and platform companies drew 3.5 million session views on the online event platform and social media.

Photo Credit: Singapore FinTech Festival 2020.



Economic How Will the Financial Services Sector Respond in 2021 (Episode 2)
From Left: Moderator: Haslinda Amin, Chief International Correspondent, Southeast Asia, Bloomberg Television
Calvin Choi, Chairman of the Board, AMTD Group
Bill Winters, Group Chief Executive, Standard Chartered PLC
Piyush Gupta, Chief Executive Officer, DBS Group
Photo Credit: Monetary Authority of Singapore

Festival, there are some serious challengers.

First, there are e-wallets by platform providers such as Tencent, and inter-government initiatives, such as that announced at the FinTech Festival: The first-of-its kind linking Singapore and Thailand users to send money between the two countries 24x7.

Bypassing blockchain's cumbersome protocols, they hold a significant advantage over Bitcoin. At less than 10 transactions per second, Bitcoin's speed is a poor fraction of industry average. "Public blockchains don't have enough scalability," said Vitalik Buterin (Founder, Ethereum, which ranks behind Bitcoin as the world's second-largest cryptocurrency by market value.) at the session "Blockchain for Good."

Second, in the crowded world of blockchain money, two schemes are gaining momentum.

One is the Central Bank Digital Currency (CBDC), such as MAS's Project Ubin developed with multiple parties, including Bank of Canada. The other is "stablecoin", the most famous of which is Libra, the subject of heated debate last year when Facebook and its partners announced plans to launch a blockchain payment system.

Blockchain Blockshow: Blockchain for Good - • Vitalik Buterin, Founder, Ethereum, Moderator: Shaun Djie, Co-Founder and Chief Operating Officer, Digix. Photo Credit: Monetary Authority of Singapore.

All these solutions reference Central Banks' cash, contrasting Bitcoin which is deliberately untethered from any centralised command.

Ultimately, Bitcoin proponents believe its "competing vision of money" – where control is distributed amongst the network participants, rather than one vested in a central authority – is a potential solution to preventing future financial crises.

Cash is King

Meantime, Covid19 has further extended the entrenched status of cash.

Cash has turned digital triggered by a spike in online shopping due to lockdowns and this consumer behavioural shift has spilled over to in-store purchases.

"Buyers and sellers are shifting significantly online", said Ryan Mclnerney (President, Visa) at the session "The Evolving Payments Ecosystem", and "also the way people engage in commerce in the face-to-face world has changed dramatically" and "touchless is king."

Such developments add impetus to further investments in today's cash infrastructure to rival blockchain.

Moreover, when it comes to cash, "it is based on institutional developments that allow everyone in society to trust the unit of account because it is a good store of value, and medium of exchange," said Agustín Carstens (General Manager, Bank for International Settlements) at the session "Policy Central Banks at the Frontier of Innovation: Digital Currencies and Today's Challenges".

"Money that we know today works", because "institutional arrangements have the backing of government and fiscal authorities, which is hard to replicate in a private environment," he added.

Essentially, "if you distil it into its more elementary essence, that element of trust that is generated by the participation of sovereign makes it at the end of day without substitute," he explained.

"When you receive a payment that's the end of story. There is no more paperwork and checks to happen," and this is enabled by "liquidity provision intra-day, and the only person that can provide liquidity is the central bank," he elaborated.

What about gold?

However, with debasement an ever-present threat, cash as a reliable store-of-value is not without its critics.

"The Fed printed two-thirds as much money in the last 6 months as it did over the prior 11 years", said Cameron Winklevoss (President and Co-Founder, Gemini Trust Company, LLC; one of the Winklevoss Twins who were famously touted as the original creators of social networking – the concept that underpins much of social media including Facebook), at the session "Payments Crypto Is the New Safe

Haven: A Conversation With the Winklevoss Twins."

So, is gold the viable alternative to cash? After all, Central Banks are some major holders of gold, a sign of confidence in the asset.

However, gold does have its detractors, and recently it recorded one of its biggest monthly price drop as vaccine optimism took the shine off it. But it has stood the test of human history and retains its universal appeal today. For the sophisticated investors, it is a reliable protection against uncertainties. For the daily consumers, it is a tangible asset, free from technological complexities and governance frailties.

Is there a clear winner?

Chris Giancarlo (Willkie Farr & Gallangher LLP, USA) put it most succinctly at the session "Will CBDCs Disrupt Stablecoins":

"If there is a winner, it is who is successful to make sure their core societal values - in the case of US, the rule of law, rights of privacy, free enterprise, markets free of government interference and government control" and "if the digital currency reflects other values, say value of surveillance of private economic activity, value of state control of legal outcomes, then the US will be very much a loser in this process."

Indeed, the message of innovating responsibly is growing. After all, adoption is driven by confidence in such features as privacy and safety.

For example, "privacy - the power to selectively reveal oneself to the world - is highly desirable", said Andrew McCormack (Centre Head - Singapore Centre, Bank of International Settlement Innovation Hub) at the session "Will CBDCs Disrupt Stablecoins", while "secrecy is not necessarily highly desirable in a payment system."

In short, a need-to-know disclosure prevents unjustifiable intrusion and abuse (identity theft, spam mail). Opacity over transactions tainted by money laundering, fraud or cyber theft threatens the ecosystem integrity.

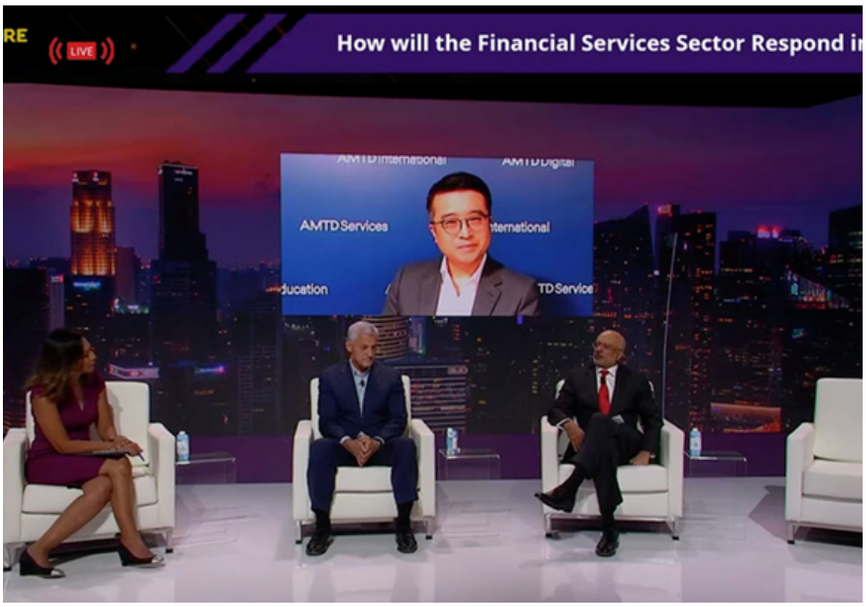
These principles are not new. In fact, cash and gold transactions are subject to stringent know-your-customer regulations and protected by banking secrecy law in several countries.

But for Bitcoin, its critics claim that the pseudo-anonymous feature without an intermediary inevitably attract illicit transfers. Many stress the need for regulations to overcome this negative perception, and as "one of the things that will be necessary before this can reach its full potential," said Stuart Levey (Chief Executive Officer, Libra Association) at the session "Can Digital Currencies Birth the Next Generation of World-Class Payment Systems?"

What has emerged is the view that innovating without undermining confidence in its ecosystem will be key for Bitcoin to compete at scale with cash and gold.

Diversification across Bitcoin, gold and cash

According to Cameron Winklevoss, "money is a technology" and "like any technology, money can always be improved upon and iterated on" and "crypto is just the latest iteration."



Opening address by Mr Heng Swee Keat Mr Heng Swee Keat, Deputy Prime Minister, Coordinating Minister for Economic Policies and Minister for Finance, speaking at the Singapore FinTech Festival X Singapore Week of Innovation & TeCHnology (SFF X SWITCH) 2020 on 7 December. Photo Credit: Monetary Authority of Singapore.

"Bitcoin is the world's first Internet-native money" and "money purpose-built for the Internet. It works the same way that your email works, which is not the case for all other forms of money", he added.

But CBDCs that leverage the technology of blockchain and the familiarity of cash may yet see the widest adoption. The Chinese online retailer JD recently began accepting Chinese digital yuan as a payment method and is set to be fully rolled out before the 2022 Beijing Winter Olympics.

At the same time, the simplicity of gold is appealing.

Faith in any of gold, Bitcoin or cash is defensible as long as we accept the unique characteristics of each.

If anything, Covid19 has underscored the importance of diversification: "COVID-19 has made us reassess what the global future holds. Supply chain disruptions have alerted us to a greater need for resilience and diversification," said Mr Heng Swee Keat (Deputy Prime Minister, Coordinating Minister for Economic Policies and Minister for Finance) at the opening keynote to the Singapore FinTech Festival.

In the same vein, perhaps the future of money has many faces, and diversifying across Bitcoin, god and gold, cash allows us to leverage the strengths and mitigate the weaknesses of each. After all, in the financial world, the number one rule is: "Don't put all your eggs in one basket."

The case for vendors in public-private advisory committees

By
Rob **Van Es**
Vice President of Illumio APAC

It's a sign of strong governance when you see public departments reaching out to the private sector for its input. In Australia, the main vehicle for this is through advisory committees, including the home department's industry advisory committee on cyber security. Announced this year, this committee features a great list of senior cybersecurity professionals at nationally important enterprises.

There's just one thing missing - representation from the security vendors themselves. There's a case to be made here that this is an oversight, but first let's address the main objections to vendors speaking directly to the government.

Of course, there is the potential conflict of interest. Any cynical infosec professional (or journalist) will be quick to point out the interests of the security vendor is to spruik their stuff, not necessarily to solve problems in the most efficient manner. Further to this, other vendors that are left out of advisory committees might also cry foul - especially if a vendor wins a contentious tender whilst also having a place on an advisory committee.

These are strong reasons for why committees are often shaped the way they are (without vendor involvement), but there's a few equally important points in the vendor's favour.

First is that it's often private vendors who are solving these problems to begin with. At Illumio, we've seen an enormous increase in ransomware attacks across a wide range of industries since the global pandemic began. As a result, we expedited the development of our endpoint micro-segmentation technology, Illumio Edge, a solution specifically designed to neutralize malware. Whilst no single vendor will have the same solution to each problem, discussing with the vendor community their own approaches and experiences in working with private businesses on these problems will give the government something invaluable: a working perspective on how efficiently the private sector can tackle such problems on its own, and where more resources might be needed to fill the gaps.

On a related note, vendors also have a unique perspective on the relative strengths and weaknesses of important state assets and private institutions. Let's take a purely hypothetical example - compliance with global security frameworks such as the EU's GDPR or, more locally, with APRA CPS 234. These are areas where private organisations actually have their own conflict of interest when on these special advisory boards. It's the vendors who are ushered in and told 'how it really is' that will have a keen understanding of how the private sector is coping with ever-increasing regulatory burdens.

Finally, there's the big picture. Cybersecurity is a profession that sees constant innovation and disruption. Vendors often have a way of viewing the world which informs their products and ultimately ends up shaping the status quo. When it comes to state assets, being ahead of the curve is vital.

Today, the old paradigms of patching and fixing every system against outside threats are being beaten by savvy attackers moving laterally throughout a network, bypassing these formidable defences entirely. In response, vendors and private organisations are turning towards Zero Trust security models. They have begun accepting that breaches will happen and that a patch won't always be available when it's needed, focusing their efforts on a default-deny approach that only provides access to those with explicit authorization in the first place.

The current government resources such as the Essential Eight are behind the curve, and mean public agencies are not being guided on adoption of Zero Trust and other important security innovations. This may change in the future, to a model similar to NIST in the United States, but there is more to be done at present.

We need to see more from the Australian government when it comes to involving vendors in these high-level discussions. Yes, the exact format of how vendors interface with government stakeholders will need to be different and carefully managed to guard against the objections listed at the top of this article. What we shouldn't do is discount the importance of vendor input because of these objections. That's throwing the proverbial baby out with the bathwater.

MYSECURITY MARKETPLACE

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

EVENTS
Access to events, locally and globally

EDUCATION
Access certified courses, webinars and labs

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

PROFESSIONAL DEVELOPMENT
Join a growing hub of security professionals.

OUR CHANNELS

SPACE & DEFENCE – TECH AND SECURITY NEWS
MYSECURITY MEETUPS
MYSECURITY EVENTS
MYSECURITY ROUNDTABLES
CCTV BUYERS GUIDE – VIDEO | SURVEILLANCE | ANALYTICS
MYSECURITY MEDIA
SMART CITIES TECH
Drones & Robotics DRASTIC news.com
AUSTRALIAN CYBERSECURITY MAGAZINE
Cyber Security
CYBER RISK LEADERS
MySec .TV
APSM | ASIA PACIFIC SECURITY MAGAZINE
AUSTRALIAN SECURITY MAGAZINE
ASEAN Tech&Sec www.aseantechsec.com
CHIEF IT TECHNOLOGY CHANNEL PARTNERS www.chiefIT.me

WhatsApp data sharing policy highlights need for enterprise-grade secure comms

By
David **Nicol,**
Managing Director, ANZ,
BlackBerry

WATCH HERE
MySec .TV

Millions of consumers have been abandoning WhatsApp in favour of rival messaging platforms, following revelations around the platform's new data-sharing policies. This brings to the forefront users' reliance on communications channels that may not meet today's security and privacy demands.

I've met many corporate and public sector executives who admit that correspondence via popular messaging apps has become commonplace within their organisation. Given sensitive information is often shared, it's imperative that security concerns are taken seriously. The recent backlash highlighted that privacy is far from guaranteed when using WhatsApp or other public services. However, this should not be the only concern.

The public sector, in particular, faces an unprecedented challenge: how to keep citizens and institutions safe while facilitating the free flow of information. To meet this challenge, government organisations must find effective ways to protect sensitive communications without adding friction to critical government operations and missions.

The myth of encrypted communications services

The popularity of WhatsApp for work purposes can be attributed to its use of end-to-end encryption for messages. However, not all encryption is created equal and government agencies must ensure that the encryption used meets relevant standards. Encryption of messages is only part of the picture when it comes to delivering enterprise-grade secured communications.

Voice and messaging communications can carry the following risks:

Data breaches

Even with policies mandating use of secured communications channels, we know that people don't always do as they're told. When employees use "more convenient" channels to communicate with colleagues or other stakeholders, there is a risk of data being shared over unsecured devices and networks, outside of the organisation's control.

A recent Forbes Insights survey found that more than 1 in 5 organisations have experienced a cyber event due to an unsanctioned IT resource.

Hacking

It's surprisingly easy to eavesdrop on or monitor modern mobile devices, even over the latest LTE and 5G networks. The vulnerabilities of these systems are well known and are routinely compromised using methods such as fake cell towers and other "man-in-the-middle" (MITM) interceptions.

Meanwhile, people are communicating via a growing

wild and counting, the sheer scale of managing this threat is already overwhelming the resources of most organisations, without adding unauthorised apps or unsecure communications channels.

Identity theft

The use of public or open communications channels – phone calls, text messages, and apps like WhatsApp – presents the risk of identity spoofing, in which cybercriminals foo l you into sharing information with people you think are trustworthy but are, in fact, nefarious imposters.

COVID-19 accelerated shadow IT

The global pandemic plunged millions of workers into virtual workplaces — effectively making home the new makeshift enterprise. The main priority was ensuring communications continued, despite the disruption. This meant standing up alternatives to in-person meetings with tools such as Zoom or Microsoft Teams and reliance on informal messaging channels to replicate casual workplace interactions.

As the pandemic and work-from-home policies drove co-workers apart, digital communication tools were vital for bringing people back together. According to Spiceworks Ziff Davis' study, Workplace Communications Trends in 2020, the use of business chat apps such as Slack and Microsoft Teams increased from 67% in 2019 to 81% in 2020. Additionally, with more people working from home than ever before, 37% of IT decision-makers reported workers preferred to use business chat apps over email— up from 31% in 2019.

With informal communications channels taking front and centre for convenience, security considerations have become an afterthought.

Secure communications in the public sector

Public sector organisations have a track record in actively seeking to protect against security threats and vulnerabilities. Some have developed sophisticated and highly specialised systems for securing top secret and classified information and communications.

For the most part, however, these legacy systems are both expensive and hard to operate. Most require special equipment — such as bulky "Frankenstein" phones — that stand out in a crowd and can compromise sensitive missions.

To work around these limitations, government employees and contractors often resort to using burner phones and other devices that are purported to evade hackers and eavesdroppers. Lacking a secure communications capability, some users have taken the risky route of using personal devices and uncertified applications.

In extreme cases, classified conversations are confined to protected networks or in-person meetings in secure facilities. With a distributed workforce now more commonplace in the public sector – this isn't always possible.

All these options can place risks and severe limitations on critical missions. While many solutions claim to deliver secure voice communications, most offer little more than consumer-level messaging solutions with encryption capabilities added on top. Thankfully, solutions suitable for higher-level sensitive or classified communications are available.

Remote security concerns drive future communications

According to the 2021 State of IT report, more than half of organisations plan to continue using flexible work policies even after the COVID-19 crisis is over. While an additional 11% of businesses plan to adopt secure communications solutions platforms by 2022, with businesses using on average five communications solutions today.

There is an urgent need to consolidate these tools and examine the Shadow IT that may have emerged within organisations since the start of the pandemic, particularly within the public sector. Adopting an enterprise-grade communications solution will ensure data is secured within a single unified stack.

Businesses and governments must use secure messaging services that are fit for purpose, not ones looking to monetise data and engage in other practices that could leave workers and operations vulnerable to malicious actors.

Make digital risk part of the board discussion

By Thomas **Fikentscher,** Regional Director, ANZ at CyberArk

WATCH HERE MySec.TV

Risk is part of doing business. Investing into a new mining facility or launching into a new vertical – in fact, almost every strategic decision by an organisation – carries a degree of risk. It is understood, assessed and weighed up against potential outcomes before a decision is made.

Why then is cybersecurity's role in positive business outcomes still not widely or well understood in Australian boardrooms?

