CYBER RISK LEADERS

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

Issue 5, 2021

China's cyber military–civilian integration

Reworking American foreign policy on China

Biden & Putin Cybersecurity talks

Use of online communities by terrorists

CIO Survey – Specialists

Remain In high demand zero trust security model

Secure network transformation

Migrating MPLS networks to the cloud age

THE RANSOMWARE WAR

Cyber Security Weekly Podcast

Cyber security weekly highlights

PLUS

MySec.TV

MySmartTech.TV

Top Women in Security

ASEAN REGION 2021

AWARDS CEREMONY – 5:00pm SGT | TUESDAY | 31 AUGUST 2021

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).

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.

The awards will take place at a virtual ceremony at **5:00pm SGT, Tuesday, 31 August 2021**.

REGISTER HERE

Please Register to attend the awards.

ORGANISERS

WISECRA
WOMEN IN SECURITY & RESILIENCE ALLIANCE

MYSECURITY MARKETPLACE

Cyber Outstanding Security Performance Awards

Recognising and rewarding outstanding performance across the cyber security sector globally

Inaugural awards coming soon

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

www.thecyberospas.com

@theOSPAs

The Outstanding Security Performance Awards

New workspaces + new tools = new risks

Work securely from anywhere with modern authentication

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

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

SecurID™
An RSA Business

SECURITY
EXHIBITION + CONFERENCE

Elevated Intelligence

For a Smarter, Changed World

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

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

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

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

17–19 NOV 2021
ICC Sydney
Darling Harbour

REGISTER NOW
securityexpo.com.au

Lead Industry Partner

ASIAL
AUSTRALIAN SECURITY INDUSTRY ASSOCIATION LIMITED

Co-located with

INTEGRATE
in partnership with
infocomm

SASE Security With True Data Protection

Make SASE real for your organisation.

forcepoint.com

MYSECURITY MARKETPLACE

CYBER WARS COLLECTION

An exclusive collection created for cybersecurity awareness

SHOP NOW

www.mysectv.shop

CYBER RISK LEADERS

Director & Executive Editor
Chris Cubbage

Director
David Matrai

Art Director
Stefan Babij

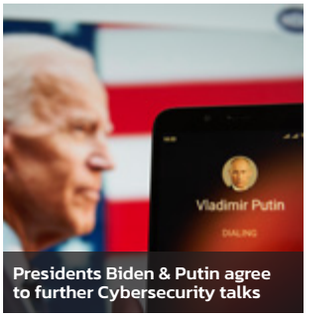
MARKETING AND ADVERTISING
promoteme@mysecuritymedia.com

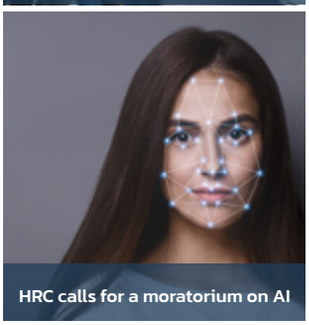
CONNECT WITH US

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

OUR OTHER CHANNELS

MySecurity Marketplace
Best in Tech
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
MySmartTech.TV





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

Geoffrey Coley
Kelly Johnson
James MacHaffie
Alan Cunningham
Andrew Curran
Guy Matthews
Ashish Shrivastava

"If we end up in a war – a real shooting war with a major power – it's going to be as a consequence of a cyber breach of great consequence and it's increasing exponentially"

– USA President Joe Biden,
visiting the Office of the Director of National Intelligence, 27 July 2021

In our previous edition, we referred to the world starting 2021 in the midst of an inflection point. You may have noticed not much has changed. The year continues much in the manner it started.

The January 6 insurrection of the US Capitol by pro-Trump rioters who were trying to stop the certification of the presidential election is but a distant memory for many. Yet still under review, currently with hearings being held by the Democratic-led House select committee.

COVID19 retains its grip, yet vaccine rollouts are gaining some momentum. The Delta variant, a highly contagious SARS-CoV-2 virus strain, officially named B.1.617.2., is reported to be as contagious as chickenpox and the World Health Organization has called this version of the virus "the fastest and fittest."

Alongside COVID19 and the misinformation campaigns, reliance on remote working and home schooling has made communication systems evermore critical. Cyber-attacks, phishing campaigns and most notably, ransomware have gained notoriety and continue to threaten critical infrastructure and supply chains. A number of high-profile cyberattacks include against critical United States infrastructure and has motivated some governments, namely Australia and the US, to consider the introduction of mandatory reporting of ransomware attacks to stem the flow of ransom payments.

Following his June meeting with the Russian President in Geneva, President Biden said he wanted Russia to take a tougher stance on homegrown cyber threats. The President highlighted hackers had extorted hundreds of millions of dollars from organisations worldwide. "We made it clear we were not going to continue to allow this to go on," President Biden said. "He (Putin) knows there are consequences. We agreed to task experts in both our countries to work on specific understandings about what is off-limits. We need some basic rules of the road that we can all abide by."

Just weeks following this meeting, Russian cyber gang REvil launched an attack on MSP provider Kaseya, claiming more than a million systems were infected and offered the universal decryptor key for $70 billion in Bitcoin. In response, working with government agencies and several cybersecurity firms, Kaseya came up with a decryptor key within three weeks after using various patches to manage the problem. By mid-July, REvil stopped communicating and some commentators have speculated US government agencies successfully disrupted the online criminal gang. There is also the suggestion the Russian Government put pressure on REvil to go quiet in the face of global publicity. Unlike some recent high profile ransomware victims, Kaseya confirmed it did not pay any ransom.

Coinciding with the Kaseya attack, on July 19, the White House announced in a background press call, "The United States has long been concerned about the People's Republic of China's (PRC) irresponsible and destabilizing behavior in cyberspace....the U.S. and our allies and partners are exposing further details of the PRC's pattern of malicious cyber activities and taking further action to counter it, as it poses a major threat to the U.S. and allies' economic and national security. The PRC's pattern of irresponsible behavior in cyberspace is inconsistent with its stated objective of being seen as a responsible leader in the world."

US Allies, including Australia, United Kingdom and European Union determined that China's Ministry of State Security exploited vulnerabilities in the Microsoft Exchange software. In a Joint statement, Australia claimed, "These actions have undermined international stability and security by opening the door to a range of other actors, including cybercriminals, who continue to exploit this vulnerability for illicit gain."

As a sign of what lays in store, the Australian Government is introducing intrusive powers when a cyberattack threatens critical infrastructure assets and the national interest. While admitting provisions in the proposed bill could prove onerous to some entities, Mike Pezzullo, Secretary of the Department of Home Affairs strongly backed it. "We think the bill strikes the right balance between specificity and detail on the one hand and general principles on the other hand." Apparently, there is no time to lose. "We're already past time," Mr Pezzullo said at a Parliamentary Hearing, referring to the cybersecurity legislation. "The clock is ticking ... the imperative is so overwhelming that we are probably past time."

Pezullo's urgency should not be overlooked and more so, as President Biden also refers to War. In April, Mr Pezzullo made headlines with reference to the beating drums of war, when he said "Today, as free nations again hear the beating drums and watch worryingly the militarisation of issues that we had, until recent years, thought unlikely to be catalysts for war, let us continue to search unceasingly for the chance for peace while bracing again, yet again, for the curse of war."

And just last week, the US Cybersecurity and Infrastructure Security Agency (CISA), the FBI, UK's National Cyber Security Centre, and the Australian Cyber Security Centre (ACSC) teamed up with an advisory listing 30 key vulnerabilities cyber actors are currently exploiting, including the vendors, products, and Common Vulnerabilities and Exposures (CVEs) associated with these vulnerabilities. But there are concerns the advisory fails to address the role human error plays in helping facilitate cyberattacks.

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 ransomware, US and China relations 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

25TH ANNIVERSARY WatchGuard

Q1 2021 Internet Security Insights

WatchGuard Threat Lab

The Firebox Feed recorded threat data from

37,409

participating Fireboxes

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

Our GAV service blocked

8,599,420

malware variants

55% decrease in basic malware

APT Blocker detected

8,434,602

additional threats

16% increase in zero day hit

Intelligent AV blocked

203,895

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

Firebox

26.4% OF MALWARE WAS Known Malware

73.6% OF MALWARE WAS ZERO DAY

High-Level Threat Trends for Q1 of 2021

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

New and Notable Threats

XML.JSLoader

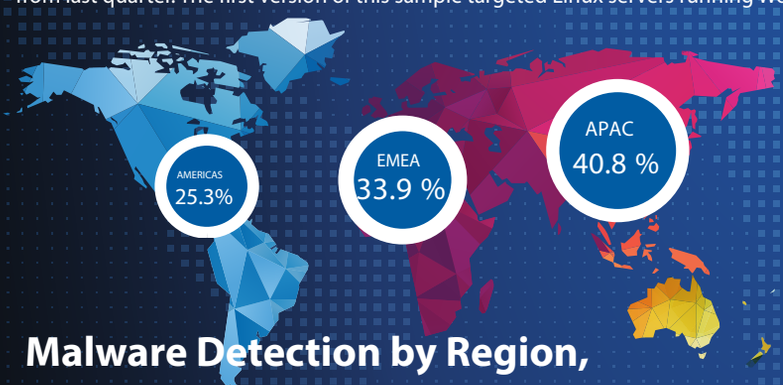
The character data (CDATA) found in the malicious XML sample contained a script that exploits an input validation flaw to ultimately launch PowerShell. The PowerShell command, hidden from the local victim, leveraged fileless techniques to download additional malware, which could take screenshots of your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

Zmutzy (Nibiru ransomware)

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

Linux.Ngioweb.B

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



Malware Detection by Region,

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

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

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

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

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

+65 3163 3992 INQUIRY.SEA@WATCHGUARD.COM WWW.WATCHGUARD.COM

New workspaces + new tools = new risks

Work securely from anywhere with modern authentication

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

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

SecurID™
An RSA Business

The ransomware war: avoid the inevitability of ransomware losses

By
Geoffrey **Coley**
Director, Strategy and Architecture for Asia South and Pacific region, Veritas Technologies LLC

A hacker group mounts a stealthy, days-long, brute-force attack on your enterprise's networks but fails to gain access. Cyber criminals test millions of passwords against a corporate sever in a massive credential-stuffing attack but get nowhere. Then, an employee clicks on a convincing link in a homograph attack, and all that hard work falls by the wayside as hackers breach the corporate network.

Despite doing everything right with your security strategy, malware is now in your network and hackers have begun silently profiling your physical, virtual and cloud-based storage in preparation for an attack. Weeks later, confident they've infiltrated the most critical IT services, they steal your sensitive data, and then use the original malware to activate ransomware that encrypts data, destroys infrastructure and wipes backups.

Your business is at a standstill, your critical data is being held hostage, and the price tag on the decryption key that will unlock your systems is tens of thousands of dollars, if not more.

This nightmare scenario has become a reality for more and more organisations in 2020. According to the Veritas 2020 Ransomware Resiliency Report, 45 percent of Australian organisations reported that their company had reported at least one ransomware attack. These attacks were extremely disruptive, with 64 percent of Aussie companies estimating that it would take five or more days to fully recover from a ransomware attack, if they didn't pay the ransom.

Such attacks are also escalating in today's digitalised setup. The Australian Cyber Security Centre's cyber threat report shows that it responded to 2266 cyber security incidents in 2019-20, including targeted reconnaissance, phishing emails and malicious software affecting larger organisations, supply chains and government entities.

With more than half (57 percent) of Australian organisations confessing that security measures have not kept pace with IT complexity, experts agree that 2021 will bring even more sophisticated and targeted attacks. Every business should assume that it is a target and plan from there. The key is a belt and braces approach that adds data backup and recovery to IT security to help prevent, contain and recover from ransomware. Furthermore, organisations must understand the notion of data management as a framework or methodology and consider the value and risk of data, including its lifecycle from "cradle to grave". We're seeing regulatory and compliance building around this.

Escalating IT complexity

Whilst you can't stop every attack, prevention strategies can minimise the number of hacking attempts that become successful. Data protection, with multiple layers of defense deployed including firewalls, email and spam filters, anti-malware endpoint protection software, and user education should be every company's first line of defence.

However, growing IT complexity created by the extensive adoption of multiple different cloud platforms, and greater use of distributed data centers, hybrid cloud operations and multiple storage and data protection

suppliers (data fragmentation) makes IT security even more difficult to assure.

As a result, IT leaders should always assume that their IT security measures will inevitably be breached and, as they struggle to defend increasingly complex networks and avoid ransomware, a sound backup and recovery strategy is critical.

It's no surprise that this IT complexity makes backup and recovery more difficult. Despite experts cautioning against giving in to ransom demands, since full decryption is not guaranteed, many companies are forced to pay at least part of what is demanded, because their backup and recovery measures prove inadequate to retrieve their data.

Veritas' research showed that companies that paid a ransom in full typically used twice as many cloud providers as those that were able to avoid payment.

Backup and recovery best practices

Backups won't prevent an attack or stop a hacker from releasing sensitive data, but an effective backup and recovery strategy is a safety net that has saved many businesses from disaster. This requires multiple copies of all valuable and critical data, and these copies must be both complete and current, with one stored offline for airtight security.