Every day we hear about businesses and government agencies being breached, often to a quite staggering degree. Now, we don't often know the full story or extent of the problem until later down the line – sometimes years later. But the very fact that critical data and assets are constantly compromised tells us that a key aspect of the business hasn't been properly risk assessed.

This is not an issue unique to Australia; it's prevalent globally. In fairness, there are some attacks that could not have been prevented.

What we are learning from the US Senate's select committee on intelligence on last year's attack on SolarWinds is that the degree of resources and hacker innovation can be overwhelming even for the best prepared organisation. Microsoft President Brad Smith estimated in testimony during the hearing that at least 1,000 skilled engineers were part of the attackers' resource pool.

But this is an exception. Most cyber attacks can be prevented from causing severe damage to an organisation. Their mitigation is, in part, down to how digital or cyber risk is understood at the executive level.

The level of understanding around this area would be less concerning if digital wasn't an essential building block of so many key business initiatives. But it is key to so much. Huge focus and large investments are being made in digital transformation initiatives. Businesses are becoming more reliant on digital technologies to accelerate the pace of innovation, gain a leg up on the competition and improve business performance.

As part of this push, they're embracing DevOps methodologies, cloud-based services and on-demand applications to increase business agility and improve efficiencies. Meanwhile, advancements in artificial intelligence, the internet of things (IoT) and robotic process automation (RPA) are helping enterprises transform raw data into meaningful insights and improved productivity.

All this, of course, increases the organisation's exposure and potential risk levels associated with an attack on digital infrastructure. COVID-19 is in part to blame for this; there has been such pressure to digitally transform in a matter of months rather than years, that certain aspects that would normally be risk assessed, have fallen by the wayside. Digital risk is one of them.

What we see at the executive level isn't an unfamiliarity with digital risk conceptually, but a lack of widespread

Microsoft President Brad Smith estimated in testimony during the hearing that at least 1,000 skilled engineers were part of the attackers' resource pool.

technical or digital literacy. This leads to not having a full picture of how all-encompassing a devastating cyber attack could be for the business. Knowledge of this and a shared sense of urgency is needed, both at the executive level and amongst senior leadership just below the board.

Take a proactive stance to digital risk

Any discussion on digital transformation has to include digital risk as a component. Without this, there can be no full understanding of the risk associated with a decision. It's all very well to call security experts in once you've been breached, but this isn't a substitute for a strategy that has considered the risk – and acted upon them - beforehand.

What we'd like to see from the board in cyber terms is what we expect in other areas of decision-making. When examining a digital initiative, amongst the first questions any board director should ask are: "If we rely more on technology, what could go wrong?"; "How do we safeguard that investment?" These questions need to be understood.

Put digital risk into the spotlight

The reality of the situation is that digital risk is one of many competing business priorities. For CIOs, project leaders or risk managers, it can be an uphill battle when you're competing with colleagues for mindshare and budget.

In many ways, however, there is no better time than now to build awareness about cyber attacks and associated digital risk. Digital is now so central to so many organisations that the task of increasing understanding about what poses an existential threat to every organisation is much more achievable than even a few years ago. It is no longer a sideshow or a nice-to-have; it is fundamental.

It's important to take any messaging and language beyond technical conversations and show executives real examples. Just last year, a leading beverages company with operations in Australia was forced to shut down key systems, affecting manufacturing and customer service for several weeks, as a precaution after being hit by a ransomware attack that targeted its computer systems.

When presenting the risks to a project, digital risk can often translate easily to reduced revenue, reputational issues, share price hits and operational interruptions. Case studies from unfortunate victims are, sadly, very easy to find.

If the board, for example, learns that the upcoming investment in automation technologies can potentially be leveraged by malicious actors to 'automate' fraudulent business transactions, more questions are likely to be asked. It might be the same if it becomes clear that every IoT device added to a business' ecosystem could potentially be used as a convenient access point by hackers that allows them to access and compromise corporate IP.

Digital transformation and cybersecurity go hand-in-hand

It's no secret that businesses must embed cybersecurity into digital transformation programs from the onset to protect data privacy, mitigate threats and manage risk.

By improving board and executive communications, creating a security-first culture and fusing security into product planning, development and operations practices, you can help your company unleash the full potential of digital transformation, with digital risk a known and managed component of it.

About the author
Thomas Fikentscher is the regional director of Australia and New Zealand for CyberArk. Based in Sydney, Thomas is responsible for driving strong customer and partner engagement, while expanding CyberArk's emerging identity security business in the region. For more information visit: https://www.cyberark.com/

How to assess, report and minimise cyber risk

By
Garrett **O'Hara,**
Principal Technical Consultant
for Mimecast Australia

Companies, government agencies, universities and hospitals are waking up to the realisation that cyber threats pose a very real, and significant, risk to their operations. They must therefore be factored into any risk mitigation strategy.

This means that, in addition to taking steps to minimise the risk of a cyber attack succeeding, effort must be devoted to assessing the level, and the nature of risk to the business resulting from cyberthreat, to enable decision-makers to understand the risks and develop appropriate responses to those risks.

This assessment needs to cover every aspect of cyber risk and especially the risk to the business itself. It needs to cover, hardware, software, people, services, supply chain processes and assets, and everything should be fully documented.

There's an essential prerequisite to a cyber risk audit, and that's a data audit. You need to identify all the data your company holds and determine its value.

Then, like any significant undertaking, your cyber risk assessment should start with a plan that identifies what you will be analysing, who'll be consulted during the analysis, and if there any regulatory or budgetary preferences that need to be taken into account.

Steps to cyber risk assessment

Once that's completed here are the steps needed to undertake a cyber risk audit.

1. Identify threat sources and events
2. Identify vulnerabilities and how they may be exploited
3. Estimate the likelihood of these threats occurring
4. Evaluate the potential impact on your business if they do occur
5. Determine the degree of risk involved
6. Rank the risks in order of priority
7. Prioritise actions and responses to critical risks

That's a very broad outline. The specifics will vary depending on your objectives and your organisation. It might be wise to bring on board a team of specialists to independently conduct your assessment: a fresh outsider's view can often see things that people close to the action overlook.

The end result of the process is a cybersecurity risk score. It provides a snapshot of the overall cybersecurity risk your organisation is exposed to.

And a cybersecurity risk score is needed not only by a company to assess its risk. It's a way to confirm that an organisation meets the compliance requirements

of government contracts, and it provides valuable information to companies looking to raise equity funding or gain insurance. If a company is looking to find a buyer, or it becomes an acquisition target, a good cyber risk assessment could boost its value.

Regardless of any need to satisfy a third party like a potential customer or investor, every organisation should aim to get its cybersecurity risk score to be as low as possible to minimise its risk of being hit by a damaging, and potentially fatal, cyberattack.

A huge part of this is paying attention to, and rigorously enforcing, some basic security measures.

Implement tools to keep external threats at bay

Protecting the perimeter is a basic first step in any security regime. This is even more important today, because the huge uplift in remote working has greatly enlarged and weakened that perimeter.

Every remote worker should be required to use a VPN for access to the corporate network, and to install and activate reputable firewalls, anti-virus and anti-malware tools. These measures will do much to reduce the risk of a cyber-attack breaching that perimeter.

However perimeter protection is no longer sufficient, just the first of multiple layers. Today zero trust and multifactor authentication are becoming increasingly common practices. They start by assuming that the network is not secure.

With zero trust every accessing device must be authorised for whatever resource it is trying to access and every access attempt is subject to strong authentication to confirm that the user and/or access device have been given permission to access the resources sought.

We're all familiar with multifactor authentication, it uses a password and second means of verifying that the person seeking access is who they claim to be, often a numeric code sent via SMS that must be entered to gain access.

Update and patch software promptly and universally

One of the world's worst cyberattacks, the WannaCry ransomware of 2017, infected over 300,000 computers worldwide and caused up to $US4 billion in losses. It exploited a vulnerability in Microsoft Windows software that the company had identified and issued a patch for.

Those organisations infected by WannaCry had not installed the patch because doing so would have disrupted their 24/7 operation, could have prevent applications

from functioning, or simply because it would have caused inconvenience. In the case of software patching sometimes cost and business implications can get in the way, with disastrous results. The golden rule needs to be that if a piece of software or hardware is so old as to be no longer supported, it should be decommissioned immediately and the business should factor that into its budget.

Perform cyber audits regularly

Misconfigured software and inappropriate access permissions tend to proliferate over time. They should be reviewed regularly and updated appropriately.

None of these activities, designed to boost cybersecurity, can be taken by cybersecurity staff in isolation, they impact the entire business. Assessing the value of data means consulting business units that own and use the protected resources. Implementing things like zero trust and multifactor authentication affect everyone. Patching software might disrupt somebody's business activities.

So CSOs must communicate to their fellow C-suite executives, with the board, business unit heads and sometimes the rank and file of the workforce to fulfil their role of assessing and minimising cyber risk and keeping the business safe. This is often one of the biggest challenges they face.

Get leadership buy in

However, board members' and executives' involvement in cybersecurity goals is crucial. Risk management and security affects all aspects of the company and a breach can have serious consequences for business operations and the bottom line.

CISOs need a direct voice on the board to drive action and investment. This means giving the CISO a seat at the table in the organisation's risk sub-committee. It will enable the board to get a better handle on the challenges and issues that directly affect their security risks, and gain more visibility into actions and investments needed to mitigate cyber risks.

Cybersecurity can be a difficult and complex topic to grasp, so frame your activities, and particularly your achievements in terms of how they impact your organisation's business and risk mitigation strategies. Here are some things you can do as a CISO to get your message across and get buy-in from the C-suite and the board.

Benchmark your cyber risk rating

Boards regularly review the markets in which they operate and assess their position relative to the competition. If you can compare your cybersecurity posture against other, preferably similar, businesses you'll get their attention.

There are security ratings platforms like BitSight or SecurityScorecard that you can use that collect publicly available information. Their data can help the board visualise their cybersecurity standing relative to the current state of the market.

Some of these dashboards can be quite detailed, enabling you to demonstrate your team's success and bolster the board's confidence in your abilities as a CISO. Even if you're not comparing your organisation to another, just a historical record of your KPIs year-on-year can provide valuable insight to the board, especially when planning (and budgeting) for future projects.

Every business a data business

But there is only so much CSOs can achieve with this 'bottom up' approach. Culture comes from the top. Directors and senior executives shape culture through the policies and practices they follow and by setting the right example through their own behaviour.

This is more important than ever. All modern enterprises are data-driven and data dependent. Any significant disruption or damage to their data systems and resources is certain to have a significant business impact.

Business leaders must understand the value of a low cyber risk score and support the initiatives necessary to achieve this. It's essential for a company's ability to win contracts, build reliable partnerships, secure financing and get the best insurance rates, and to make sure it stays in business.

About the Author
Garrett O'Hara is the Principal Technical Consultant at Mimecast having joined in 2015 with the opening of the Sydney office, leading the growth and development of the local team. With over 20 years of experience across development, UI/UX, technology communication, training development and mentoring, Garrett now works to help organisations understand and manage their cyber resilience strategies and is a regular industry commentator on the cyber security landscape, data assurance approaches and business continuity.

Top Women in Security

ASEAN REGION 2021

NOMINATIONS OPEN 8th MARCH 2021 | INTERNATIONAL WOMEN'S DAY

This initiative has been established to recognize women who have advanced the security industry within the ten countries of the Association of Southeast Asia Nations (ASEAN).

Nominations are scheduled to open on **Monday March 8, 2021,** coordinating with International Women's Day.

The **Top Women in Security ASEAN** awards follow similar initiatives in India, as well as Africa, Europe and Canada and form part of a global campaign by the Women in Security & Resilience Alliance (WISECRA). This initiative is open to all ASEAN countries following very successful Top Women in Security Awards held during 2020 in Singapore, Malaysia and Philippines.

We have gathered unique industry partnership arrangements, bringing together key chapters of premier, global security industry associations and professional women in security groups in Singapore. Malaysia, Indonesia, Philippines, Thailand and including the ASEAN Region Women in Security Network. We thank them for their support.

Nominations close 30 May, 2021. The awards will take place in July 2021.

Please nominate at your earliest opportunity.

NOMINATE HERE

ORGANISERS

MYSECURITY MARKETPLACE

WISECRA WOMEN IN SECURITY & RESILIENCE ALLIANCE

MEDIA PARTNERS

WOMEN IN SECURITY MAGAZINE

MYSECURITY MEDIA

SecurityMatters

IFSEC GLOBAL

SUPPORTING PARTNERS & ASSOCIATIONS

ASIS Thailand Chapter | ASIS Philippines Chapter | ASIS ASEAN REGION | ASIS Malaysia Chapter | ASIS Singapore Chapter | OWASP

ISACA Manila Chapter | ISACA Malaysia Chapter | ISACA Indonesia Chapter | ISACA SINGAPORE | ISACA JAKARTA

ISACA Bangkok Chapter | IWIS | ISRM

Embracing digital identity will only happen though education and enhanced learning

By David **Chadwick,** Director of Identity and Biometrics for Unisys

WATCH HERE MySec.TV

Australians are increasingly expecting seamless interactivity between their online and physical lives, and identity is an area that must keep pace with those expectations.

Whether it's for online services, physical ID checks, or even proving personal historical information like vaccine records, a solution that straddles the digital and physical worlds is required to move Australia forward into the future.

GovPass is one such initiative currently being developed by the government. Once implemented this digital identity scheme will, in theory, improve online identity security and expand the accessibility of online verification systems to vastly improve on the availability and convenience of online and offline services in Australia.

Considering the positive impact it could have on the lives of Australians, it's concerning that the initiative could end up in the scrap heap alongside Bob Hawke's Australia Card or Joe Hockey's Access Card if efforts aren't made to help Australians on board with how it will work.

Despite the government investing a further $250 million towards the system at the last Federal Budget, Australians are largely unaware of GovPass and are generally sceptical of government technology solutions, presenting a unique challenge to the government to educate citizens to embrace a new world of access and autonomy.

There is willingness to embrace digital identity

Australians know how important their identity is. Indeed, 56 per cent of Australians are concerned about unauthorised access or misuse of their personal information, according to data from the Unisys Security Index 2020.

Research undertaken by Unisys revealed many Aussies are already using a multitude of ways to verify their identity in a digital environment, for example 76 per cent use passwords to unlock their phone or laptop and 44 use their fingerprint to unlock their device showing a steady adoption in the use of digital identity in everyday circumstances.

Unisys analysis also found that Australians see great value in a Digital ID system, with 61 per cent stating it would be easier to use than the traditional, in-person 100-points ID check. It's not just Millennials and Gen Zs keen to move to an easier way, 58 per cent of those aged 45 and above supported the use of a Digital ID.

We are also witnessing a growing demand for easier ways to access government services such as Centrelink and Medicare with around 69 per cent of Australians already using their identity to access the government's MyGov services and 29 per cent to access MyHealth Records.

The desire for convenience is echoed in access to other services, too. Six in ten Australians (63 per cent) would be willing to use digital identity to renew their passport, and 55 per cent of people are willing to embrace digital identity to collect parcels from Australia Post.

Barriers to adoption

However, the desire for convenient access to services is tempered by barriers to adopting digital ID solutions.

One of the biggest roadblocks is the relatively unknown nature of the Govpass initiative. Data from Unisys shows only 27 per cent of Australians have heard of the government's Digital ID initiative. Of those respondents, less than half (48 per cent) said they understood how the digital identity system would work.

Australians also see a centralised digital ID scheme as a risk to their personal cybersecurity, and are resistant to the concept due to fear of sensitive information being shared with other parties. More than half of Australians (53 per cent) still believe that the only way to securely confirm who they are is to be physically present for identification.

This unease demonstrates a strong misunderstanding of the technology, perhaps owing to a number of factors present in our society that perpetuate myths, including media misrepresentation and alarmism, historic delivery issues of tech and identity solutions from governments, and the proliferation of false or misleading information through digital platforms.

Behavioural Psychology Specialist Kris White believes we have a general level of distrust for governments, especially relating to the emergence of new technologies.

"The negative experiences which we have encountered previously come to mind when we don't understand

"Technology can be a particularly emotive topic because of its rate of change and the struggle to keep up to date. Whether it's the Terminator or robots taking jobs, narratives of the dangers of technology tend to persist in society despite efforts to prove otherwise."

something, or don't realise the degree to which it's going to help us in everyday life," says Kris.

"Technology can be a particularly emotive topic because of its rate of change and the struggle to keep up to date. Whether it's the Terminator or robots taking jobs, narratives of the dangers of technology tend to persist in society despite efforts to prove otherwise."

"That said, just look at social media and smartphones as an example of how comfortable we can become with technology once it is pervasive in our daily lives."

There is however an opportunity to overcome this barrier and successfully adopt the governments digital identity systems.

What the government need to do

The centralised digital identity scheme will use existing documentation to be able to virtually confirm the identity of an Australian by matching data held by another agency, rather than data sharing. The reality of this is that there is less risk of identity theft due to sensitive information being held in fewer locations by fewer parties.

But actually creating GovPass is only the start of the government's journey to achieve widespread acceptance of a digital ID.

As a voluntary scheme, the government need to be aware that pre-existing beliefs and biases may prove a barrier to swift uptake of the initiative, however, through careful communication and a belief in the solution, the government can be successful in the long term.

The Morrison Government, currently in charge of delivering GovPass, has an opportunity to be transparent and educate Australians on the value of this system. Only once the general public are regularly exposed to this new technology can they b egin to understand and value how it will improve their lives.

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most digitally demanding businesses and governments on Earth.

Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing.

Education is essential for ICS Cyber Security Preparedness

WATCH HERE MySec .TV

By
Daniel **Ehrenreich,**
Consultant and Lecturer, SCCE

About the Author
Daniel Ehrenreich is a consultant and lecturer acting at Secure Communications and Control Experts, and periodically teaches in colleges and present at industry conferences on integration of cyber defense with industrial control systems; Daniel has over 29 years' engineering experience with ICS for: electricity, water, gas and power plants as part of his activities at Tadiran, Motorola, Siemens and Waterfall Security. Selected as the Chairman for the ICS Cybersec 2021 conference taking place on 11-2-2021 in Israel. LinkedIn

Cyber security awareness for Industrial Control Systems (ICS), also known as Operating Technology (OT (, is highly important for managing water and electricity supply, transportation, communications and manufacturing facilities. Effectively educating the control engineers and users on ICS-OT cyber security risk can be done through well-defined preparedness. The education program shall involve a) ICS operators and experts, b) IT experts who want to learn ICS basics and cyber defense solutions and c) managers who must make correct decisions related to allocation of resources. This paper highlights few important processes and allow you effectively achieving these goals.