Here are five practices for recovery to keep in mind:

- Execute backups regularly: To limit damage from a ransomware attack, run backups at least daily, and employ continuous data protection on critical data, to shrink your Recovery Point Objective (RPO). This will reduce potential data loss to levels that minimise the impact to the business. Also regularly practise recovering data, in an automated or orchestrated way, to ensure that the right information is being protected, and that systems can be brought back on-line in a timely manner. AI can now also help to 'selfheal' backup sets that become corrupted.
- Store backups in multiple locations: The best practice for backup is to keep three or more copies of your data, on at least two different types of media (e.g. local disk and public cloud), one of which is offsite and offline (the '3-2-1 principle'). However, 27 percent of the Australian companies covered in the 2020 Veritas Ransomware Resiliency Report had failed to put off-site backups in place. Keeping backup copies of your data in off-site locations makes it harder for hackers to capture all copies of your data, because ransomware can typically only encrypt the files and data that it can access directly.
- Harden backup platforms: Ransomware will often encrypt the operating systems and data stores of many backup platforms. Thus, you need backup solutions that are protected against malware and have intrusion detection systems built-in. These hardened systems can often be used to restore other backup environments, further improving network protection. It goes without saying that you must be vigilant in updating backup software regularly, to address known vulnerabilities and improve functionality.
- Consolidate backup solutions: Many cloud and SaaS providers offer in-build data protection as an add on, and many data protection companies specialise in protecting specific environments or workloads. However, these solutions can add to IT complexity, making it harder to enforce consistent and comprehensive backup policies. Importantly, they can significantly complicate the process of restoring data in the wake of an attack, as administrators grapple with multiple tools and platforms at an already stressful moment, as they try to reassemble the primary data set.
- Understand your data: Unless and until a business understands what data it has and where, it's impossible to build an effective backup and recovery strategy. Veritas research shows that 52 percent of business data is 'dark', meaning the organisation doesn't know what it, or its value, is. Once an organisation gets on top of this challenge, they're able to back up all the data that's important to them.

We can be sure that malicious ransomware attacks will continue to pose critical threats and are becoming more sophisticated and potentially devastating. The time to act is now; for security and peace of mind, assess your backup and recovery strategy, and make your backup processes more robust, no matter where your data and applications are hosted.

Yes ransomware is scary, but you don't have to be a victim

By
Kelly **Johnson**
Country Manager, ESET
Australia

Ransomware is not new but for most of its history it has not been the headline-grabbing threat it has become in the last few years. Today's ransomware plague is essentially the product of a perfect storm of technology – both that deployed by attackers and that used by victims – combined with a maturing of the tactics criminals use to enact ransomware attacks.

While ESET Research has seen a decline in the detection of ransomware attacks in both late 2020 and the first part of 2021, this decline in detections isn't the good news it might appear to be. Instead it reflects a growing sophistication in how criminals launch these attacks. The days of embedding malicious code in email or website links and hoping someone clicks have been replaced by a targeted approach, with criminals paying other criminals for hacked access to networks or launching brute force attacks against networks via remote access.

Ransomware has become the last stage of a chain of events leading to a network being compromised and the criminals who launch the final attack may not be the ones responsible for compromising the network in the first place. They also are often not the authors of the ransomware code they deploy. Sophisticated operators have moved to running a ransomware-as-a-service model, giving other criminals access to their code in return for a portion of any ransom they obtain. This lowering of the technical skill needed to 'enter the market' combined with large earnings some gangs have made from high-profile attacks has helped power the growth in groups launching attacks focused on high-profile targets.

Another factor fuelling the boldness of recent attacks, such as the attack on Colonial Pipeline in the US that shut down its pipeline and created fuel shortages, is a change in blackmail tactics. While attackers are still encrypting systems and demanding payment in return for giving the victim the ability to unlock these systems, they are also frequently stealing data and using a very public threat of its release to pressure the victim to pay up.

In the recent attack in New Zealand on the Waikato District Health Board, the attackers emailed stolen patient data to news outlets as proof that they had the ability to make good on their threats in an attempt to put public pressure on the DHB. One gang that targeted several high-profile victims in the US even made a public announcement that it will not encrypt victims' data anymore and planned to focus solely on data theft and extortion.

Finally the rise of cryptocurrency has provided perhaps the most vital boost, creating an almost tailormade payment system that is low risk for the offender and comparatively easily laundered. The fact that the FBI

recovered the bulk of the money extorted from Colonial Pipeline appears to have had more to do with the criminals lack of sophistication in Bitcoin laundering than it does the ability of law enforcement to block cryptocurrency as a payment system for extortion.

And the money to be made for such low-risk crimes is substantial. Meatpacker JBS paid a ransom in Bitcoin equivalent to $US11 million to end the attack that disrupted both its North American and Australian operations, with its CEO Andre Nogueira saying that "we felt this decision had to be made to prevent any potential risk for our customers". Despite both governments and security companies worldwide, including ESET, recommending victims not pay ransoms to attackers, JBS clearly felt that the ultimate cost of its operations being shut down for an extended period was worse than paying off the attackers. As long as victims feel they have no choice but to make this decision, ransomware will continue to escalate.

Nor should the increase in such high-profile attacks against major enterprises make smaller businesses think they are safe from attack. A ransomware attacker is first and foremost attacking your reputation. Whether they are encrypting your systems or holding your data to ransom, the pressure they are bringing to bear is based on how much reputational damage they think you are willing to sustain. Smaller companies are just as susceptible to this as large enterprises and it is likely that the scale of attacks on SMBs is largely under-reported, since no one wants to disclose they've been a victim of an attack unless they have to.

All of this points to ransomware continuing to be a major threat for the foreseeable future. Which means you need to plan to protect yourself from a successful attack as well as to mitigate any damage and provide for a quick recovery if the worst happens.

Most of the measures businesses should take to strengthen their defence against ransomware are not new. But it's never a bad time to revisit and audit your defences:

Cybersecurity training for staff

The process of compromising your network's security can start at multiple places and the most obvious remains human error by your staff. Exploiting poor cybersecurity awareness is one of the most popular methods for attackers attempting to breach your security and ensuring that all staff are properly trained on cybersecurity best practice goes a long way to mitigating this risk.

Use a multi-layered security solution

'In 2018, for example, an RDP attack against LabCorp, one of America's largest clinical laboratories, allowed the attacker to compromise 7000 systems and 350 servers even though the attack was contained by the company within 50 minutes.'

So you're not a specialist in security? Good news, there are people who are and they make some fantastic products. Besides your employees, a good multi-layered solution is your first line of defence to protect you not just from ransomware but everything that cyber criminals will throw at you. No solution is perfect, and like everything they need to be properly configured and kept up to date, but without a solution you might as well be offering cyber criminals tea and cake.

Lock down remote access

An RDP endpoint is a device, such as a database server, that is running Remote Desktop Protocol (RDP) software so that the device can be accessed over a network, including the internet. It's a convenient way for staff, particularly IT staff, to be able to access your systems no matter where they are, but it's also a security risk if not set up properly.

Gaining unauthorized access via RDP has significant benefits for threat actors; it has the potential to evade endpoint protections and allows the perpetrator to rapidly compromise multiple systems within a single organisation. In 2018, for example, an RDP attack against LabCorp, one of America's largest clinical laboratories, allowed the attacker to compromise 7000 systems and 350 servers even though the attack was contained by the company within 50 minutes. Investors later sued the company claiming that the company's board failed to address security problems that led to financial losses.

Businesses have fallen victim to ransomware attacks because they have left RDP endpoints protected only by a username and password. Usernames are easily deduced and passwords can be brute-force broken by code. Ensuring that access is locked out after a limited number of wrong attempts to enter a password is a simple fix that many businesses fail to implement.

You should also be aware of what RDP endpoints you have and who has access to them. A regular audit to ensure that unnecessary remote access points are terminated rather than left in place is also critical. The forgotten remote access point is a disaster waiting to happen.

Secure your endpoints

COVID-19 saw an explosion in the number of endpoint devices accessing many companies' networks as workers relocated to home and in some cases used their own devices to access the network. Ensuring that endpoint protection software is running on such devices, and is properly configured, is essential to maintaining the integrity of your network.

Keep up to date

It should go without saying that your systems should always have updates and patches applied but sadly this is not the case with many businesses. Lack of in-house IT resources or the inability to apply upgrades to out-of-date legacy systems that remain mission-critical can lead to known vulnerabilities remaining unaddressed for months or even years past the point when a patch was issued for them. Leaving these vulnerabilities in place is no different to gambling. Eventually the house wins and you lose.

Limit what you put online

Digital transformation is driving a dramatic shift in how much data companies routinely trust to be accessible in some form online. You need to assess the trade-off between business benefit and the risk of putting some data into an online environment, so audit your exposure and balance convenience with security.

Back it up

Yes you're always being told to maintain backups. It's a refrain as old as IT. But in the age of ransomware it takes on a new urgency. Maintain backups of critical data and check those backups regularly to ensure their integrity. Store the most valuable data off-line.

Have a plan

Business continuity plans, like backups, are one of those things everyone knows they should have, and really, they will get around to doing it one day. Don't be caught with the need for such a plan without the existence of one.

CYBERSECURITY
EXPERTS ON YOUR SIDE

COMPLETE PROTECTION FOR YOUR BUSINESS

For more than 30 years, ESET® has been developing industry-leading IT security software and services to keep businesses safe from evolving threats.

AT THE GLOBAL FOREFRONT OF RANSOMWARE DEFENSE

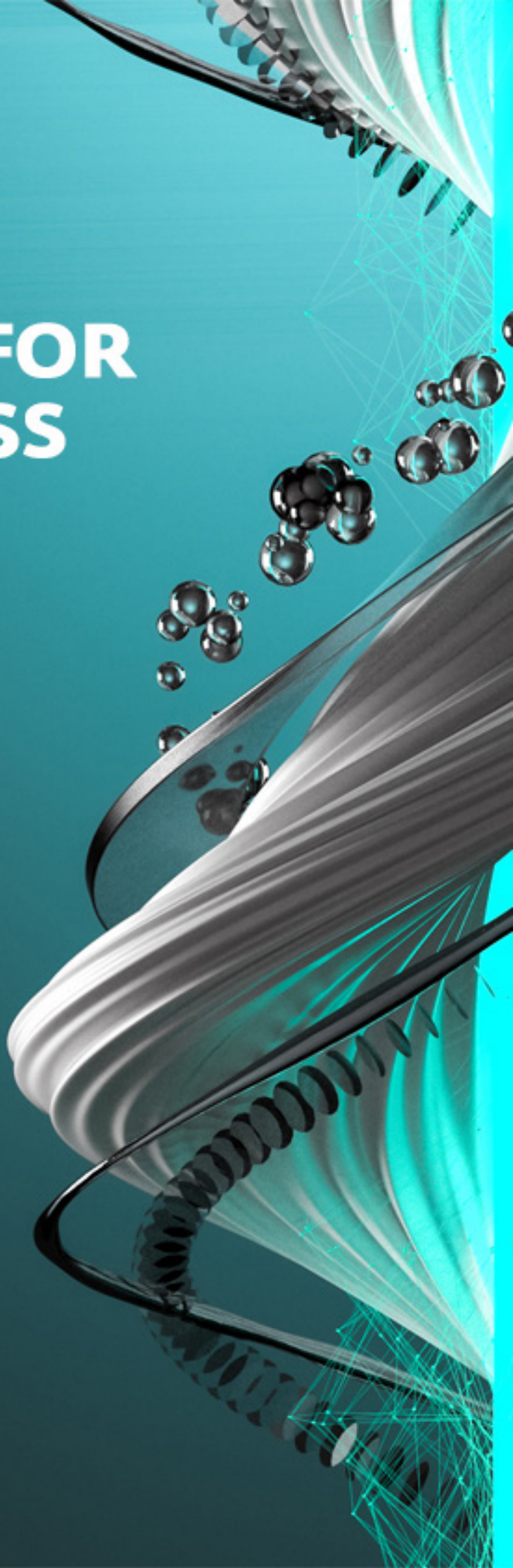
110M+
users are protected by our technology

400K
business customers in 200+ countries and territories

13
global Research & Development centers

30
years of continuous technology innovation

Learn how we can help you secure everything that matters to your business.



China's goals and future prospects for cyber military–civilian integration

By James **MacHaffie** independent analyst on Asian security topics, including cybersecurity. He holds a doctorate in international politics from the University of Leicester.

China's cyber security strategy, first enounced in 2016, has evolved under Xi Jinping. It has become multilayered, with both civilian and military components that interact with each other. This military-civilian fusion (MCF) (junmin ronghe,军民融合) is integral to China's cyber superpower ambitions. (China Brief, 2019) The ultimate goal is for China to become a "cyber superpower" (Wan luo qiang guo, 网络强国).

Xi Jinping delineated this goal in a speech on April 19, 2016. ("Speech at the Work Conference for Cybersecurity and Informatization," Zai wan luo an quan he xin xi hua gong zuo zuo tan hui shang de jiang hua, 在网络安全和信息化工作座谈会上的讲话) (Xinhua, April 19, 2016) Both Xi and the Chinese Communist Party (CCP) see the control of cyberspace as critical for the long-term survival of the regime.

The first civil-military cybersecurity innovation center was unveiled in late 2017. (People's Daily, December 28, 2017) In China's peaceful rise to great power status the CCP has sought to project the image of strength, uniformity, and internal stability. (Xinhua, January 24, 2020) To that end, Xi has spearheaded efforts to restrict Internet access, and make China more resilient in the cybersphere, with the ultimate goal of having cyber sovereignty. In other words, to stifle dissent and exclude Western states as much as can be enabled.