Differentiation among IT and ICS zones

IT cyber security expert mong the key principles and allows predicting most paths which an attacker may consider. For achieving more granular and as accurate as possible prediction, you may use the Industrial (Lockheed Martin) Cyber Kill Chain as well as the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) principles introduced for ICS in 2020.

- Non-attack risk factors: First you must consider two incidents which might risk the ICS process, cause unexpected operation outage or damage but are not considered as a real cyber-attack; a) failure of an ICS sensor, a PLC, a communication appliance or an unexpected software bug, and b) incorrect action done by an authorized person. All these might lead to a panic response by the ICS-OT operator.
- Negligent behavior of people: You must consider actions such and inserting a not-certified USB stick to the ICS network, failure to detect a social engineering action, negligent supply chain processes, allowing remote connection to the ICS without authenticating the connecting person and his computer, consistent use of simple or repeating passwords, poor physical security, and more.
- Intentional attack by an insider: Such adversary might use his knowledge and attack the ICS directly or through the IT network, manipulate the Enterprise Resource Management (ERP) process, alternate parameters on utility processes; HVAC, data center cooling, UPS, fire alarm, in buildings, etc.
- Attacking the ICS Network: Direct access to the ICS network through a "Backdoor" connection, conducting Man in the Middle (MitM) access, using a spoofed identity, DDoS attack, compromising the firewall between the IT and ICS networks, leaking out information from the ICS, etc.
- Manipulating the ICS process: Considering direct sabotage on the HMI, Engineering station, PLCs, field sensors, synchronizing GPS or NTP, manipulating

the process through APT attack, exploiting Zero-Day vulnerabilities, etc. These actions are capable causing outage and damaging the machinery.

Methods for ICS cyber defense

Deployment of an effective cyber defense on ICS-OT shall be based on the overall risk factor, calculated by the likelihood of an attack and the harming impact (R=I*P). Consequently, the PPT Triad-based defense method shall be defined according to the architecture, data protocols, utilized communication media, etc.

- Allow performing antivirus and other updates on the ICS only after intensive safety testing.
- Conduct periodic cyber security assessment for detecting new vulnerabilities for the entire ICS.
- Strengthen the perimeter security particularly for all installations which attackers might access.
- Deploy strong segregation among the IT and ICS zones and among unrelated control appliances.
- Prioritize use of ICS oriented FWs, DMZ, Data Diode, SIEM, white-listing programs, etc.
- Use IDS for detecting ICS-related anomaly conditions at Purdue Model levels 0, 1 and level 2.
- Deploy strong authentication (such as 802.1X) prior connecting any device to the ICS network.
- Perform in-depth inspection of all files and media prior transferring them to the ICS network.
- Always supervise the remote access process and block the connection a.s.a.p. after completion.
- Adhere to the ISA-IEC 62443 international standard and regulations for ICS Cyber security

Educating your staff on cyber security risks

Cyber security experts know well, that high % of “successful” attacks were possible due to lack of awareness and experience in their organization. Therefore, periodic and well-tuned education for all personnel shall be a mandatory action for achieving ICS Cyber security posture. Among employees who shall participate are; a) System operators and ICS maintenance engineers who must upgrade their cyber security skills, b) IT cyber security personnel who must learn how ICS operates and how it can be protected and managers and decision makers who must understand this topic for properly allocating resources.
The training program must include sessions on the ICS applications and architecture, description of risks to the ICS components and periodic drills with demo illustrating an attack-process. The corporate CISO and the management shall clearly define responsibilities for dealing with the following post-incident tasks:

- Instant attack mitigation, blocking the lateral expansion of the attack and minimizing damages.
- Collection of detailed forensics-related data on the attack details and reporting to all stakeholders.
- Effective and rapid activation of DRP for restoring the operation according to the defined BCP.

Summary

Industrial organizations must have documented and practiced methodology for dealing with cyber incidents. ICS cyber security experts must have the knowledge and experience for supporting their organization. These actions will help you complying with industry regulations and preventing incidents that might risk lives of people, cause operating outages and damage to machinery. Therefore, the managements shall allocate adequate resources and acquire the need expertise for effectively dealing with cyber security.

Mitigating reconnaissance attacks on power grids

By
John **Hines**,
Head of Cybersecurity
(Asia-Pacific),
Verizon Business Group

Power grids are a key part of Australia's critical infrastructure that are increasingly coming under attack from malicious cyber threats. Both customers and regulators of energy and utilities firms demand a reliable, resilient service from power suppliers, which means utilities organisations must ensure they include cyber threats as part of risk mitigation – along with mitigating any cause of IT outages such as engineering challenges, bad weather and natural disasters.

There are concerns from both the industry itself as well as the government on the increased activity in cyber-attacks on Australian critical infrastructure. Most recently, Peter Dutton flagged "catastrophic" consequences of the rise in cyber attacks on critical infrastructure at The National Security Summit as a surge in reconnaissance attacks in recent years could be a potent warning of disruption to come.

Fortunately, there are key actions that utilities organisations can take to minimise the threat, starting with identifying risks at an early stage through advanced threat intelligence.

What are reconnaissance attacks?

Reconnaissance attacks are the first stages in what is known as an Advanced Persistent Threat (APT). A popular way to describe a typical APT attack methodology is the cyber kill chain. There are seven key stages of a cyber kill chain:

1. Reconnaissance: Initial harvesting of information on the potential individual within a target organisation.
2. Weaponisation: Combining an exploit with backdoor malware in a deliverable payload.
3. Delivery: Ensuring the payload arrives in the target organisation's network via email, USB or other means.
4. Exploitation: Exploiting a vulnerability to run code on the target organisation's system.
5. Installation: Installing malware on a key asset.
6. Command and control: Opening a communications channel to remotely control the malware.
7. Actions and objectives: Accomplishing the original goals of the attack, such as a power grid hack.

Reconnaissance is, therefore, the first in a multi-stage attack aimed at gathering information on the target system's weaknesses to ensure the best chance of success. The end goal could be anything from installing ransomware to stealing sensitive data or hijacking and sabotaging key assets. It's the cyber equivalent of a burglar scoping out which properties to rob.

Active versus passive reconnaissance

Reconnaissance attacks can be furt her broken down into two key types: active and passive attacks.

Active reconnaissance is the quicker and more direct option, although it also exposes the attacker to potential discovery. They will usually attempt to map the organisation's network, identify hosts and services, and conduct a port scan, typically using powerful scanning tools.

As a percentage of total cyber attacks, there were more breaches of confidential data (23%) on these industries than virtually any other sector over the past seven years.

Any vulnerable services associated with open ports may be exploited during this process to clear an attack path into the network.

Passive reconnaissance is intended to provide useful information on networks, hosts, security policies and employees without setting off any alarms. If active reconnaissance involves trying to open any virtual windows or doors, passive reconnaissance is about observing from a safe distance. This could be achieved by investigating source HTML files on public-facing websites and information on employees' social media sites or by searching public online records. They may even try to impersonate an authorised user by hijacking employee accounts.

Why are utilities at risk?

Verizon's 2020-2021 Cyber-Espionage Report highlights the utilities sector as one of the most frequently targeted by attackers. As a percentage of total cyber attacks, there were more breaches of confidential data (23%) on these industries than virtually any other sector over the past seven years.

According to an article by McKinsey, outlining threats to the energy sector, energy companies are at risk across the whole value chain, from power grid generation and transmission to distribution and customer networks. It suggests three reasons why the sector is vulnerable:

1. An increased number of threats and actors – ranging from financially motivated cyber criminals to nation-states.
2. An ever-expanding corporate attack surface that includes operational technology (OT) as well as information technology (IT) systems spread across a large geographic area.
3. The convergence of physical and cyber systems, which means that global attackers can use code to sabotage facilities.

In the real world

Unfortunately, these are no longer theoretical threats. A 2019 study of global utility professionals warned that over half (56%) had experienced at least one shutdown or data loss incident in the previous year, and 25% had been impacted by nation-state reconnaissance attacks.

Australia's critical infrastructure organisations, including state-owned utilities and hospitals, were initially alerted to the ongoing threat, by the Prime Minister, Scott Morrison's announcement last year of a "sophisticated state-based actor with significant capabilities" behind a "malicious" wave of attacks over the previous year. The announcement indicated that Australia's critical systems were being routinely challenged by hostile cyber snooping, with the intent behind the attacks including possible disruption and intellectual property theft.

Terry Roberts, a US national security and cyber intelligence executive with over 25 years' experience, indicates his view on the intensions and objectives of these probable state actors in what he calls 'the new cyber Cold War'. Roberts discussed two probabilities of these attacks being:

1. To gain root control of a network; and
2. To conduct long-term reconnaissance on their targets' architectures, operations, communications and data.

Federal government concerns over these probable outcomes have led to proposed amendments to the Security of Critical Infrastructure Act 2018, which would give national security agencies powers to step into the networks of some operators of critical infrastructure to disrupt and fend off major attacks.

A recent PwC survey of Australian executives has revealed they are anticipating a higher likelihood of cyber attacks over the next year than their overseas counterparts. And global research firm Gartner predicts there will be a surge in dedicated cybersecurity committees in organisations across the world in the next few years. According to the analyst firm, 40% of boards of directors will feature such a committee, overseen by a qualified

board member, by 2025. This is up from less than 10% today. The research firm made particular note of asset-intensive enterprises such as utilities, manufacturers and transportation networks where security threats targeting cyber-physical systems will present an increased risk.

How can utilities better defend themselves?

The financial impact of COVID-19 is currently a top concern for the power grid and utilities industry. This makes it more important than ever that the sector be able to detect and snuff out potentially costly cyber attacks at the earliest possible stage.

Fortunately, there are various tools and tactics available to help reduce risk in this area. These include:

- Reviewing information publicly available via the corporate website and other online resources to minimise accidental data exposure.
- Educating employees to minimise sharing of personal information online, be alert to phishing attacks and manage passwords securely.
- Rolling out multi-factor authentication to reduce the risk of account hijacking.
- Mapping all network-connected devices, ensuring appropriate security controls are applied and disabling any not in use.
- Disabling any high-risk services and closing ports where appropriate.
- Conducting red team exercises to test detection and response capabilities.
- Conducting regular pen testing to find security gaps and patch any vulnerabilities.
- Considering firewalls and intrusion prevention systems to detect and block port scans.
- Threat intelligence and managed services

Threat intelligence offers another important tool to spot and block reconnaissance activity early on. The best approaches blend automated machine-based learnings with human intelligence to proactively address threats. That means a combination of analytics trained to automatically spot behaviour in NetFlow data that deviates from baseline norms and human analysts' input to flag critical findings and reduce false positives.

Managed services are a good option for organisations that would prefer to outsource this capability to trusted global partners who can offer a team of trained experts in this field.

The Cyber-Espionage Report (CER) is Verizon's first-ever data-driven publication on advanced cyberattacks. The CER is one of the most comprehensive overviews of the CyberEspionage landscape, offering a deep dive into attackers, their motives, their methods and the victims who they target. The report serves as a tool for better understanding these threat actors and what organisations can do to hunt, detect and respond to Cyber-Espionage attacks.

This data-driven report draws from seven years of Data Breach Investigations Report (DBIR) content as well as more than 14 years of Verizon Threat Research Advisory Center (VTRAC) Cyber-Espionage data breach response expertise. The CER serves as a guide for cybersecurity professionals looking to bolster their organisation's cyber defence posture and incident response (IR) capabilities against Cyber-Espionage attacks. Download a copy of the CER at verizon.com/business/resources/reports/cyber-espionage-report/

MYSECURITY MARKETPLACE

EVENTS

Search and find all upcoming featured security events

Tue, Feb 23

Cloud and Datacenter Digital Week 2021

Wed, Feb 24

World Cloud Show - Vietnam

Tue, Mar 02

SupercomputingAsia 2021

Tue, Mar 02

Cyber World Congress: 24-Hour Virtual Cyber Security Event

Plus many more!

COVER FEATURE

Why 5G matters in a world of IoT, VR, AR, AI and Edge

By Guy **Matthews,** Editor of NetReporter

When 4G launched, it offered some significant performance improvements over 3G. But with 5G something far more profound is going on. The doors of possibility have been blown off their hinges. So what lies beyond?

With all the buzz that surrounds 5G right now, it is an interesting contrast to look back at the much more straightforward early days of 4G and LTE, believes Patrick Filkins, Senior Research Analyst with independent consulting firm IDC.

“Back then, we saw the emergence of four pillars - cloud, mobile, social networks and Big Data,” he recalls. “All these fantastic technologies were starting to emerge, but in silos. Now we’re at a stage that I call ‘multiplied innovation’.”

Under this umbrella of multiplied innovation, Filkins sees a sometimes bewildering array of different technology categories: AI, IoT, blockchain and much else besides: “We have all these new standardized natural interfaces that allow applications to flow more freely than ever, and we have the advent of new platforms and communities,” he says. “It's all very exciting. It's all very intense. And it's all very complex.”

A unifying force is needed that has the power to tie all this innovation together and make sense of it, and that, in the opinion of Filkins, is where 5G comes into its own.

“We have new insights being driven by AI-based automation, enabling real time decisions,” he explains. “We have IoT endpoint sensors. There's so much information being generated out there in the technology ecosystem, it's becoming a problem that the industry is trying to manage. Now, we also have the new dynamic edge, and more reach than ever. There are service providers, cloud providers and enterprises themselves defining this new edge, driven by the ability to host applications and carry out processing in areas where we couldn’t before. So in this context, you can start to understand how 5G can help.”

Filkins looks ahead to more applications coming to the fore across multiple ecosystems, as well as API stacks, bringing new expectations, new societal norms and new ways of building networks. Added to this mix are new challenges driven by COVID-19, and the all-important imperatives of trust and security.

Filkins believes we should judge 5G not simply by its list of capabilities, just seeing it in term of bits and bytes: “It's about supporting new applications,” he enthuses. “It's about supporting new use cases. We need to look at what

Figure one: The impact of DX

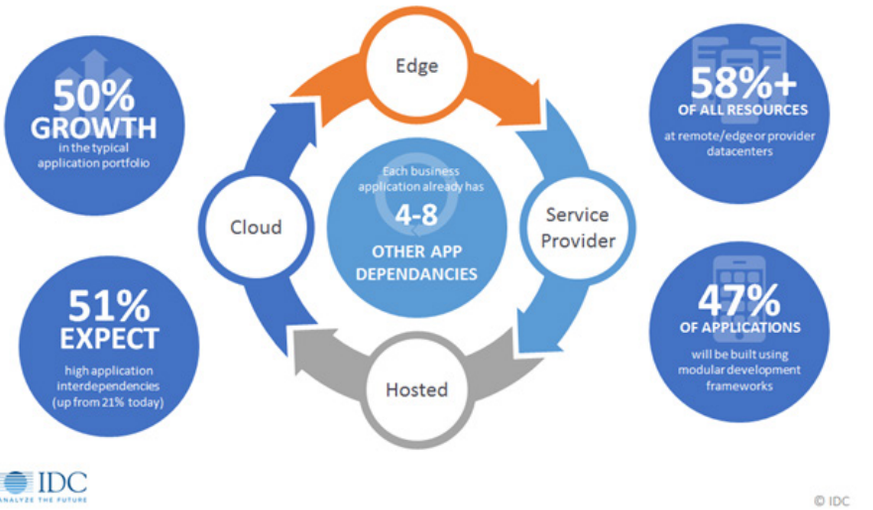
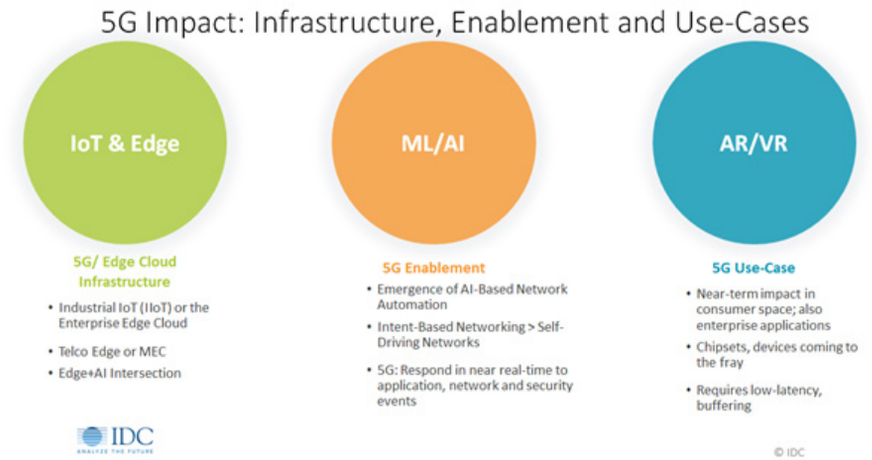


Figure two : The impact of 5G



5G can unlock."

IDC's research puts some numbers on this: "We see 50% growth in the typical application portfolio," says Filkins. "We see massive interdependencies being built, where each business application has four to eight other app dependencies. We see 58% of all resources at the remote edge needing a network backbone. How does the network help solve that problem? Plus we see 47% of applications being built using modular developed net frameworks. Networking needs to evolve to write the story, and I think 5G helps make that story happen."

5G's design, he says, is cloud-native to enable distributed software-mediated micro services. It has a service-based architecture designed to be programmable, leveraging AI-led automation to solve complexity, and help address different use cases and applications: "There's a lot of capabilities baked into the 5G core network that we haven't really unlocked yet that we're just starting to unlock now," he notes.

A number of industry experts were asked to help to drill down further into 5G's potential, looking first at the importance of 5G with IoT and Edge.