MCF's Two-Pronged Strategy

Beijing has denoted what amounts to a two-pronged strategy on cybersecurity with MCF, utilizing both military and civilian sectors, which overlap. The People's Liberation Army (PLA) has taken the lead in Xi's cyber strategy, recognizing the important role cyberspace plays in "informatized warfare." (Xin xi hua zhan zheng,) (Xinhua, September 24, 2019). In the most recent Defense White Paper (Xinhua, July 24, 2019), the PLA recognizes cyberspace as a "security threat" to China (Yan jun an quan wei, 严峻安全威). As such, the Chinese military, working in conjunction with the civilian sector, especially the Cyberspace Administration of China (CAC) has made enhancing its role in cybersphere activity, looking for threats, a priority. (PLA Daily, September 14, 2020)

The PLA's role in domestic surveillance is slight, as its focus is on foreign (mainly US) influences on China's cybersphere, with the Strategic Support Force being the lead agency in cyber warfare and security issues. (China Brief, 2016) However, recipients of foreign communications, if deigned harmful to the regime from a national security perspective, may be monitored, and punished under the national security laws. (SCMP, April 28, 2020) The main onus on implementing and overseeing the cybersecurity laws

will fall on the CAC. The Cyberspace Administration was founded in 2014, tasked with ultimately implementing Xi's cybersecurity policy. (Qiushi, September 16, 2018) The CAC decides which websites will be censored, and what content will be filtered through its firewalls.

While the coordination between the CAC and PLA Strategic Support Forces is loose, they still represent the two governmental organs that are responsible for implementing Beijing's cyber strategy. The intersection of military and civilian control of Chinese cyberspace is consistent with Xi's centralizing of power within the CCP bureaucracy itself, with centralized control of China's cybersphere the ultimate goal. (PLA Daily, March 15, 2018)

Xi and the CCP, for the last several years, have incrementally been attempting to centralize control over China's cybersphere. Beijing continues to establish innovation centers around the country to not only showcase and upgrade China's technological innovations, but also to establish a link to MCF. (Xinhua, January 20, 2021) The point of these centers is twofold. One reason is to make the Chinese public more comfortable with the MCF notion, as the party-state realizes its goal to become a cyber superpower, and also to ideally mute any domestic dissent to the idea. The second reason is to set up recruiting posts for the PLA SSF. The centers provide a ready manpower pool for the Strategic Support Force and other units that the PLA may want to establish.

There are some drawbacks to Xi's push for military-civilian fusion, and increased governmental control over the Internet, namely that the people will push back against it. So far, Beijing has gambled that the rewards are worth the risks. The recent unrest in Hong Kong may have encouraged an acceleration of MCF, as the regime worries the Internet could be used for greater popular mobilization against it. Currently, the protest movement has been stifled, no small part due to enforced quarantines during the coronavirus pandemic. However, with the implementation of the new national security law (香港国家安全維持法) for Hong Kong, and its draconian punishments, the situation may change rapidly for Beijing. (Xinhua, June 30, 2020) The law does not specify the utility of MCF in Hong Kong, but the semi-autonomous region might prove to be a test case for the regime's integration plans. (For the law itself see: Xinhua, June 30, 2020)

MCF Integration after the Covid-19 Pandemic

Since the Covid-19 pandemic began, Beijing has sought to strengthen and expand MCF. (People's Daily, May 13, 2020) This is, perhaps, the next stage in the development of the military-civilian integration plan that Xi and the CCP envision. (Cyberspace Administration of China, March 13, 2018) This acceleration of MCF has not gone without notice by the United States, and other foreign states. Beijing experienced significant criticism during the Covid-19 pandemic, particularly from the Trump administration, for its handling of the coronavirus situation to perceived meddling in the 2020 US presidential election. (Nikkei Asia, October 28, 2020) Part of this criticism focused on China's military-civilian fusion to the point the United States has blacklisted several Chinese companies with strong links to the PLA. (The Diplomat, November 30, 2020)

China has pushed back on these criticisms, stating that the US, in its history, has commonly practiced MCF, and that China will take all necessary measures to protect its interests. (Beijing Daily, December 3, 2020) The criticism from the US and its allies has caused consternation from China, as Beijing continues to denounce the criticism. (Foreign Ministry of China, January 15, 2021) Despite this, or perhaps because of, the hostility Xi remains adamant that China will continue on its path of technological development, creating a new cybersecurity paradigm, which includes military-civilian fusion. (China Daily, November 24, 2020) It is a stance that Beijing is not backing away from, and appears unwilling to compromise on. (Cybersecurity Administration of China, March 15, 2021)

China plans to establish more innovation centers in the future, promote more reforms, and promote Xi's vision of China as a technological superpower on the cutting edge of modernization. Many of these changes have seemingly benign intent, to improve the standard of living among everyday Chinese. However, beneath that veneer the party-state seeks to exert its total control over the cybersphere. This control, ideally for the CCP, will occur gradually over time, in order to avoid any dissent, either domestic or foreign, to its ultimate goals.

To that end, military-civilian integration on cyber initiatives will continue, and may accelerate yet again. Along with Xi, the PLA has pushed back against American assertions that military-civilian fusion is anything but benign. (People's Daily, November 13, 2020) For China's military, MCF serves as a conduit for fresh recruits to the Strategic Support Force and other units that conduct informatized warfare, where the PLA is increasingly convinced any conflict with the US will be conducted. China also worries about the Internet as a staging ground for anti-regime activism, and would prefer to have this unpredictable medium under more control.

Conclusion

Military-civilian fusion is not a new concept for China, nor did it start with Xi Jinping, however it is integral to the party-state's strategy on making China a cyber superpower and ultimately centralizing control of cyberspace. This integration is not exclusive to the cybersphere, but it does play a key role in how Beijing wants to shape its cybersphere for the future.

If military-civilian fusion is to succeed for China, then it must be done through a compliant population, or at least an unsuspecting one. The expansion of cyber innovation centers throughout China serves the purpose of both mollifying the people and recruiting fresh talent into the PLA. However, Xi must walk a tightrope between two extremes in this approach. Move too quickly on military-civilian integration and it risks alienating the people, and foreign adversaries alike. Move too slowly and Beijing risks losing its moment to obtain more control over its cyberspace and create momentum toward cyber sovereignty.

'Military-civilian fusion is not a new concept for China, nor did it start with Xi Jinping, however it is integral to the party-state's strategy on making China a cyber superpower'

Shifting Interests: How the Biden Administration can rework American foreign policy on China

By Alan **Cunningham**

It goes without saying that China is becoming a very large and serious power. Since the late 1970s, China has grown exponentially as an economic powerhouse, combining standard Capitalist and Communist economic models while being set "to become the third largest economy by 2030".

Militarily, within the past twenty years, China has evolved from "a sizable but mostly archaic military" to one that is ahead of the United States in the form of shipbuilding, air defense systems, and conventional ballistic/cruise missiles while also taking steps to become pioneers in cyberwarfare and introducing "new military hardware" into their military systems. China has, diplomatically, militarily, and economically become a truly imposing force and poses a real threat to U.S. and Western interests in the Asia-Pacific region and elsewhere.