Shekar Ayyar, EVP & GM, Telco and Edge Cloud with VMware believes we have all learned to recognise 5G as a technology that delivers better bandwidth, lower latency and a number of improved general characteristics: "But then there's a whole lot of stuff that's happening underneath the covers," he notes. "I would call this the infrastructure or platform for 5G. At that level we're seeing things like the bringing of wireless and wireline networks together. Service providers and operators, having moved up the chain of virtualizing and cloud-defining their own network infrastructure, are now making sure that security and privacy are built in. This is going to enable us to take the benefits of 5G and then translate them into fascinating improvements for everyone, both on the consumer and enterprise side. We're seeing two worlds collide, the cloud world of the hyperscalers, public cloud entities as well as private clouds within enterprises. And then you have the comms world of the telcos."

Ayyar is optimistic that as cloud and comms come together, we will see programmable API-based interfaces that developers can access to create a rich new set of applications on top of edge infrastructure, all catalyzed by 5G.

So much of 5G's potential is brand new, enthuses Mikael Bäck, Vice President & Corporate Officer with Ericsson: "If you look at the World Economic Forum, we had a demonstration in Davos this year of industrial robots working together and communicating," he recalls. "This just couldn't have happened before. We have so many use cases that I think it's almost meaningless for us to sit and

"Back then, we saw the emergence of four pillars - cloud, mobile, social networks and Big Data," he recalls. "All these fantastic technologies were starting to emerge, but in silos. Now we're at a stage that I call 'multiplied innovation'."

list them all. In the end, 5G will be a bigger thing than 4G ever was. There are consumers uses of course, and we are starting to see industrial versions, such as the early adopters in the car industry who are looking to connect the car to a rolling data centre in a way that we have never seen."

But Ronnie Vasishta, SVP Telecom with NVIDIA, believes it is important to remember that both 5G and AI are in the early innings of their use and deployment: "AI is being used in multiple different areas and applications," he says, noting that to really take advantage of this scenario, 5G must embrace AI. "Most people have realized that AI can add value in certain over-the-top services, for example cloud gaming. And we're also seeing the early days of 5G with XR, AR and VR. We had a demonstration in Coventry University in the UK, where we were able, together with partners, to put an AI solution together that allowed medical students to be fully immersive in their studies. You don't have to use cadavers any more, you can actually get inside the body in an immersive way on campus."

Bäck of Ericsson says that for the moment, the vendor is mainly using AI to operate and run networks more efficiently for its customers: "The first thing we did was the simple steps, like automation in our managed service operation, automating manual tasks," he explains. "We're utilizing our role in the middle of the ecosystem and our unique knowledge of the network. Network optimization is one of the obvious tasks that benefits very early from AI, and also resource utilization."

Bäck sees much potential in the areas of augmented reality and virtual reality: "We have been looking at this since about 2014 when we started with the early test systems," he says. "AR and VR are cases where 5G can bring latency down to maybe to one millisecond and really create a true experience that you couldn't do before."

Vasishta of NVIDIA is already excited about future potential, even where it is not yet defined: "We need the ability to plan for the future in terms of use cases," he says. "And see how revenue can be driven by those use cases, I think the easier ones to comprehend are those in the network management space with spectral efficiency and getting more out of spectrum. More challenging is how to take advantage of latency and performance gains."

Ayyar of VMware believes this is the right time to take stock and consider where we go next with 5G: "We need a reformatted set of new applications that are going to take advantage of 5G, improving everything from efficiency and economics as well as global connectivity. All this with the pandemic still upon us, both bringing us closer together, even as we are getting sequestered in our own environments."

Bäck of Ericsson wants 5G to become a digital platform that we use to digitalize almost all sectors of society over the next few years: "That is something we have never done before, certainly not at all on one single scalable platform," he concludes.

In summary, Vasishta of NVIDIA is unable to remember a discussion on why 4G matters: "Just the mere fact that we're asking the question of why 5G matters indicates that it's important," he believes. "5G is the framework that enables so many capabilities where you need the latency, the performance, the standardization. Just think about the sheer amount of data that's being generated through this enablement of 5G anytime, anyplace, anywhere."

MYSECURITY MARKETPLACE

VIRTUAL AND IN-PERSON

INDUSTRY NETWORKING OPPORTUNITIES

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

REGISTER FOR ACCESS

PROMOTE YOUR BRAND

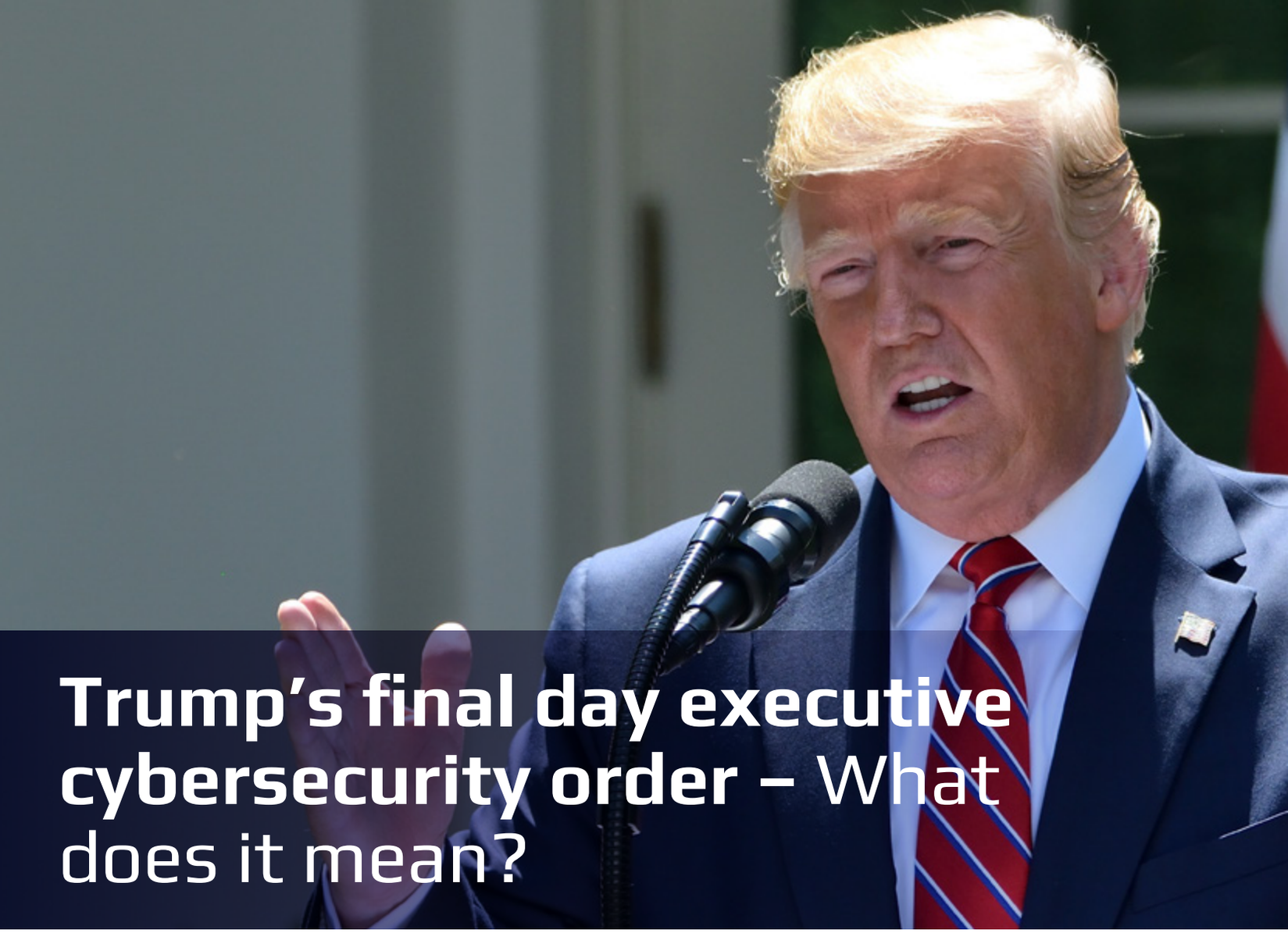
SEARCH THE MARKETPLACE

ALL | EVENTS | COURSES | WEBINARS | REPORTS | BOOKS | WHITEPAPERS | SOLUTIONS

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

SEARCH

www.mysecuritymarketplace.com



Trump's final day executive cybersecurity order – What does it mean?

By Tom **Wadlow**

As the curtain fell on one of the most unconventional, eventful and arguably controversial presidential terms in American history, outgoing White House occupant Donald Trump signed a raft of Executive Orders as Joe Biden officially took over as the country's 46th President.

Among them, a directive which seeks to thwart foreign cyber operators from using US infrastructure to launch malicious attacks.

The Order, titled 'Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities', is designed to reduce access to and the ability to use American information communication technology services for nefarious purposes, according to National Security Advisor Robert C. O'Brien.

In a statement announcing the move on January 20, he said: "Today, President Donald J. Trump signed an Executive Order that closes a longstanding, critical, security loophole for United States Infrastructure as a Service (IaaS) products, one abused by those seeking to harm our country."

The move by the former President is believed to be in response to recent high-profile hacks which have infiltrated US organisations, the most notable being the attack which infected software at SolarWinds, a campaign which also targeted government agencies. The foreign hackers managed to access the company's infrastructure and install malware in a software update – exactly the sort of activity this Executive Order is designed to prevent.

So, how does the directive aim to do this and what could it mean for businesses?

Former President Trump affirms in the Executive Order document: "To address these threats, to deter foreign malicious cyber actors' use of United States IaaS products, and to assist in the investigation of transactions involving foreign malicious cyber actors, the United States must ensure that providers offering United States IaaS products verify the identity of persons obtaining an IaaS account for the provision of these products and maintain records of those transactions."

In short, the Order provides the United States Department of Commerce with the power to impose record-keeping on foreign transactions and, if necessary, block American infrastructure companies from doing business in countries where their products are used as launchpads for cyber-attacks (by individuals or even governments).

Similar powers are granted to block foreign operators who have accounts with US-based organisations, if said operators are shown to be involved in malicious activity.

"Foreign malicious cyber actors threaten our economy and national security through the theft of intellectual property and sensitive data, and by targeting United States critical infrastructure," O'Brien's statement added.

"By gaining access to United States infrastructure-as-a-service (IaaS) products, foreign actors can steal the fruits of American innovation and prepare destructive attacks on our nation's critical infrastructure with anonymity. Malign actor abuse of United States IaaS products has played a role in

every cyber incident during the last four years, including the actions resulting in the penetrations of United States firms FireEye and Solar Winds.

"Today's action by the President is a major step forward in giving our nation's network defenders and investigators an advantage in protecting the American people from those wishing to do us harm."

If the Order makes it into US law, businesses will have to be prepared to prove the security of their business with foreign entities both at home and abroad.

It would result in new customer vetting regulations for IaaS providers (including tech giants like Google, Amazon and Microsoft), as well as record-keeping requirements for foreign customers, including sales made through resellers, an avenue often used by cyber criminals in order to hide their identity before carrying out attacks.

For smaller businesses, the processes involved could strain resources in a more challenging way.

Reacting to the announcement, Founder of American cyber firm Luta Security Katie Moussouris tweeted: "IaaS providers still have to figure out how to run an international intelligence data operation, verify real IDs of foreign customers, and resellers' customers.

"That said, having heard enough hums of a similar melody recently in context of #SolarWinds with lawmakers and policy makers, I don't expect this tune to fade too far out of earshot in the next administration."

And there is no denying that malicious cyber activities have had devastating consequences, not only in terms of national security but also financially. According to the FBI's annual Internet Crime Report, for example, cybercrime cost American businesses and individuals more than $3.5 billion in 2019.

Following the Solar Winds breach there is wide recognition of the need to strengthen domestic cybersecurity defences, and this proposal has been met with a mixed response from industry protagonists.

Jon DiMaggio of Virginia-based cyber-threat analyst firm Analystl told Bloomberg that he welcomed the move.

He said: "It certainly isn't the first time supply chain attacks have happened, nor is it the first time the US government has been aware of the problem. It's about time we started looking past the vendor cost to determine what technology we allow to support critical government infrastructure."

However, major doubts remain as to whether the directive will make a genuine positive impact.

"The way I see it, Trump's Executive Order is like a kid playing with his squirt gun in the middle of a war zone," commented Maria Sirbu, VP of Corporate Communications at global IaaS provider Voxility.

"The chances of having any real influence on the bad guys are so infirm that I am afraid it will work the opposite – giving bad actors more options to look compliant and avoid being identified, if it goes through in the first place.

"Executive Orders need to start with real measures for internet regulations, more visibility into cloud giants, acting agaisnt hate speech and hate crime, harassment and so on. With a few thousand Executive Orders in place on different fronts we might see some differences. Cyberattacks are far more sizeable than cloud and IaaS, however, and the more we talk about 'digitalisation', the more incidents we'll see.

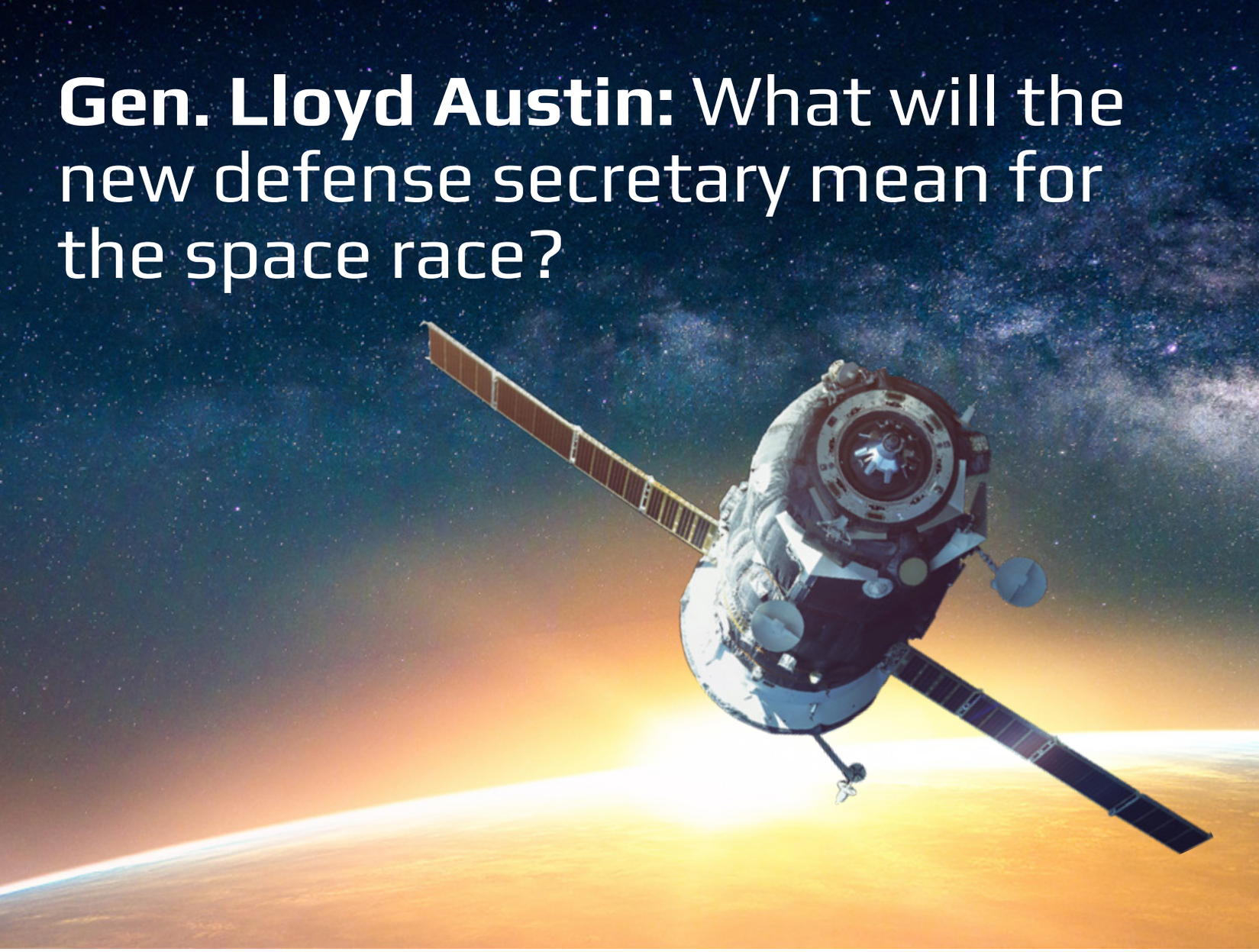
"In terms of the burdens this will place on businesses having to comply, I see it transforming into a war itself. In a way, the European Union is fighting to protect privacy rights as best it can with full enforcement of GDPR and other privacy related laws, while the US wants less privacy by ordering companies to collect data on foreign actors. I do not see it ending well. For sure, we will witness an extended comment period allowing all actors (hopefully) to submit an input and that will be a decisive moment. However, I personally wonder if the internet is not too big already to be regulated."

It is important to note that any new reporting regulations are far from becoming a reality at the current time.

An Executive Order is only the beginning of the process – the fate of the Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities directive ultimately lies in the hands of the Biden administration.

Indeed, the new President has the ability to overturn any Executive Orders made by his predecessor, and the cyber reporting directive could feasibly be among those which are revoked or altered as it journeys towards implementation. The Department of Commerce has six months to draft and propose regulations, by which time President Biden could have issued another Executive Order to amend or stop it in its tracks.

Gen. Lloyd Austin: What will the new defense secretary mean for the space race?



By Jonathan **Dyble**

The space race. A term coined in the 1950s, it has described various shifts in the balance of extra-terrestrial power in decades gone by.

Its first was first used quite literally, referencing the United States' and the Soviet Union's competition for space-based supremacy after the latter of the two countries launched Sputnik on October 4, 1957.

By all accounts, Sputnik wasn't much to look at. It was only about the size of a beach ball (23-inches in diameter) and weighed less than 190 pounds. But it was the world's first artificial satellite and, therefore, signified historic progress.

"That launch ushered in new political, military, technological, and scientific developments," wrote NASA on its 60th anniversary, the organisation having been founded in 1958 with the mandate of sending human passengers to space – a goal the Russians again beat them to.

"While the Sputnik launch was a single event, it marked the start of the space age and the US-USSR space race."

Fast forward six decades and today's space race looks a little different.