Given the extreme importance that China has upon global affairs, it is apparent that a new shift has come with the Biden administration. Recently, at the G7 summit, President Biden tried to "persuade fellow democratic leaders to present a more unified front to compete economically with Beijing" by calling out China's human rights abuses while also considering opening up talks with Xi Jinping to discuss these issues. This is a marked shift from Trump's more Chinese benefiting policies.

In my view, countering China's long-term ambitions or goals is difficult as, like the United States, they are quite sure of themselves and their positions and are determined to succeed in their individual desires. The American position on China is also in need of reform and reworking.

The Center for American Progress has described U.S. policy in dealing with China in this way, stating, "the United States has pursued a strategy that is fundamentally flawed. Instead of channeling public resources to support American innovation and invest in American workers, Washington assumed the United States could coast on a combination of natural comparative advantages and status quo technology dominance, much of which stemmed from investments made decades earlier. That approach has not worked. China is investing heavily in emerging technology sectors—such as artificial intelligence and next-generation mobile communication—to successfully chip away at U.S. technology leadership and global market share. However, in the United States, many workers are unable to find good jobs in the information economy. In sum, the United States has lagged on the very areas of strength it needs to compete against an increasingly powerful China".

U.S. policy has been one that, at first, has ignored China, with it only being recently that the U.S. has actually started paying attention to the serious economic and technological challenges and threats that China has. Examining just one issue, it is known that the U.S., in a technological and cybersecurity format, is massively unprepared for cyber

threats and technological intrusions by hacking groups, foreign powers, and individual hackers looking to siphon information.

It is known as well that China is one of the largest perpetrators of cybercrime and are immensely capable of committing electronic and technological intrusions of U.S. systems and infiltrating the private industrial sector. In terms of what the U.S. can do to combat this and to form a front against increased Chinese ambitions that may be harmful to domestic policies and American interests, the U.S. should create an alliance combined with similar world powers to stand against increased Chinese economic and technological dominance and commit more resources and effort towards improving the security of our industrial and technological forms.

Center for Strategic and International Studies recommends a similar approach, though they recommend this in dealing with Xi Jinping's economic strategy, the Belt and Road Initiative. They recommended that, "The U.S. government should take the lead to develop and implement a formal integrated multilateral infrastructure development mechanism that can effectively compete with the BRI to counter China's geopolitical gains.

Toward this end, an Infrastructure Development Coalition (IDC) should be formed by combining the national infrastructure development programs and initiatives from the United States, Japan, Australia, New Zealand, India, France, and Germany. Only by combining the resources and expertise of these programs can the United States and its allies and partners effectively compete with the BRI. More importantly, what will allow the United States and its allies and partners to counter the BRI's geopolitical gains is how the organization, structure, and strategic focus of the IDC synergizes the capabilities of each nation's development program".

Having a tactic like this is potentially an effective one and would limit the reach of China's economic plan. A unified front too would prove to strengthen relationships with our allies and would allow the U.S. to try and counter Chinese interests.

There are many areas that must considered when using military power or force to deter an enemy from gaining further ground or influence without provoking a conflict that leads to physical combat. In my opinion, one of the best ways to combat Chinese influence is to gather the necessary allies to make a collective stand against aggression and improving our own country's security and internal defenses against infiltration; these recommendations are similar to what the Pacific Council on International Policy has recommended.

As I mentioned previously, China is exhibiting a stunningly effective ability to infiltrate U.S. government computer systems and databases and are exceptionally adept at cyber intrusion and industrial CI (counterintelligence) operations. Improving our country's counterintelligence reserves and the ability to root out foreign operatives is essential to combating any enemy, but especially Chinese intelligence. The Pacific Council suggests, "Leveraging China's desire for stability and prosperity at home to discourage destabilizing behavior, and to encourage its active participation in tackling global challenges...Rather than engaging in transactional bargains, U.S. leaders should continue to make the case to their Chinese counterparts that Beijing should refrain from provocative behavior, such as blocking sea lanes or freedom of navigation in disputed territories, and cooperate to solve global challenges like the North Korean nuclear crisis, because it is in China's long-term strategic interests to do so. Chinese leaders, including Xi, have reiterated over the years in speeches and in major strategic documents that China seeks to contribute to peace and stability in the world—and the United States should hold Chinese leaders accountable to this promise".

This is certainly an interesting tactic, applying pressure to force the Chinese government to hold up to the values they often claim to be for and appealing to the common threat of North Korea are viable tactics that may potentially work. As well, working with such a large adversary on a tactic both can find equal ground in may work in rebuilding or repairing the relationship and can assist in fixing incidences or problems that may occur within the South China Sea.

'China seeks to contribute to peace and stability in the world—and the United States should hold Chinese leaders accountable to this promise'

About the Author

Alan Cunningham is at Norwich University pursuing an MA in International Relations. He has gained admission to a PhD in History program at the University of Birmingham in the UK and will begin work as an AP U.S. History Teacher. He aims to become a U.S. Navy Officer in 2022. He has been published in the Jurist, Security Magazine, and the U.S. Army War College's War Room among others.

Presidents Biden & Putin agree to further Cybersecurity talks.

By
Andrew **Curran**
Staff Writer,
MySecurity Media

United States President Joe Biden has met with Russian President Vladimir Putin. High on the agenda was countering cyberattacks originating in Russia. President Putin denied Russia was responsible for most of the cyberattacks but admitted countering the threat was important.

Cybersecurity experts have welcomed the acknowledgement from Russian that ransomware and other types of cyberattacks are a pressing global problem. Insiders agree more than half the world's ransomware attacks now come from Russia.

Following the meeting in Geneva, President Biden said he wanted Russia to take a tougher stance on homegrown cyber threats. The President said hackers had extorted hundreds of millions of dollars from organisations worldwide.

"We made it clear we were not going to continue to allow this to go on," President Biden said on Wednesday. "He (Putin) knows there are consequences. We agreed to task experts in both our countries to work on specific understandings about what is off-limits. We need some basic rules of the road that we can all abide by."

The meeting follows several high-profile cyberattacks on critical United States infrastructure, including the recent Colonial Pipeline and JBS ransomware attacks.

The United States has marked 16 sectors as critical infrastructure that should be off-limits from cyberattacks. Those sectors include telecommunications, healthcare, energy, and food.

"We need to throw out all kinds of insinuations, sit down at the expert level and start working in the interests of the United States and Russia," Putin said at his media conference following the meeting. The Russian President said the specific details and commitments to counter cyberattacks were yet to be worked out, but negotiations would commence.

The proposed cybersecurity discussions have met with a positive response from cybersecurity insiders. Meg King, Director of the Science and Technology Innovation Program at The Wilson Center in Washington, DC, said;

"President Biden's announcement that the US and Russia will task experts in both countries to address the threat of ransomware attacks being carried out within Russia to discuss what's off-limits and to follow up on specific cases is critical.