Now very much a multi-horse race with the US and China seen as the frontrunners, February 2021 will see both countries land unmanned spacecraft on Mars and deploy rovers to reveal contending images of our closest neighbouring planet.

Indeed, this modern space race remains a cold conflict (if a conflict at all). Its importance has not waned, however, with outer earthly strides signifying superiority of technology – arguably the most revered form of soft power.

New secretary of defense Gen. Lloyd Austin

Let us turn attentions to the Biden administration, and more specifically towards General Lloyd Austin – the President's new defense secretary.

Born on August 8, 1953, Austin is a retired four-star army general steeped in accolades. He previously served as the 12th commander of the United States Central Command (CENTCOM), was the 33rd Vice Chief of staff of the United States Army, and the last commanding general of the United States Forces – Iraq Operation New Dawn.

Having retired from the armed forces in 2016, he has been serving on the boards of three multibillion-dollar companies (Raytheon Technologies, Nucor and Tenet Healthcare), and is now the first ever African American secretary of defense.

Being from a military background, his appointment required a special dispensation from both chambers of Congress that typically prohibits military officials serving in the role within seven years of their retirement from active military service.

But having been voted in 93 to 2, he will now lead the Pentagon and oversee the 1.3 million men and women on duty who make up the United States Military.

"It's an honour and a privilege to serve as our country's 28th Secretary of Defense, and I'm especially proud to be the first African American to hold the position. Let's get to work," Austin tweeted upon confirmation of his appointment.

What it means for the space race

So, what can we expect from Austin?
Space policy was hardly a footnote of the Trump administration, the last four years having seen governmental calls to lay the groundwork for lunar colonies on the moon, the launch of Space Force and the resurrection of the National Space Council.

But with a change in administration will naturally come a change in policy, and in relation to space, Austin has already dropped a hint of his own ambitions.

Testifying to the Senate Armed Services Committee in early January, he presented his views to lawmakers: that while the US still maintains an edge over China, the gap between the two country's space capabilities has been diminishing.

"We'll have to have capabilities that allows us to hold, to present a credible threat… a credible deterrent, excuse me, to China in the future," Austin stated.

"We'll have to make some strides in the use of quantum computing, the use of AI, the advent of connected battlefields, the space-based platforms. Those kinds of things I think can give us the types of capabilities that we'll need to be able to hold large pieces of Chinese military inventory at risk.

"And so, I believe that we still have the qualitative edge and the competitive edge over China. I think that gap has closed significantly, and our goal will be to ensure that we expand that gap going forward."

The challenge from China

The land lies in a precarious position at present.
China remains somewhat blindsided from global space initiatives, with US congress having barred NASA from working with Chinese organisations a decade ago. The Asian powerhouse has taken matters into its own hands as a result, and is on track to launch its first space station by 2022.

Bloomberg also reports that while NASA is working on plans to return humans to the moon in the coming decade, China is preparing its own unmanned lunar mission with the goal of putting its own astronauts on the moon in the near future.

In the private sphere, California-headquartered SpaceX still leads the way. Yet numerous private Chinese-backed space startups have been making headlines. Galaxy Space – a venture backed by Chinese billionaire Lei Jun – operates China's first 5G satellite, for example.

Indeed, between Mars and the moon, tensions in space are hotting up between the two countries and are unlikely to cool based on Lloyd Austin's early comments.

Arguably the most contentious topic that the new defense secretary will have to confront, however, is the Artemis Accords.

Not only does this agreement comprise plans to land the first woman on the moon by 2024, and establish a crewed lunar based by 2030, it also stipulates the establishment of exclusive moon zones.

While many nations signed onto the agreement, China denounced the accords as supporting the United States' "political agenda of moon colonisation".

The polarisation existing between NASA and its key rivals – China and Russia – propels the possibility of conflicts over lunar sovereignty.

Whatever stance Austin and Biden's administration choose to take – that of confrontation or cooperation – it is a quarrel that is becoming increasingly impassioned, and one to watch with regard to global security for the next four-plus years.

How the disposable nature of tech is putting your businesses data at risk

By Rick **Vanover**

It has become common practice for people to chase the latest technology trends. As tech becomes part of our everyday life, the lifecycle of our devices becomes smaller and smaller.

This is posing a huge issue to the sprawl of data.

With the lifecycle of tech shortening, many are abandoning old devices at second-hand stores (thrift shops) and selling them to new owners without thinking about the data and personal information that is left on there.

Many people are now working from home and opting to use a personal computer to get work done. This is making the challenge of controlling and managing your organisations data near impossible. With data now sprawling across company and personal devices, there is no control over it, especially when it is sold on to its next home, left behind at a second-hand store or thrown away.

To add to this, workplace trends like BYOD (Bring Your Own Device) are gaining popularity and making it harder for organisations to keep track of data. IT teams have less control over employees' personal devices and so protecting the data on it becomes a challenge. Things like a lack of encryption or outdated operating systems can lead to potential hacks and data loss.

This is something organisations need to consider when implementing a cyber security strategy. This means educating staff in understanding the risks involved with discarding old devices and setting up the right protections within an organisation.

Educating staff

The first step in managing this is for IT teams to educate employees about the risks involved with using personal devices for work purposes and then eventually discarding it. Employees should be trained in the security practices of an organisation and also understand how that translates to personal devices.

Part of this should be educating staff on how to properly wipe the contents of their phones if they eventually discard it to a second-hand store. This is not something that is considered by most organisations, but it should be as one in

10 Australian mobile consumers are choosing to participate in the second-hand phone market.

Employees also need to be briefed to understand how to identify potential malware, phishing, or ransomware attacks on their personal devices. If employees are able to identify these threats, it mitigates risk of data being lost at all.

Protections

If educating staff fails, there are some protections IT teams can manually put in place to mitigate risk even further.

- Constant software updates – if employees opt to use their devices for work purposes, this has to be under the precedent that the phone is updated regularly. Be sure to provide employees with the support necessary to deliver these updates.
- Password security – to minimise security risks, roll out a compulsory monthly password change. Also ensure that you are putting up restrictions around the type of passwords employees are using, making it less obvious to potential hackers.
- Encrypt data for protection – smartphones and tablets have encryption options that will provide protection of storage. Smartphones that are encrypted have a lower risk of being hacked.
- Clear all phone data – if employees decide to move on to a new device or stop using their current device, ensure you manage the deletion of all data from that phone and a strict policy around discarding devices.

As work from home has become the new normal this year, it is becoming increasingly complicated to manage the sprawl of a company's data. While these agile work trends had been predicted for the next 5-10 years, organisations were not prepared for them to become so mainstream in 2020. As we look to the future, this is only going to become more and more complicated.

It's important for IT teams to understand all the risks as their companies take on more flexible working arrangements in the new future. A huge part of this is of course understanding the risks that come with using personal devices, particularly in the process of discarding them or sending them to a new home.

Why your access control system could be compromising your security

By
George **Moawad,**
Country Manager for Genetec, ANZ

WATCH HERE MySec.TV

No country has felt the tension between China and global western-style liberal democracies more keenly that Australia. Former Australian Ambassador to China Geoff Raby recently noted that Australia-China ties are at their lowest point in history since Australia aligned itself with the United States in pushing back against China's economic ascendancy. And early indications are that they're unlikely to get much better in 2021.

This is causing a headache for industries directly impacted by trade restrictions (most notably higher education, agriculture and pharmaceutical) but it's also prompting businesses from all sectors of Australian industry to re-evaluate their relationship with Chinese technology vendors. Especially when it comes to the physical security technologies used to protect critical infrastructure, cities and businesses.

The potentially devastating cyber security and privacy risks of installing untrustworthy security cameras are beginning to be better understood. This is partly thanks to initiatives like the Australian Government's Cyber Security Strategy 2020 and the introduction of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 to Parliament in December last year. However, the issue of access control has largely remained under the radar. Until now.

The access control threat

As the saying goes a lot takes place behind closed doors, which is why a robust access control system is imperative. Who is coming and going, when, where and how often, are powerful tools for managing and understanding the physical dimensions of a business or government. If a bad actor gets their hands on this type of information, it can cause a significant privacy breach, or in the case of critical infrastructure – a catastrophe.

Determining the ownership, partners, the supply chain and track record of access control manufacturers is therefore critical; now more than ever. This is because in the past, the focus was on securing the perimeter and using access control systems to simply open and close doors. However, modern IP-based access control systems have changed. They are now being used to implement complex access rules, analyse building usage, monitor for atypical behavior and manage time-sensitive access requests within their facilities and much more. All of which offers a gold mine of information for hackers.

The problem is, there's a tendency among some in the security industry to overlook the risks associated with potentially malicious hardware in the desire to reduce costs. Whilst jeopordising safety or security capacity in any commercial enterprise is increasingly a matter of criminal liability, the scale and sophistication of the threat is also a very real threat to national security. Clearly, a close look is needed as your access control system is now a potential vector for a cyber-attack.

Future proof your reputation (and your technology)

Access control systems have a long life-cycle. It takes time to both procure and implement, so it isn't something that is easy to quickly replace. This means that if businesses take the cost-cutting route, they could be taking a big financial, reputational and operational risk. You don't have to look too far to see the upheaval caused by the mandated removal and replacement of Huawei from UK networks. And closer to home there's currently significant scrutiny around the Australian Defence Department's decision to extend a contract with a Chinese-owned company to store data in its Sydney facility.

Given the fast pace of change around geo-political events, it's entirely conceivable that new regulation could be implemented that would require companies to replace their systems way before their planned end-of-life. At best its short sighted and at worst negligent to trim costs by cutting due diligence corners.

Secure the supply chain

It isn't just the access control vendor that you need to do due diligence on; you also need to look at the ownership structure and track record of their supply chain partners. For example, when purchasing a high-quality physical lock, we would expect to take ownership of all of the keys to unlock it and we would exercise caution with who we entrusted these to. Yet, it isn't unusual for organisations to install a digital access control system without considering who may, through error, omission, or poor design have access to this vital infrastructure.

Further, because the product lifecycle of an access control system can be up to 20 years, it's no surprise that some systems are presently lagging behind. It's for this reason that buyers must future-proof their systems before upgrading their hardware. Cyber security issues including manufacturer reputation and track record, and vendor supply chain should all be considered as part of the due diligence and selection process.

Protect national security

Whether or not you are protecting IP, critical infrastructure or highly classified information, it's vital to ensure you're protected from the devastation hackers can cause. Unfortunately, state-sponsored attacks are on the rise. At the time of writing, the ramifications of last year's Solar Winds hack continue to be felt. Hacking group Cozy Bear, which has ties to the Russian Intelligence Agency SVR, is the likely culprit, although the investigation discovered Chinese hackers had also exploited a software flaw to help break into US government computers. And of course, in June last year China launched a bold and broad cyberattack on Australian organisations including governments, educations, health and essential service providers.

Access control therefore can't be overlooked as part of your network cyber security plans. With the proliferation of IoT, and its integration with networks, any access control system must have a strong cyber defense or run the risk of exposing the organisation to increased cyber-risk and even more worryingly, to actual physical threats of doors being opened or locked without their permission.

Across all industries, from financial services to casinos, data centers to hospitals, the installation and connections of your access control vendor must be taken seriously. Modern access control can provide a lot of value, so invest in it and choose your partners wisely.

COVER FEATURE

Big SaaS-pectations

By
Nathan **Godsall,**
Director of Solutions
Engineering, Riverbed APJ

When speaking to customers at the moment, I often catch myself drawing comparisons between their networking issues and luxury cars.

I find the similarities between a 40-year-old Holden Camry and a lagging on-premises network rather uncanny. What I'm in the business of doing is figuring out how even the most traditional, tech-resistant businesses can feel like their network drives like a Ferrari.

The main way organisations are looking to rev the engine and accelerate their productivity is through software-as-a-service (SaaS) applications.

According to Riverbed's Future of Work Global Survey 2020, 42 per cent of business leaders globally put "increasing the use of cloud services or SaaS apps" as their top priority for the next two years.

The current crisis has meant businesses are leaning on the likes of Office 365, Microsoft Teams and other cloud platforms to stay connected and maintain performance throughout extreme disruption.

It's no surprise then that the public cloud services market has grown an overall 6.3% in the past year, one of the few ICT sectors that is experiencing growth, according to a recent Gartner report.

Businesses are moving away from traditional on-premise software in favour of installing multiple SaaS applications that provide services ranging from finance to HR, sales and more. As remote work proves itself to not be a phase, but rather a movement, SaaS applications are going to continue to take charge.

The cloud sector will only continue to grow and vendors will only continue to innovate, creating systems and platforms that accommodate for the new normal and create as seamless an experience for workers, no matter where they are logging in from. As the conveyor belt of shiny new SaaS platforms continues to churn out enticing new capabilities, businesses need to prioritise how they are organising their applications to ensure both their employees and customers high expectations are met.

A swing and a miss

In a recent report by ESG and Riverbed, it was revealed that 73 per cent of global organisations are experiencing poor SaaS performance on a monthly basis, with 90 per cent indicating that this performance degradation is impacting their business.

With the exorbitant spend going into these platforms, this simply should not be the case.

Diagnosing the problem can be tricky. It could be one of many reasons and often the cause of poor performance isn't clear.

Businesses might try short term solutions, such as adding more bandwidth, instead of fixing the underlying problems that come with an old school or overcrowded network. By this point, it's too late, you've missed the shot. When employees are forced to make up for lost time caused by poorly performing applications, this hurts productivity and minimises the opportunity for business growth.

The inconvenient truth

This doesn't mean businesses should shy away from a cloud-centric future but it does show why businesses should be clear about the potential impact that moving applications to the cloud can have on overall performance. Doing so will put you in a better place to develop a network plan that ensures nothing is compromised.

The current state of the world is already taking a toll on productivity and profitability and businesses should not let preventable obstacles take a toll too. Businesses can, and should, take back control over their cloud performance. Tools like our very own SaaS Accelerator help to do just that – improving performance by 8-10 times.

Faster SaaS apps mean less time waiting and more time creating. It means employees can spend more time solving problems, collaborating, and engaging with clients. It could mean the difference between watching the spinning wheel at your desk or logging off early to catch the sunset or cook dinner for the family.

From a customer perspective, faster SaaS could be the cornerstone to a major sale – businesses should never underestimate the value of a swift customer experience on purchasing propensity and NPS (Net Promoter Score).

In today's cloud-first digital age, it is finally possible to have your cake and eat it too. You can meet employee, customer and stakeholder expectations without paying through the nose for it, driving that Holden Camry like a Ferrari.

MEDIA CHANNELS

MySec.TV

The MySecurity TV Channel delivers news and interviews to 2,500+ subscribers on subjects across the security and technology domains and for all MySecurity Media channels.

Cyber Security Weekly Podcast

Commenced in November 2017, the Cyber Security Weekly Podcast has surpassed 250 interviews and provides regularly updates, news, trends and events. Available via Apple & Android. Reaching **400,000** downloads!

CYBER RISK LEADERS

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

SPACE & DEFENCE TECH AND SECURITY NEWS

A dedicated channel for all things in Space, including Defence and Military Technology and related Aeronautics, Information Systems, Communication Systems and Space Exploration.

AUSTRALIAN CYBERSECURITY MAGAZINE

The Australian Cyber Security Magazine was launched in agreement with an industry association and has since expanded beyond to the Cyber Risk Leaders Magazine. This channel continues to be a leading source of cyber security news and updates for the Australian and New Zealand market.

AUSTRALIAN SECURITY MAGAZINE

The Australian Security Magazine is the country's leading government and corporate security magazine channel. Providing editorial and up-to-date news, trends and events for all security professionals in the ANZ and Oceania.

SMART CITIES TECH .io

Your one-stop shop for all things technology, connected and applied intelligence with applications for the home, buildings, cities and infrastructure.

APSM | ASIA PACIFIC SECURITY MAGAZINE

The Asia Pacific Security Magazine maintains a strong focus on regional events and trends. Published since 2010, the APSM has developed a global reputation for quality content and is distributed across all digital channels.

Drones & Robotics DRASTIC news.com

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

CHIEF IT TECHNOLOGY CHANNEL PARTNERS www.chiefIT.me

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

ASEAN Tech&Sec www.aseantechsec.com

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

CCTVBUYERSGUIDE VIDEO | SURVEILLANCE | ANALYTICS

Your one-stop shop for all things CCTV, surveillance and detection technologies with applications for the home, buildings and cities.

promoteme@mysecuritymedia.com
www.mysecuritymedia.com

How old school back-up is holding back the IT industry

By
Anthony **Spiteri**
Global Technologist, Veeam

WATCH HERE
MySec TV

The global pandemic has irrevocably changed the way businesses everywhere operate, tightening the link between a robust IT infrastructure and business continuity.

However, the transition has not been seamless with many businesses unable to adapt to the new environment without downtime. In July alone, Australians reported a net loss of $12.3 million from more than 18,500 scams.

With all this going on, it's surprising that many IT teams are still relying on legacy back-up solutions.

Most legacy backup solutions in the market today are difficult to use. By putting too much effort into backup, IT admins lack the time, resources and simply the energy to tackle real business challenges.

Today's backup technology landscape is now more agile and multifaceted than ever, offering tons of options for any size and budget, and consequently making it very hard to make the right choice. These days, IT needs to think not one, but several steps ahead, ta king ransomware, vendor lock-in, storage capacity and cloud mobility, as well as unpredictable world economical and health factors, into the equation.

To add a cherry on top, the events of 2020 have now compounded these pressures like a match to a tinderbox.

'Australians reported a net loss of $12.3 million from more than 18,500 scams.'

Data protection now needs to be a priority.

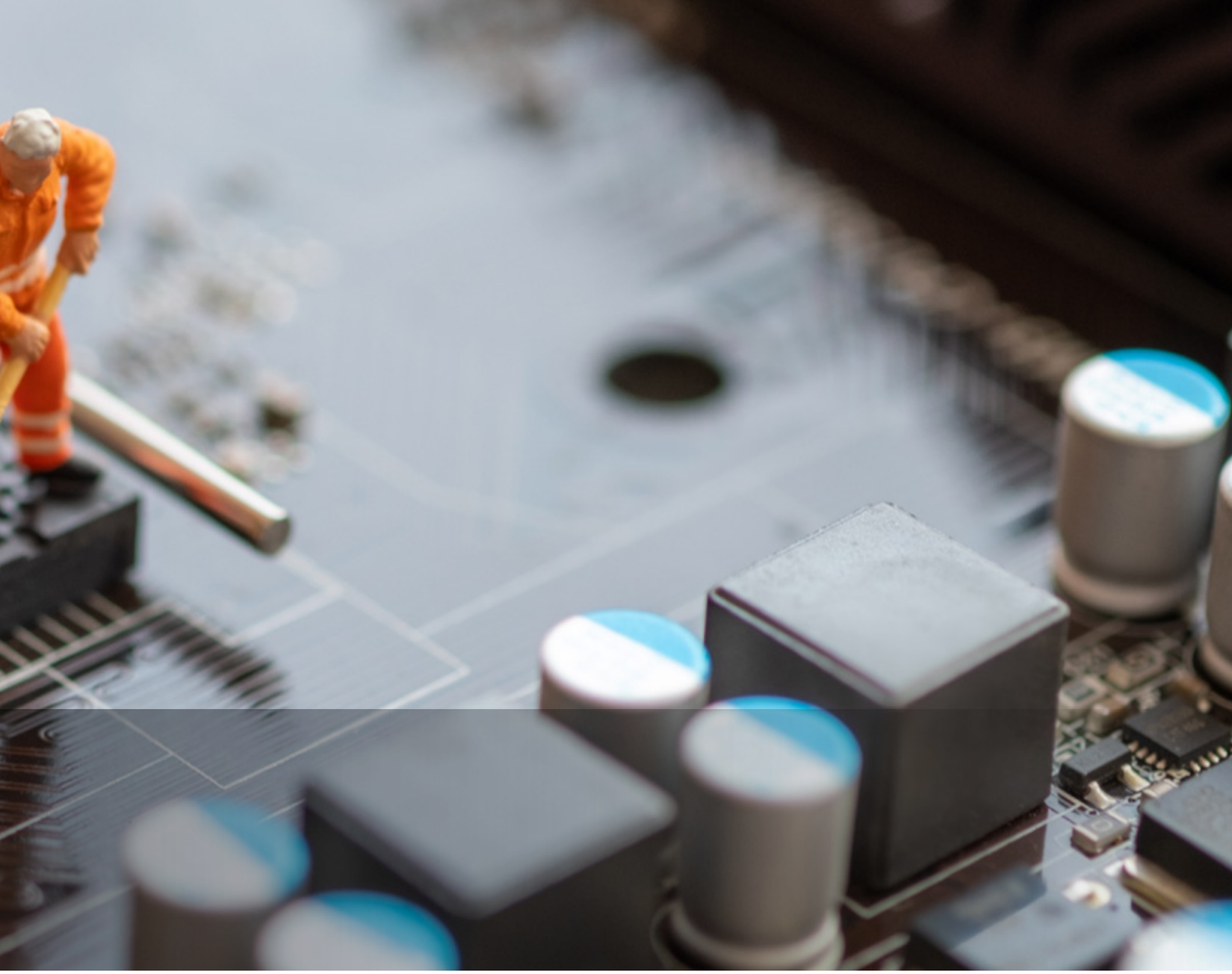
Below are four of the main challenges facing the industry today as it still relies on legacy solutions.

1. Dealing with unreliable back-up

Under the pressure of the pandemic, IT teams need to ensure employees work is still backed up from home. This is not an easy job when using legacy solutions, which use 20 year old code and try to retrofit it for the IT challenges of today.

In addition, dedupe databases often become error-prone and can cause complete data loss. Many solutions lack data recovery verification or only provide this availability for limited platforms. Another issue is visibility into what is working and what's not. All too often, IT admins only find out there's an issue when it's too late.

Many companies chalk this up to a lack of training or skills. This is untrue. If a backup solution is stable, reliable



and easy to use, then you shouldn't need a Ph.D. to use it.

2.The cost of protecting data

Data protection can be quite costly when you take into account, hardware, software and storage costs.

Not to mention the less tangible, often forgotten costs: downtime and data loss. For example, a recent study showed that one hour of downtime for a high-priority application is estimated to cost $67,651. This number is $61,642 for a Normal application.

In addition, downtime and data loss can have an impact on your relationship with your customers or damage to brand integrity.

3.Seeing a return on investment

It can sometimes be hard to see a return on investment, when it comes to data backup.

An ROI consideration for your benefit is data reuse. All data protection solutions encapsulate a great deal of data. In today's ecosystem, data is power, and the right ROI calculation isn't simply crunching the numbers of time saved versus money invested, but also the value provided by putting your data to work.

4. Time and resource drought

IT teams are also challenged with a lack of time and resources. With so much going on, the last thing they need to be doing is 'babysitting their backup.' Far too many products in this industry are hard to use and complicated.

Another important factor is your backup software needs to be able to evolve with the organisation. If adding a new NAS device or changing cloud storage requires you to change your data protection strategy, spend time re-educating IT staff.

Key takeout

It is no longer an option for businesses to make do with older legacy solutions. Businesses are being forced to digitally transform and adopt all sorts of new technologies in order to survive and thrive during the work from home era.

It's time for IT teams to step up and introduce back-up solutions that are reliable, simple and flexible.

Protecting company data in the event of a breach

By Daniel **Lai,** archTIS CEO

The Reserve Bank of New Zealand became the latest major organisation to suffer a serious and malicious cybersecurity attack in January this year when it's third-party file sharing system was hacked.

In its latest update on the event, RBNZ said the nature and extent of the breach was still being investigated, and that some commercially and personally sensitive information may have been illegally downloaded. Investigations into the attack were continuing, though the breach was said to be contained.

RBNZ isn't alone in its recent cybersecurity suffering. Just last year, the Australian Government was forced to respond to a breach which resulted in the details of thousands of MyGov accounts put up for sale on the dark web.

Regis Healthcare, Melbourne TAFE and the Department of Home Affairs also faced major security breaches to their data systems in 2020. Unfortunately, in today's cybersecurity landscape, it may only be a matter of time before your organisation falls victim to an attack too.

Research by Accenture in its 2020 Cyber Threatscape Report found that the COVID-19 pandemic had resulted in businesses being increasingly exposed to opportunistic cyber threats, including phishing campaigns, discontinuity of information security operations and long-term financial constraints.

The report warned that the ongoing economic fallout as a result of the pandemic could create serious financial challenges for companies' information security operations. Meanwhile working from home policies further exposed companies to cyberattacks, as employees relied on less-secure home Wi-Fi routers and VPN connections to do their jobs rather than company infrastructure.

How can data be protected in the event of a breach?

While New Zealand's central bank hasn't yet provided many details about the breach, it's likely that the hacked third-party file sharing system was cloud-based.

Most breaches of this type are generally caused by a compromised user account, via malware, phishing or by over-sharing, where an anonymous URL is shared without requiring the individual user to authenticate.

In most security software and with many security policies, the login process is not robust enough to guarantee that a logged in user is who they say they are, in

Research by Accenture in its 2020 Cyber Threatscape Report found that the COVID-19 pandemic had resulted in businesses being increasingly exposed to opportunistic cyber threats, including phishing campaigns, discontinuity of information security operations and long-term financial constraints.

many cases risking large amounts of data.

A strong security capability should be based on 'Zero Trust' and not automatically trust any user—but instead verify anyone trying to connect to any systems, applications, or individual data files before granting access.

Incorporating a 'trustless' policy may include attribute-based access control, a security model that evaluates attributes rather than roles to determine access, such as security clearance, time of day, location and device to determine who is able to access, edit and download files.

This gives organisations granular, dynamic control over the access of information by making intelligent decisions in real-time on whether the user should be given access to the requested information based on all of these parameters.

Benefits of real time, attribute-based access and sharing control

Using a solution leveraging attribute-based policies to control access to sensitive data has many benefits, including user specific encryption, which means that each user opens their own encrypted copy of the original document. Most importantly it allows contextualised access to the individual and is dynamic against a range of different risks scenarios. Like who they are, their role, where are they accessing the information from, on what device?

It also offers time limited access, which allows access to users for a short period of time and denying access after that window is closed and secure reader mode, when users only require read access.

Personalised watermarks incorporating attributes such as name, date and time can be added in order to track chain of custody of printed materials and deter photographing.

An attribute-based policy also reduces attack surface, preventing copies of a document from being left in unnecessary locations if a file is added to a chat message, sent in an email or edited using a cloud-based program.

A 'trustless' security model is the future of Trust in a digital economy

Today, organisations should assume they will be compromised by a bad actor, disgruntled employee, or malicious software. Zero Trust should not just be employed for system and application access, it must also extend to individual file access.

Only by using intelligent, real-time data security controls that leverage attribute-based policies, can you prevent a compromised user account from resulting in data loss.

Daniel Lai is the chief executive of archTIS, a global technology provider of innovative solutions for secure collaboration of sensitive information.

Container Forensics - What to do if container get compromised

By
Pushkar **Tiwari**

About the Author
Pushkar is Director Development in Symantec Enterprise Division of Broadcom Inc. He has been leading Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) solutions. He has more than 15 years of professional experience in Cyber security and enterprise software.

As forecasted by IDC, 80 percent of the workload is shifting to Containers/Microservices by 2023, which would curtail the need for per-app infrastructure by 60 percent, and accelerate the digital service resiliency by 70 percent. Containers have become the new norm for the development process, and Kubernetes has risen as a standard for container orchestration platforms. Through Kubernetes, you can manage the containers with clusters in the public cloud, hybrid cloud, as well as in the multi-cloud environment. More and more cloud workloads are shifting to containers as these make an ideal choice for cloud environments – thanks to their lightweight nature and efficiency. However, consequently, containers, containing the workloads running in the cloud, are increasingly becoming a target of cyber attackers. The article discusses the challenge of container security and highlights how container forensic can play its role to avoid damage if the container gets compromised.

The Compromised Containers Cases

In February 2018 - Tesla cloud resources were hacked to run cryptocurrencies. According to the RedLock researchers, the hackers had intruded Tesla's Kubernetes console which was not password protected. Similarly, in 2019, Docker Hub usernames, hashed passwords, GitHub and Bitbucket access tokens were exposed in the hack. A user who fails to change his account password and may have their accounts auto builds modified to include malware.

It was further found that the Docker hub had public images with embedded crypto-mining malware. Docker containers have been gaining popularity over the past few years as an effective way of packaging software applications. This is also attracting the attention of malicious actors intending to make money by crypto-jacking within Docker containers and using Docker Hub to distribute these

Where is risk introduced in the container lifecycle?

- Application code
- Image Components
- Orchestration System
- Container engine

Unique to Containers

- Underlying host
- Perimeter and network

images. Based on malicious Docker Hub account analysis, it was revealed that it was hosting six malicious images intended to mine the cryptocurrency, Monero. The coin mining code within the image intends to evade network detection by using network anonymizing tools such as Proxy Chains and Tor. The images hosted on this account have been collectively pulled more than two million times.

The Factors Behind Container Attacks

The recent report from Skybox Security outlines the vulnerabilities and exploits in play over the first half of 2019 in a measured presentation that avoids overstating threats. The report reveals several trends that enterprises need to pay attention to, not least of which is the rapid growth of vulnerabilities in cloud containers.

Cloud containers are lightweight and more portable than virtual machines (VMs), they can replace traditional VMs in many cloud computing deployments because of their speed and simplicity. The problem is that ease of deployment can lead to security headaches.

Containerized applications rely on many supporting services that store containers (registries), orchestrate container lifecycles, monitor their execution, and direct traffic in and out of the containers. Furthermore, containerized applications and microservices go together, which increases the number of components and interactions for an application. All of which means several separate parts need to be secured and it also means there's a larger number of potential attack targets.

The above-mentioned conditions might lead to the following vulnerable factors:

- Exploiting vulnerabilities in container images
- Security misconfiguration, stolen credentials
- Using containers from untrusted repositories

Besides, attackers have various incentives to break containers such as:

- Leverage the compute for cryptocurrencies mining
- Botnet attack
- DDoS attack
- Bring down your cloud service
- Bad reputation

How to operate containers at an enterprise-scale?

Step 1: Is your Incident Response Process Ready?

1. **Identification**
   Identification of incidents by monitoring security events, leveraging security monitoring tools from security vendors.
2. **Coordination**
   Notify the on-call responder, reviews and evaluates the nature of the incident report to determine if it represents a potential data incident, and initiates an incident response process.
3. **Resolution**
   Investigating the root cause, limiting the impact of the incident, resolving any immediate security risks, implementing necessary fixes as part of remediation, and recovering affected systems, data, and services.
4. **Continuous Improvements**
   New insights that can help you enhance your tools, training, and processes.

Step 2: Follow container security best practices

- Build the smallest image possible
- Remove unnecessary tools
- Package a single application per container
- Avoid running processes as root
- Use images from trusted sources
- Sync all your logs to a centralized location
- Invest in container-specific tools either from security vendors or open-source
- Keep run book ready to execute common mitigation options

Step 3: Follow key mitigation practices

- Send an alert – alert
- Restrict from other workloads – isolate
- Stop running processes – pause
- Kill and restart running processes – restart
- Kill running processes but not restart – Kill

- Keep run book ready to execute common mitigation options

The Challenges for the Container Forensic

Root cause analysis is the key for any attacks to understand the impact of damage and identify the correct resolution and prevention in the future. Container forensic is astronomically complex and challenging compared to forensic analysis of legacy cyber-attacks.

Container observability and forensic is challenging due to the following:

- Highly dynamic nature
- Not so great for visibility
- The complex nature of digital forensics (as container environments yield enormous amounts of data at high velocity necessitating the right tool and expertise)
- The short life span of containers
- Ephermal file systems
- No true snapshot capability
- When performing forensics on a container, it often feels like we are running blind with scissors

Container Forensic - Data sources

The data sources are critical in container forensic as they provide a different impact on forensics investigations depending on the incident being analyzed. A thorough overview of each of these data sources is required to forecast the impact they would have on investigation involving network intrusion, malware detection, and insider file deletion.

Following are the data sources for container forensics that must be taken into consideration:

Logs

- Cloud Infrastructure logs / Kubernetes logs
- Audit logs
- Application logs
- Operating system logs
- Network connections
- User logins
- SSH sessions
- Processes
- Execution

Snapshot of the node

The next step might be to snapshot the disk of the node that was running the container. You might then move other workloads off and quarantine the node to run the additional analysis.

- Identify affected nodes and all attached disks
- Create a duplicate of the disks while online
- Send the duplicated disk image for analysis
- Leverage docker explorer tool
- Compare the difference in binaries on disk snapshot

Container Visibility Tools

It is suggested that the devops, security analysts first leverage the variety of tools available to them when working with Docker and Kubernetes. These include utilizing the Docker statistics API to help obtain system metrics, which can be highly useful for those only needing to understand how one's system is impacted by its container load when operating at scale.

Container visibility tools help in finding what is happening in the system and help answer these critical questions.

- Are there unexpected files?
- How do you get real-time info without logging in?
- How do you gather information remotely from multiple systems?
- Tools like Google Rapid Response (GRR) can be leveraged
- Download browser history
- Get details about a file
- Dump memory for a process
- Searching for a bad Jar/malware signature.

Conclusion

When it comes to containers, the recent increase in vulnerabilities is directly tied to a lack of security hygiene. The ease with which developers can deploy identical containers across environments means that container adoption will continue to grow and, as a result, your attack surface will grow if vulnerabilities aren't aggressively managed. A container management process that includes frequent scanning — both pre-and post-image build and launch — orchestration engine patching and base/parent image standards will go a long way towards ensuring that only safe containers are being deployed.

MYSECURITY MARKETPLACE

COURSES

Search and find all upcoming featured courses

FEATURED COURSES

Mon, Apr 05 $625.00

SCADA & ICS Cyber Security Course

Free Online Training

Risk Management Framework Online Training

Free Training

ESET Cybersecurity Training

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

Plus many more!

CONTAINER FORENSICS

WHAT TO DO IF CONTAINER IS COMPROMISED

AS FORECAST BY IDC

80% of the workload is shifting to **Containers/ Micro services by 2023**, which would curtail the need of per-app infrastructure by 60 percent, and accelerate the digital service resiliency by **70%**.

Containers have become the new norm for the development process, and Kubernetes has risen as a standard for container orchestration platforms. Through Kubernetes, you can manage the containers with clusters in public cloud, hybrid cloud, as well as in multi-cloud environment.

However, consequently, containers, containing the workloads running in the cloud, are increasingly becoming a target of the cyber attackers.

THE CHALLENGE OF CONTAINER SECURITY AND HOW CONTAINER FORENSIC CAN PLAY ITS ROLE TO AVOID THE DAMAGE IF THE CONTAINER GETS COMPROMISED.

THE COMPROMISED CONTAINERS CASES

In February 2018 - Tesla cloud resources were hacked to run crypto currencies. **According to the RedLock researchers,** the hackers had intruded Tesla's Kubernetes console which was not password protected.

Similarly, in 2019, Docker Hub usernames, hashed passwords, GitHub and Bitbucket access tokens were exposed in the hack. A user who fails to change his account password and may have their accounts auto builds modified to include malware.

THE FACTORS BEHIND CONTAINER ATTACKS

THE RECENT REPORT FROM SKYBOX SECURITY OUTLINES

The vulnerabilities and exploits in play over the first half of **2019** in a measured presentation that avoids overstating threats. The report reveals several trends that enterprises need to pay attention to, not least of which is the rapid growth of vulnerabilities in cloud containers.

Cloud containers are lightweight and more portable than virtual machines (VMs), they can replace traditional VMs in many cloud computing deployments because of them speed and simplicity. The problem is that ease of deployment can lead to security headaches.

Where is risk introduced in the container lifecycle?

- Application code
- Image components
- Orchestration system
- Container engine
- Underlying host
- Perimeter and network

Unique to Containers

Containerized applications rely on many supporting services that store containers (registries), orchestrate container lifecycles, monitor their execution and direct traffic in and out of the containers. All of which means there are several separate parts that need to be secured and it also means there's a larger number of potential attack targets.