"Sold as a mutual interest, which President Putin confirmed separately, this technical working group will deepen and create relationships necessary to get a better early warning about criminal hacking groups and agree on efforts to stop them. Putin's comment that 'we need to get rid of insinuations' and 'begin consultations on this topic' suggests that Russia will cooperate, at least at the working level."

"We'll see where it goes," says cybersecurity expert Rick Newman from Yahoo Finance. Newman notes not all cyberattacks from Russia are sponsored by government or intelligence agencies there. But says the country offers a safe harbour to hackers providing they don't attack Russian interests. Newman says this needs to stop.

"He could crack down on them if he wanted to," Newman said about President Putin.

Cyber Security
WEEKLY PODCAST

Working in partnership with law enforcement – ESET cybercrime investigations

Alexis Dorais-Joncas
Head of R&D ESET
Montreal Branch

Download on iTunes

GET IT ON Google Play

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

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

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

00:00 00:00

LISTEN HERE

Cyber Security
WEEKLY PODCAST

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

Mary Jo Schrade

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

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

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

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

Download on iTunes

GET IT ON Google Play

Cyber Security
WEEKLY PODCAST

The emerging role of bitcoin in spreading malware

Professor Dr. Christian Doerr

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

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

Episode 268 – THE EMERGING ROLE OF BITCOIN IN SPREADING MALWARE

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

Download on iTunes

GET IT ON Google Play

00:00 00:00

LISTEN HERE

Europol sees increasing use of online communities by terrorists.

By
Andrew **Curran**
Staff Writer,
MySecurity Media

The European Union's law enforcement agency, Europol, says terrorists are taking advantage of the global pandemic to promote their various causes. Europol released the Terrorism Situation and Trend Report 2021 this week. The report warns COVID is having ramifications on how terror groups promote and recruit. Increasingly, terrorists are harnessing the online environment.

The report deals with terror trends and acts within EU member states. There were 57 completed, failed, and foiled attacks across the 27 EU member states in 2020. In total, 449 people were arrested for terror-related offences, and there were 422 concluded court proceedings.

Arrest numbers were down on previous years, and the number of terrorist attacks remained stable. But there is a distinct trend towards harder to detect unsophisticated lone wolf attacks. Europol suggests the pandemic could be one reason why.

"The online domain plays a crucial role in enabling violent extremists to spread their propaganda and sow hatred among potentially vulnerable and receptive audiences," said Catherine De Bolle, Executive Director of Europol.

The report found Jihadist terrorism remains the greatest threat to the EU. But the report also flagged the rising importance of online communities in right-wing terror activity.

COVID restrictions have hampered the ability of terrorists to organise large scale sophisticated terror attacks. Across Europe, targets like museums, churches and stadiums mostly remained closed.

With physical meetings more difficult, Europol noted a discernible increase in online networking. Organisers use the online environment to promote, recruit, and radicalise individuals. Concurrently, Europol noted radicalised individuals were becoming younger than usual, and the risk of lone-wolf attacks increased. This fits with the notion of young people sitting at home during the pandemic, interacting with online communities on their computers.

Europol says right-wing white supremacist or neo-Nazi groups, in particular, have increasingly relied on online communities to spread their propaganda and recruit members. The 2019 Christchurch shooting that killed 51 people was linked to transnational online communities.

"Suspects, linked to online communities with different degrees of organisation, are increasingly younger – with some of them being minors at the time of arrest. Right-wing propaganda is mainly disseminated online, and gaming platforms have been increasingly used for spreading extremist and terrorist narratives," said Europol in a statement.

The crime agency also suggests the pandemic increased social polarisation. This, in turn, increased wider acceptance of violent behaviour. Europol also believes the stress caused by the pandemic and associated restrictions may facilitate violence, especially among unstable or otherwise vulnerable people.

"Terrorists exploit different events, controversies and vulnerable individuals," said Claudio Galzerano, Head of Europol's Counter-Terrorism Centre.

Europol's Executive Director, Catherine De Bolle, used the report's release this week to call for greater investigative powers and increased co-operation from the private sector, particularly those operating online platforms that host extremist material and facilitate radicalisation.

De Bolle would like to see more real-time information sharing, greater uses of technology, and a stronger data protection framework. She argues this is essential to keep the EU safe from terrorism.

Cyber Security
WEEKLY PODCAST

Deepfakes, shallowfakes & cheapfakes – seeing is believing

Dr. Nasir Memon

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

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

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

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

00:00 00:00

LISTEN HERE

Download on iTunes

GET IT ON Google Play

CIO survey confirms Cybersecurity specialists remain in high demand

By
Andrew **Curran**
Staff Writer,
MySecurity Media

A growing IT skills shortage is seeing CIOs offer bigger salaries as they attempt to retain key workers. According to a recent survey, over 80% of CIOs are worried about losing their best IT workers. As a result, nearly 75% of those CIOs will offer their IT workers a pay increase this year.

Specialist global IT recruitment agency Robert Half released their 2021 Salary Guide on Monday, April 26. Included in that guide was a survey of 100 top CIOs. The Guide found the IT sector was thriving, but there is an increasing concern about a growing IT skills shortage, especially in the top tier and niche corners of the sector.

"There is an increased demand for tech talent as companies expand their IT teams and enhance their digital capabilities because of the pandemic," said David Jones, Robert Half's Senior Managing Director (Asia-Pacific).

The most in-demand workers have strong backgrounds in IT security, IT management, business transformation, development or design, and business intelligence. The recruitment agency says workers with skills and experience in these areas are well-positioned to receive pay increases this year.

"A demand-supply imbalance is driving wage growth in the tech sector," says Mr Jones.

Despite the pandemic and the shift to working from home, the survey found demand for top talent across all industries remains strong. Prospective employers are willing to headhunt, and CIOs need to deploy a range of incentives to retain their key IT workers.

While many industries shed workers during the pandemic, the IT sector proved resilient, with most IT workers retaining their jobs. In 2021, 30% of CIOs plan to increase their IT workforce. There is a particular demand for cybersecurity talent.

The pandemic hastened the shift to a digital environment. Coupled with that is an increase in corporate cyber risks. Strong cybersecurity defences have become a priority for companies investing and operating in the digital environment.

Cybersecurity specialists with a background in information security, network security, cloud security services, web security, and security architecture can expect to see a high demand for their services.

"Companies need experts to help avert future digital issues, such as ensuring cybersecurity is in place before a security breach happens," says Robert Half's Salary Guide.

But it's not all bad news for CIOs. While most are willing to pay more to keep their top IT talent, the pandemic reinforced the need for job security. Despite the best efforts of headhunters, many IT workers are reluctant to leave their existing employer, particularly if their continued employment seems certain.