The above-mentioned conditions might lead to the following vulnerable factors:

1. **Exploiting vulnerabilities in container images**
2. **Security misconfiguration, stolen credentials**
3. **Using containers from untrusted repositories**

Attackers have various incentives to break containers such as:

- **Leverage the compute for crypto currencies mining**
- **Botnet attack**
- **Ddos attack**
- **Bring down your cloud service**
- **Bad reputation**

HOW TO OPERATE CONTAINERS AT AN ENTERPRISE-SCALE?

STEP 1 IS YOUR INCIDENT RESPONSE PROCESS READY?

Identification
- Identification of incident by monitoring security events, leverage security monitoring tools from security vendors.

Coordination
- Notify the on-call responder, reviews and evaluates the nature of the incident report to determine if it represents a potential data incident and initiates an incident response process.

Resolution
- Investigating the root cause, limiting the impact of the incident, resolving any immediate security risks, implementing necessary fixes as part of remediation, and recovering affected systems, data, and services.

Continuous Improvements
- New insights that can help you enhance your tools, training, and processes.

FOLLOW CONTAINER SECURITY BEST PRACTICES

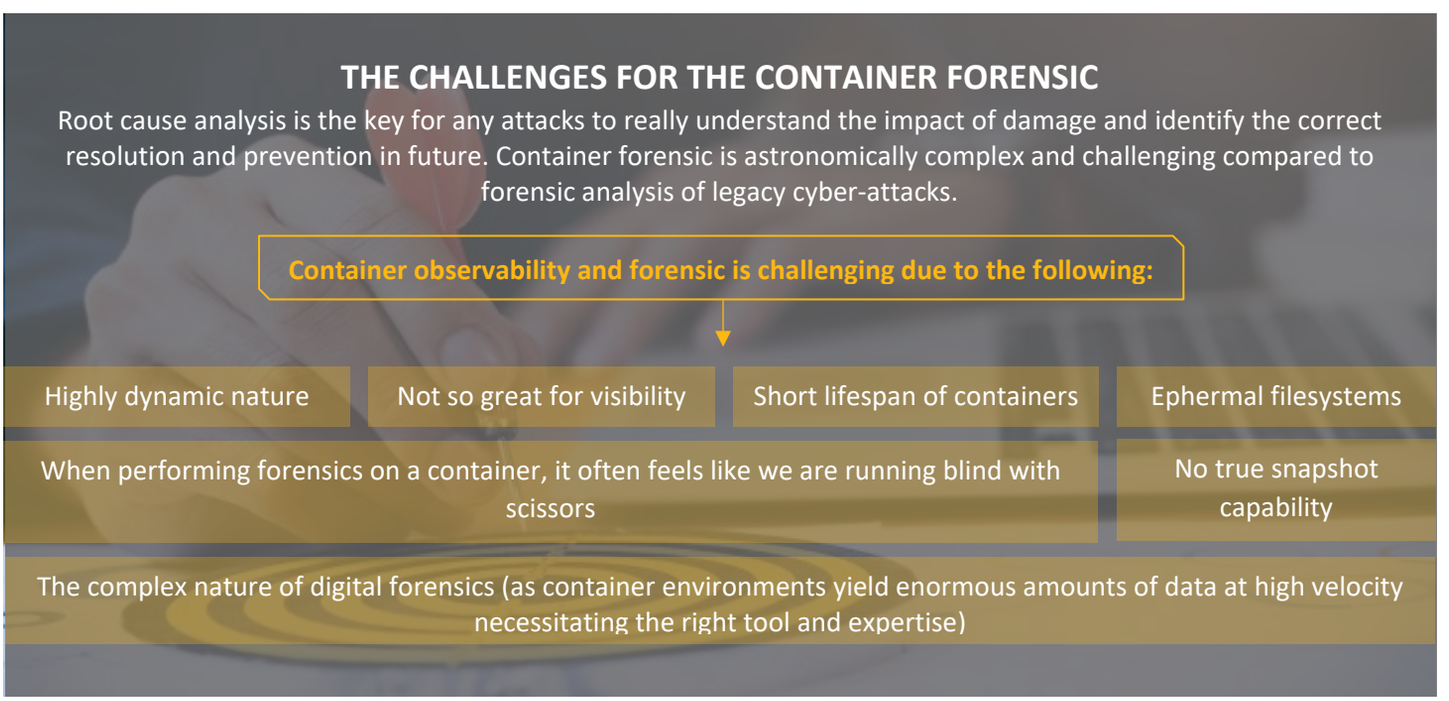
STEP 2

- Build the smallest image possible
- Remove unnecessary tools
- Package a single application per container
- Avoid running processes as root
- Use images from trusted sources
- Sync all your logs to a centralized location
- Invest in container-specific tools either from security vendors or open-source
- Keep run book ready to execute common mitigation options

STEP 3

FOLLOW KEY MITIGATION PRACTICES

- Send an alert - alert
- Restrict from other workloads - isolate
- Stop running processes - pause
- Kill & restart running processes-restart
- Kill running processes but not restart - Kill
- Keep run book ready to execute common mitigation options

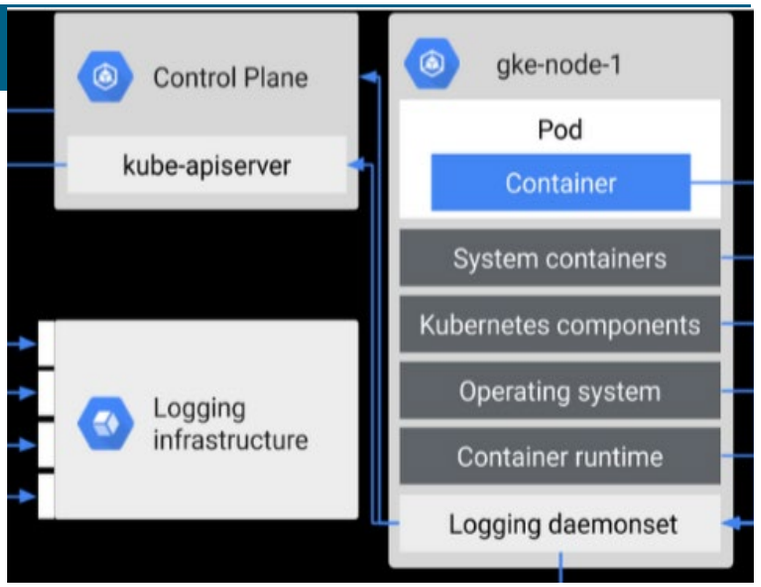


CONTAINER FORENSIC - DATA SOURCES

Following are the data sources for container forensics that must be taken into consideration:

1. LOGS

- Cloud Infrastructure logs/Kubernetes logs
- Audit logs
- Application logs
- Operating system logs
  - Network connections
  - SSH sessions
  - Execution
  - User logins
  - Processes
- Application logs



2. SNAPSHOT OF THE NODE

The next step might be to snapshot the disk of the node that was running the container. You might then move other workloads off and quarantine the node to run additional analysis.

- Identify affected nodes and all attached disks
- Leverage docker explorer tool
- Create duplicate of the disks while online
- Send the duplicated disk image for analysis
- Compare the difference in binaries on disk snapshot

3. CONTAINER VISIBILITY TOOLS

- Are there unexpected files?
- How do you get real time info without logging in?
- How do you gather information remotely from multiple systems?
- Tools like Google Rapid Response (GRR) can be leveraged
  - ✓ Download browser history
  - ✓ Get details about a file
  - ✓ Dump memory for a process
  - ✓ Searching for a bad Jar/malware signature.

THINGS TO NOTE

In terms of security, containers may also be weaker because they share an OS kernel and components. They also require a deep level of authorization (usually root access in Linux environments) to run in the first place. Thus, attacks have a much greater potential to carry down into an underlying OS and over into other containers.

CONCLUSION

When it comes to containers, the recent increase in vulnerabilities is directly tied to a lack of security hygiene. The ease with which developers can deploy identical containers across environments means that container adoption will continue to grow and, as a result, your attack surface will grow if vulnerabilities aren't aggressively managed. A container management process that includes frequent scanning — both pre- and post-image build and launch — orchestration engine patching and base/parent image standards will go a long way towards ensuring that only safe containers are being deployed.

Securing the modern workforce: Zero Trust in a SASE architecture

By Nick **Savvides**

WATCH HERE MySec.TV

COVID-19 has driven a not just a revolution in the way we work but also in the technologies we use. Today, the working sphere has become far more flexible for many more workers. Employees now need to access their data from outside their traditional locations, and through new applications, often outside of the visibility of their security tools that assumed fixed perimeters. These changes have firmly established a realisation that organisations must adapt far quicker than anticipated to the changing security environment.

One of the key challenges with such upheaval is that users will be looking for any possible shortcuts and workarounds to help make their workflow easier and, without the structure of the workplace, many will find their risk perceptions decreasing.

Between the increased threat of malicious attacks brought about by the expanded threat surface, combined with less visibility over potential insider threats, security teams face a daunting challenge in securing data and supporting legitimate actions in a world that looks nothing like the one traditional security structures were built for.

Traditional security and the modern workforce

When our data and applications lived inside our own data centres, so did our security stacks. However, when data and applications moved to the cloud, our security stacks unfortunately stayed planted where they were – all while separate cloud specific security tools gained traction.

This divergent model delivered the worst of both worlds where the flow of data for all users, even remote users, was forced to pass through an on-site central data centre through established security measures, while some cloud applications had completely different security measures. Wide-scale remote working amplified these problems resulting in weak performance, high latencies, and connection failures – placing security firmly in the way of productivity.

In order to avoid the performance problems, many companies now connect their mobile or remote employees and their branch offices directly to the internet and cloud applications. They use technologies such as SD-WAN, but are forced to forego the peace of mind provided by centralized on-premise security technologies.

This updated model, with multiple access points across a wide geographical landscape, has become the ideal target for cybercriminals looking to extort sensitive data. And those cybercriminals aren't wasting any time – according to a study by the University of Maryland, hackers attack every 39 seconds, or an average of 2,244 times a day. This, coupled with the fact that 83% of enterprise workloads will be in the cloud by 2020, means securing the cloud has become a high priority.

SASE brings networking and IT security to the cloud

To address these performance and security considerations, the Secure Access Service Edge (SASE) model has

'53% of companies had over 1,000 sensitive files open to every employee. This statistic becomes all the more alarming when nearly 75% of data breaches happen due to risky insider behaviour or as a result of compromised access'

been developed. It is the latest security and networking architecture model which promises to converge network, web, data, and cloud app connectivity with security to be delivered via the cloud.

SASE is able to address the challenges of securing a remote workforce by converging networking and cyber-security in the cloud - and thus directly to where the applications and data reside. Importantly it equalises security outcomes, by ensuring all users have the same level of coverage. This is achieved by combining the necessary security and connectivity technologies and making them available as a comprehensive cloud service; from Secure Web Gateway, Firewall as a Service, Cloud Access Security Broker or Data Loss Prevention/ Data Leakage Prevention to SD-WAN. As a result, SASE architecture enables companies to connect their users and branch offices around the world directly to the cloud through a single security layer, while simultaneously increasing performance.

Addressing the insider threat: SASE and Zero Trust

Unfortunately, attacks by malicious outsiders aren't the only issue facing organisations. Though the idea might seem paranoid to some, the truth remains that people are the largest threat in any business. According to Varonis, 53% of companies had over 1,000 sensitive files open to every employee. This statistic becomes all the more alarming when nearly 75% of data breaches happen due to risky insider behaviour or as a result of compromised access (Gartner).

Traditional insider threat solutions were designed for the traditional infrastructure-centric security, and required complex integrations and specialist skills to build, operate, and manage. It required a high level of sophistication and specialist knowledge, not just in the security operations and response teams, but also in the business to apply context and understanding. Modern enterprise networks that have evolved into highly distributed environments make this challenge even greater with the traditional systems struggling to integrate with the various networks, applications, and systems. Not to mention, the working from home explosion has caused this problem to be amplified even further.

While the new landscape brings challenges, it also offers us opportunities to improve our overall security posture by adopting the very same concepts that have created the challenges. Insider threat technologies need input signals from user activity from all sources, network activity, application activity, and endpoint activity in order to understand the users and build risk profiles.

SASE helps with this because it brings visibility into the network and application usage that can feed the insider threat analytics however, it alone is not enough. Here is where the Zero-Trust concept can further assist. Zero Trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk/trust levels based on context – each individual operation and interaction is assessed and real-time mitigations, controls, and interventions can be applied. While many people and organisations focus on one component of Zero-Trust, the Zero-Trust Network Access, piece that delivers micro-permitters and secure connections to applications and systems, Zero-Trust is much broader.

If we take the guiding principle of Zero-Trust, of continuous assessment and risk understanding, we can further improve our insider threat posture. This is achieved, by feeding further user activity signals from endpoint monitoring, and access control systems, along with the signals from the SASE environment into the insider threat analytics.

By integrating the SASE stack and endpoint monitoring and control, we can in real-time, feed the output of those analytics back, responding to risks as they emerge. For example, a user might be about to inadvertently leak confidential data via an upload, but as the analytics have determined the user has been displaying risky behaviour from their continuous monitoring, the insider threat system can tell both the endpoint and the SASE stack to dynamically block uploads and removable storage copies for that user, thus preventing the loss event before it can occur.

For the first time in cyber-security, these advanced capabilities are within reach of all organisations, as they have also been digitally transformed into a cloud service with expert guidance, further extending the convergence in the cloud. This provides organisations of any size the ability to gain meaningful visibility and immediate action into risky user behaviour, significantly reducing risk exposure by bringing forward both detection and response to the earliest points in the chain.

Utilising the continuous assessment of Zero Trust in conjunction with established practices such as behaviour centric cybersecurity in a SASE infrastructure would mean a comprehensive security solution can be spread out far and wide to multiple endpoints through the cloud – identifying and eliminating malicious actors, or actions, at the source. SASE, with its convergent architecture and single layer security system, is proving to be a viable solution to all the cybersecurity needs of a remote working enabled future.

By combining SASE with Zero-Trust and comprehensive user and behaviour analytics, this new security model not only simplifies security but significantly reduces risk exposure by service the primary defence against the most valuable of modern assets: Data.

Culture Shift of IT security in agile world

By
Gerald **Pang**

About the Author
Gerald Pang has 17 years experiences in Information Security Management across various Industry working closely with business leaders, with specialization in IT security, GRC and Data Privacy. He is Certified Information Systems Auditor (CISA); Certified Information Security Manager (CISM); Certified Information Systems Security Professional (CISSP); Certified Information Privacy Manager (CIPM) and Certified SAFe® Agilist (SA) with a Master in Information Technology from Queensland University of Technology

Agile software development is becoming more prevalent in the digital evolution of today's world. Culture shift in Agile is meant to help organizations to be more efficient and effective in product development, in order to meet the demands of customer or end-user. Through Agile, teams work collaboratively and provide fast development and delivery of a product.

While the transformation of software development has progressed, the management of information security and risk organization in such environment is not defined and adapted to support such an environment.

Based on SAFe Agile Principles by Scaled Agile, this article will suggest 4 culture shift in IT Security organization may consider in order to adapt to the recent trend of Agile Software development.

Integration of Agile and Security mindset

In line with the principle of a mindset "Apply system thinking and to assume variability & preserve option", the first transformation that an organization may consider is to involve IT Security as part of the Agile team. Most of the time, IT Security will only involve either before the start of development or after the development is completed. IT Security should be part of the team to provide guidance and determine the security controls to be added for the development iteration.

As IT security cuts across technology and business functions, involving IT Security in synchronization events will provide clarification on security requirements. This will enable the different platform teams to be aligned on security requirement to be implemented at various levels of the solution.

IT Security being part of the Agile team, will also mean that they too need to assume variability. This means that IT security should be aware that the product requirements and risk will change throughout the product development iteration. The dynamic development environment requires IT Security to consider the ever-changing risk landscape and determine the IT controls to be added within a development

iteration to mitigate the risk. IT control requirements could be represented as features and user stories for the product, which can be added into the backlog and prioritized based on the exposed risk of the product. The implementation of security controls requires risk- based decision to be made on every iteration, while guided & driven by corporate policy.

Security driven by economic and value

Another key principle of Agile is to organize the deliverables around the value of the product while taking an economic view on the development of the product to achieve the shortest sustainable lead time with the best quality and value. In that perspective, IT Security controls should only be implemented if it is of value to the product. The value of IT security controls can be defined as the effectiveness to mitigate a given threat that has impact to the product if realized. Risk assessment needs to be made to determine the threat and risk that the product is exposed to and determine the IT controls to be put in place to mitigate the expose risk. Beside selecting the IT security controls for the product, prioritization using models such as Weighted Shortest Job First (WSJF) should be adapted and performed on IT security controls to determine the economic value and priority that the controls should be added to the product. Based on the prioritization, IT security controls can be added incrementally in each iteration in relative to product market exposure and added functionality. It is tempting to have all IT Security controls to be added to the application on first release, however, the controls may not directly provide the economic or risk mitigation benefits of the product.

When taking an economic view on security, IT Security should organize security controls and requirement around the value that customer and societal demands. A paradigm shift in the traditional way in handling security and governance is required, where IT Security should assess the risk mitigation value that the security controls is provided to the products. To assess the value that security control has on the product, one should assess and determine if the security control has any value in protecting the company or customer interest at the point of the iteration. Threat and risk assessment can be performed to determine which controls should be added to an iteration in order to meet the security controls required to support the value and risk exposure of the products.

Security Implementation with Agility

The principle of limiting Work-In-Progress (WIP), reduce batch sizes and manage queue lengths can also be applied to security implementation and controls. Security implementation can be broken down into batch sizes represented as user story for the team to implement for each iteration. A clear user story and objectives will ensure that security implementation can be evaluated objectively in every milestone. With security requirement broken down into batch sizes, security implementation can be scaled accordingly and to be prioritized for each iteration based on risk assessment. Primary security controls could be prioritized first while secondary security controls can be put into the backlog for future iteration. Building of on Security functionality can be done incrementally in a series of short timeboxes, adding value and features to the solution as time progresses. Results in the incremental development of the security functionality could be evaluated, allowing incremental capabilities to be presented and evaluated by stakeholders for constructive feedback.

To support the fast incremental approach of software development, security testing and assurance must be adaptive, fast and not cause impediment to the development process. Security testing and assurance must be able to adapt to the ever-changing and incremental iterations. DevSecOps continuous, secure release culture needs to be embedded into team to improve secure development and operations through enhanced security engineering practices. Security tools such as tools used for Dynamic App Security Testing (DAST) or Static App Security Testing (SAST) are integrated and automated in the development process. With integrated tools, vulnerabilities and security issues can be identified early

in the development process, thus allowing the team to plan and work on remediation. Security Penetration testing and security bounty program could be organized to detect security flaws and issues not detected during the fast pace development of the products. With the speed of development, there will be an increase in the reliance of security tools to monitor, detect and defend threats to the application.

Empower Team to make Security Decision

The traditional organization mentality is that cybersecurity is driven by the Security and Compliance team. With this traditional mentality, the organization does not utilize the capability nor the knowledge of the workers at large to drive cybersecurity. Everyone in the organization could be motivated and empowered to make security decisions. To unlock the intrinsic motivation, the organization should first embrace on the core value that security requirements are as important to any features that are added to the product. An organization must see that security provides assurance and confidence to the consumer, thus provide a wider acceptance of the product in the market. With the core value of the importance of security, Teams should be encouraged to explore and make security decisions based on security principles and values. Teams should adopt innovation to ensure security features and controls are added to enhance the security of the product and continue to strive that their product will not fall victim to attacks.

For the team to make a decision on Security controls and risk, it is important that they are empowered to make security decisions. Empowering the team will require an organization to train everyone in the team in secure coding and the ability to evaluate code and application from an attacker's perspective. The team should be able to perform security testing and will have the ability to remediate the issue found. With team empowered to make decisions on security, it will cut down the turnaround time needed for application testing.

What is the implication for IT Security?

The evolution of Agile mindset in product development has been gaining popularity in IT organization transformation. Agile has helped organization to bring the best of teams together to collaborate in order to achieve rapid and continuous delivery of product while maintaining customer satisfaction. However, while the transformation of software development has progresses, the management of information security and risk in such environment is not defined and adapted to support such an environment.

With the culture shift in IT Security to align with Agile mindset, there is an opportunity for IT security and Information Risk to better support an organization that has transformed into an Agile culture. With the right mindset and a willingness to shift the way we manage IT Security and risk; we will be able to align with Agile mindset and provide the required support for IT Security and risk in a fast and dynamic software development environment. The adaptation of security practice within the Agile framework, will enable IT security professional to help the development team to manage risk and balance the security requirement in accordance to the threats and demands of the society. IT security involvement in Agile projects will enable the product to have the right balance of security controls to manage risk.

The evolution of Agile mindset in product development has been gaining popularity in IT organization transformation. Agile has helped organization to bring the best of teams together to collaborate in order to achieve rapid and continuous delivery of product while maintaining customer satisfaction.

CYBER RISK LEADERS

MYSECURITY MEDIA APP

App now available

on iTunes &

DOWNLOAD NOW!

Download on iTunes

GET IT ON Google Play

www.CyberRiskLeaders.com

TECH & SEC WEEKLY

AEROSPACE, DEFENCE & SECURITY TRENDS

MySec.TV

NEWS & INTERVIEWS

10,000 DRONES OVER CITIES OF THE FUTURE? THE SESAR JU URBAN AIR MOBILITY RESEARCH PROJECT GOF 2.0

WATCH HERE

HOW I NAVIGATED GETTING A JOB AT ATLASSIAN AS SECURITY TRAINING MANAGER

ALICE WHITE
Security Training Manager

ATLASSIAN

WATCH HERE

CALIFORNIAN POLICE COMMENCE VR TRAINING

ERIC PEREZ
Director of Virtual Systems Sales

InVeris

WATCH HERE

INDUSTRY 4.0 & ADVANCED MANUFACTURING IN AUSTRALIA

DR JENS GOENNEMANN
AMGC Managing Director

AMGC

WATCH HERE

IBM SECURITY'S X-FORCE THREAT INDEX : APAC INSIGHTS

MATTHEW GLITZER
Vice President, Asia Pacific

IBM Security

WATCH HERE

ANALYSIS OF AN ATTACK ON AUTOMOTIVE KEYLESS ENTRY SYSTEMS

DR DENNIS KENGO OKA
Principal Automotive Security Strategist, Synopsys Software

WATCH HERE

CANBERRA'S NEWEST DATA CENTRE & AUSTRALIA'S SPACE LAUNCH CAPABILITY

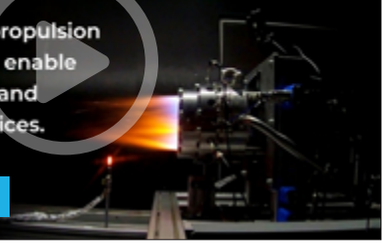
AIDEN TUDEHOPE
Managing Director

macquarie GOVERNMENT

WATCH HERE

AUSTRALIAN SPACE LAUNCH CAPABILITY - ROTATING DETONATION ENGINE RESEARCH

Next generation propulsion system that could enable high-speed flight and space launch services.



WATCH HERE

PODCAST HIGHLIGHT EPISODES

Cyber Security
WEEKLY PODCAST

March 8, 2021

Episode 249 – The Big Biz of Cryptocrime – Pandemic year of 2020

Kim Grauer is the Head of Research at Chainalysis, where she examines trends in cryptocurrency economics and crime. Using Chainalysis data and software, she works with government agencies, exchanges, financial institutions, and insurance and cybersecurity companies to help solve some of the world's most high-profile cyber criminal cases.

DOWNLOAD HERE

March 1, 2021

Episode 248 – Quantum technology and implications for security in today's computer infrastructure

Jane Lo, Singapore Correspondent speaks with Tommaso Gagliardoni, PhD, an Italian cryptographer, mathematician, and quantum security researcher. Tommaso obtained a degree in Mathematics at the University of Perugia, Italy, and a PhD at the Technical University of Darmstadt, Germany, with a dissertation on the quantum security of cryptographic primitives.

DOWNLOAD HERE

February 24, 2021

Episode 247 – Insights into the Centre for Cybersecurity, World Economic Forum – Interview with the Lead, Strategic Initiatives

DOWNLOAD HERE

February 18, 2021

Episode 246 – Security & Surveillance Market Update 2021 – with Genetec ANZ Country Manager

Interview with George Moawad, ANZ Country Manager for Genetec and discussing the 2021 market outlook and trends within the security applications and security operations sector.

DOWNLOAD HERE

February 17, 2021

Episode 245 – Protecting us and our kids online – #StarttheChat Interview with the Australian eSafety Commissioner

Following Safer Internet Day 2021 we reached out to Julie Inman Grant, Australia's eSafety Commissioner to speak about online safety, public awareness and international trends.for an IT security perspective.

DOWNLOAD HERE

February 13, 2021

Episode 244 – Cybersecurity startup 6clicks sets sights as the next Australian unicorn – Interview with Founder & CEO

Interview with Anthony Stevens, Founder and CEO of 6clicks. We speak with Anthony following the recent close of a $5M capital raise and setting out ot be the next Australian unicorn.

DOWNLOAD HERE

February 12, 2021

Episode 243 – Security vulnerabilities in SolarWinds Orion Platform & Serv-U FTP – Insights with Trustwave's Craig Searle

Interview with Craig Searle, Director, Consulting & Professional Services (Pacific) at Trustwave discussing the new SolarWinds vulnerabilities discovered – PLUS its Safer Internet Day 2021 #SID2021

DOWNLOAD HERE

February 11, 2021

Episode 242 – Video surveillance market and analytics application hard drives – Interview with Seagate – MySecTV Takeaway

Interview with Jeff Park, ANZ Country Manager for Seagate discussing the application of purpose built surveillance drives for video systems and using AI and analytics for advanced business and operational applications.

DOWNLOAD HERE

Security versus agility: How do we achieve the best of both worlds?

By
Lindsay **Morgan,**
ANZ Director, Government Security at SAP

If 2020 taught us anything, it's that the weakest link often defines the strength of a chain. Major crises and national challenges have reinforced the importance of collective success – when even one element struggles, so does the larger group.

It's an especially important principle in cyber security, where the tiniest vulnerability can open entire ecosystems to potential harm.

It's also relevant to the government's attempts to strengthen its cyber security and critical infrastructure posture while supporting industry to do likewise. A major component of the government's 2020 cyber security strategy, the draft legislation on Protecting Critical Infrastructure and Systems of National Significance would expand the label of "critical infrastructure" and create new security obligations and mandatory reporting for various public and private organisations.

These organisations could face steep penalties if they don't answer the call to become deeper partners with Australia's government in all aspects of security, particularly cyber.

The government is clearly taking a more holistic approach to cyber security – and so are enterprises. But this gets tricky once you factor in cloud solutions (Public and Private), whose agility and scalability are increasingly necessary for organisations to capitalise on the value of rich data, streamline distributed operations, realise cost efficiencies and make better use of contemporary and emerging tech.

However, platforms like SAP HANA have evolved over a decade to help reconcile some of these tensions. Let's take a look at how.

Can cloud solutions complicate security?

Regardless of architecture, security teams have to think carefully about who has access to data and how they're accessing it.

Most recently, with on-premise architecture, it was a little more like a traditional building with an entrance and an exit. It's a lot simpler to control security when you're managing limited entry points. While many or even most cloud providers have robust security measures in place, cloud solutions do come with more entry points.

However, the security of those entry points differs based on public versus private cloud, as well as a wide variety of factors. For instance, within public cloud, there's simply a greater number of side doors that require the same level of security. With private cloud, you control who has a door and what you let in and out.

That doesn't mean organisations should sacrifice the benefits of all public cloud solutions – in fact, that might do more harm than good. It just means that security considerations need to govern any decision to bring new cloud extensions or providers into your environment. But ensuring scalable, enterprise-wide solutions is where things can get trickier.

Solutions that marry security with flexibility

In many organisations, elements of information are taken out of core systems and put into other data lakes, repositories or spreadsheets. The same piece of information is not only repeated in multiple areas but also with varying degrees of security applied to each of those different locations. If the weakest link determines the strength of the chain, then this approach means there are far more links whose strength is even harder to control or test.

Solutions like SAP HANA, whose 10-year evolution has always been anchored in protecting information and assets, can go a long way to resolving this sort of issue. As an enterprise-scale in-memory database designed to allow end users to have a conversation with their data, HANA caters to large volumes of data and diverse use across a broad user community. The way this can be leveraged for better security is simple: the more information you have in a secure, controlled, unified container, the easier it is to protect that information with centralised security measures.

HANA also enables real-time anonymisation of data displayed in SQL views. This means companies can analyse even the most sensitive and regulated of records – such as those in healthcare – while still protecting data and supporting compliance with privacy standards like the European Union's General Data Protection Regulation (GDPR).

Solutions like Data Warehouse Cloud are the next evolution in further resolving tensions between innovation and security. It allows organisations to extend secure data environments to secure cloud solutions, combining features of HANA with the rigorous security frameworks provided by a range of hyper-scalers. So, even in complex multi-cloud systems, you can achieve a consistent enterprise-wide data management framework and connectivity to other systems, whether that be public, private, on-premise systems or ubiquitous data sources like IoT devices.

Two big mindset shifts need to happen across all of industry and critical infrastructure sectors. First, when it comes to IT systems and reporting environments, we too often test them based on how we expect them to perform. Particularly from a security perspective,

Changing how we think about cyber security

Various types of platforms and architectures can help achieve robust, enterprise-wide security frameworks without sacrificing the benefits of cloud. But strengthening your security posture will also depend on shifting mindsets and educating stakeholders about cyber security and management of risk. There are plenty of business imperatives for this already, but 2021 will see additional regulatory control and incentives as the federal government takes a bigger role in cyber security.

Two big mindset shifts need to happen across all of industry and critical infrastructure sectors. First, when it comes to IT systems and reporting environments, we too often test them based on how we expect them to perform. Particularly from a security perspective, we need an extra level of testing that focuses on what malicious actors want to do and what they're going to try. It's important to test systems based on how we want them to be used but also how we don't want them to be used.

Secondly, we often talk about how to collect data, store data and extend data. Cyber security compels us to ask: what are we going to do with this data? How will people use it? This is particularly crucial now that workers are less tethered to offices or corporate networks. It's more important than ever to think about the potential usage of data and truly consider its security risk, ensuring that the device and solution set you're using to present or extract that data is genuinely secure.

The choice between security and innovation is a false one. Still, the topic is undeniably complex and demands ongoing discussion and thought.

So, what are you doing to protect your organisation while still pushing it forward?

MySec.TV NEWS & INTERVIEWS

INDO-PACIFIC INTERVIEW SERIES | BY CHRIS CUBBAGE

WATCH HERE

CHINA'S GRAND STRATEGY AND AUSTRALIA'S FUTURE IN THE NEW GLOBAL ORDER

– BOOK REVIEW WITH GEOFF RABY

Special interview with Geoff Raby, author of a new book – 'China's Grand Strategy and Australia's Future in the New Global Order'

Geoff Raby was Australia's ambassador to China (2007–11); ambassador to APEC (2003–5); and ambassador to the World Trade Organization (1998–2001). He was awarded the Order of Australia in 2019 for services to Australia–China relations and to international trade.

This interview will review Geoff's work and the new emerging world order of competition and disruption, particularly in the APAC region with consideration to the impacts on Australia, ASEAN and US-China relations.

WATCH HERE

THE US INDO-PACIFIC STRATEGY – THE GREAT POWER COMPETITION

We speak with Zack Cooper, Senior Research Fellow with the American Enterprise Institute (AEI), Washington.

Zack previously served as assistant to the deputy national security adviser for combating terrorism at the National Security Council and as a special assistant to the principal deputy under secretary of defense for policy at the Department of Defense.

He currently studies US strategy in Asia, including alliance dynamics and US-China competition. He also teaches at Georgetown University and Princeton University, codirects the Alliance for Securing Democracy, and co-hosts the "Net Assessment" podcast. Dr. Cooper is currently writing a book that explains how to predict the future path of US-China military competition by examining how militaries change during power shifts.

WATCH HERE

THE US INDO-PACIFIC STRATEGY – IMPACTS FOR AUSTRALIA & THE REGION (INCLUDES XTEK INTERVIEW)

In today's episode we speak with Prof John Blaxland, Strategic & Defence Studies, Australian National University for his insights into the regional defence, security and trade activities and the release of the US Strategic Framework for the Indo Pacific.

We also speak with Philippe Odouard, Managing Director of XTEK Limited and their recent MOU with Milram Robotics and defence applications for #drones and #robotic platforms.

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."

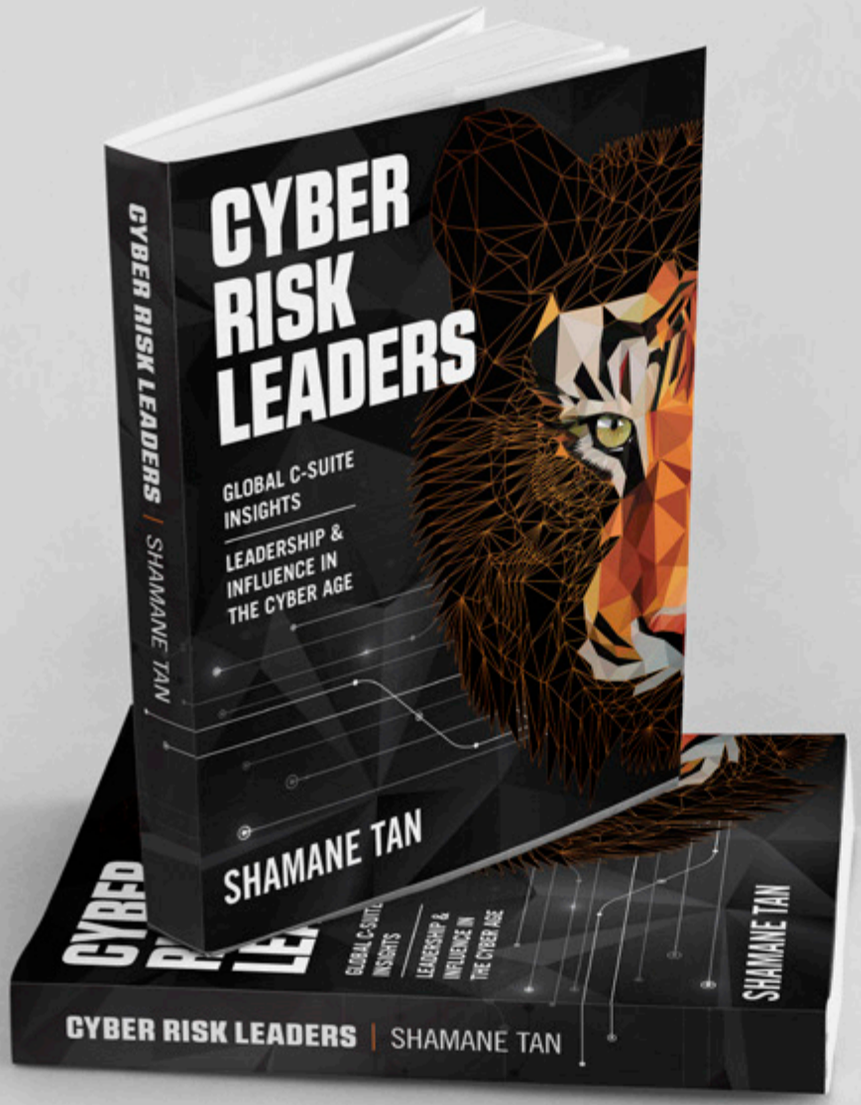
CEO, Cyber Security Capital (UK)

★★★★★

"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

MYSECURITY MEDIA

www.mysecuritymarketplace.com

CYBER RISK LEADERS

Cyber Security
WEEKLY PODCAST

MySec.TV
NEWS & INTERVIEWS

Download on iTunes

GET IT ON Google Play

MYSECURITY MARKETPLACE

THE HUB

ENGAGE WITH LEADING INDUSTRY BRANDS

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

REGISTER FOR ACCESS

PROMOTE YOUR BRAND

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

CHECK OUT THE LATEST PRODUCTS

Access Control, Network security
Enable Zero Trust with RSA

Access Control
YubiKey 5C NFC

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

Endpoint Protection
Malwarebytes Endpoint Detection and Response

www.mysecuritymarketplace.com