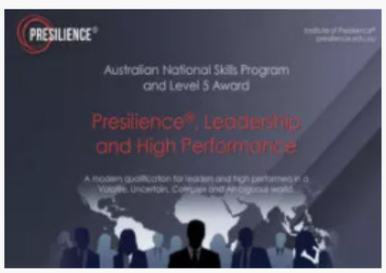
"Competition for niche skillsets such as cybersecurity remains tough as more workers stay with their existing employer," the guide says.

For companies not able to increase salaries, focusing on job security may be one way to retain key IT and cybersecurity workers. According to Robert Half, offering a range of worker incentives, such as working remotely and an improved work-life balance, can be highly effective in retaining key IT workers.

MYSECURITY MARKETPLACE

COURSES

Search and find all upcoming featured courses



Fri, Jun 18 10% Discount

Presilience®, Leadership and High Performance

Tue, Jun 01 $800

SCADA & ICS Cyber Security Course

Tue, Apr 13

Bachelor of Cyber Security

Plus many more!

Selecting winning solutions to ensure secure network transformation

By Guy **Matthews**
NetReporter

Everyone is agreed that the events in the past year have added a lot of fire and urgency to digital transformation. But what does that look like on the ground, at the enterprise coalface? Who is deploying what, and why?

To delve a little deeper into this issue, independent analyst firm GlobalData looked at its extensive database of CIO and CISO names to see what they have been spending on ICT services and where the money is going. Dustin Kehoe, Director, Research APAC & MEA Regions with the firm, was especially interested to drill down into what's happening in Singapore: "We looked at 3,000 accounts there, and right away noticed a dramatic increase of over 6% in spending in 2020 compared to 2019," he notes. "We expect that trend to continue. We've never seen a dramatic increase like that in Singapore before."

So where did all this spending go? Kehoe says the top investment areas were networking, cloud and data centre and security: "In terms of vertical markets, I see these three as increasingly interlinked," he believes. "The biggest growth areas for ICT spending we found to be healthcare, consumer goods and retail."

But what is the agenda that drives this all this transformation? What are the business drivers? "A business might want to move into an adjacent market, they might want to improve operational efficiencies," speculates Kehoe. "For that they need an IT system that's not going to tell them that a workflow that makes sense is not possible because it's not supported."

He gives the example of China and Live Streaming eCommerce: "It's a $60 billion industry and it works by instead of me transacting and buying my shopping online, I join up, via virtual reality, with celebrities and influencers and ask them questions directly in a live environment. They give me advice on the products that I'm interested in, phones, lipstick or whatever. It's the biggest growing live streaming industry in the market, and would not be possible without an amazing customer experience that is all about high capacity video, low latency networks, and a lot going on in between to create a look and feel that is like real time. Behind it all is a cloud-native platform."

As for other enabling technologies, Kehoe believes in APIs as important for promoting interoperability, as well as containers and microservices, and he sees a need for open source to change the culture through DevOps.

"But IT cannot do everything alone," he warns. "IT and line of business need to work with each other to create a change management framework. Without that you do not have transformation. We do not see digital transformation as just an IT project. We see it as a collection of many projects, multiple projects and skill sets and capabilities you bestow on an organization, so they can deliver their goods and services and bring them to market differently. That is why it is increasingly interlinked, interdependent to

business outcomes."

Units of compute, network and storage are getting smaller and smaller, notes Kehoe, and that means CIOs must start to think of infrastructure in terms of code: "It's about scalable applications, deployed without thinking about what sits beneath the hood. We want speed and agility without compromising security and compliance. You move too fast, you get security breaches. You move too slow you've lost the pace, your competitors have developed, you're losing market share and your physical customers have gone elsewhere."

Further ahead, Kehoe sees cloud and networking evolving to be both interdependent and highly decentralized: "Different types of networks, multi-service networks, will be running different sorts of cloud environments. We're also going to go from hybrid to multiple clouds, and underpinning all of this is SASE, identity and access management, data loss prevention and governance along with various methodologies."

To broaden the conversation on network transformation, Kehoe checked in with some leaders in the tech space to hear what they think, and also what their customers are saying.

"COVID has accelerated digitization needs in both the consumer and corporate sectors," notes Andrew Yeong, VP & Head Asia Pacific with Tata Communications. "We see from all sides an increasing use of work-from-home tools, and increasing cloud to cloud data communication. All this needs speed, accessibility and mobility at the same time. What's changing as well is the security component. These are the areas we are looking at with our customers. We're also looking at moving from traditional remote VPN access to corporate networks of the past to faster, more secure methods like SASE. We're also looking at the customer experience. We have customers like banks and manufacturers who demand the highest service levels in quality from us. They want omni-channel, and they want it anytime, anywhere. This all has to be done in a very agile and responsive fashion so whatever applications we build, whatever design of platforms we choose, it has to be self-service."

If the role of a bank is to deposit money and transfer money via a network, then the availability of that network is of paramount importance, says Richard Christopher, Global Head of Network Services with Standard Chartered bank. "The expectation is that the network is frictionless. Its presence should never be felt. It needs the scalability, resiliency and the security to make it to deliver the bank's digital agenda and the bank's future strategy. In that sense the importance of the network has never been greater. And now clouds are an integral part of any global network solution."

Christopher says another key component is cyber: "The role of the network is changing so as to be not just transport but also a means to provide cyber risk reduction and protection of critical assets."

Security is front and centre to any ICT investment strategy, agrees Terence McCabe, Chief Technology Officer for Asia Pacific and Japan with Nokia: "We have seen that many of the security threats that we that we face and many of the infrastructural issues that have arisen recently don't happen in agile environments," he says. "Static environments and are often the most at risk. You're working against a continuously changing set of threats, so it's important that your defences are changing in a similar manner, and are using the best available technology and methodologies. If you look at AI for threat detection as an example, that's evolving incredibly quickly, and anyone who isn't using that is leaving themselves exposed as a result. I don't think it's a choice between agility and security. Agility can contribute to security and we should look at it in that way."

McCabe sees 5G as a critical piece of the jigsaw: "It's a large step beyond what we've seen with previous generations of mobile network," he points out. "As the 5G network expands it gives us a network that is that is sliceable, that can have dedicated quality of service and dedicated security domains associated with specific applications with specific use cases. Perhaps in a manufacturing plant or in a warehouse, you deploy private networking technologies to support your automation needs. But as the workload moves out of that controlled environment it may move into an environment where the wide area you use is a slice of a public network. End to end use cases are already being developed, and there's some tremendous opportunities there."

Angus Luk, CTO Smart Retail with Lenovo, agrees with this vision: "We are a PC manufacturer and we try to adopt a lot of 5G connectivity in our devices," he expands. "5G is a purpose-built piping network and I think there is a lot of

evolution that we will see in the coming years. On top of that there's edge computing where we will also see a lot of technology transformation."

Yeong of Tata Communications says 5G and other new technologies offer a way for Tata and other telcos to look at ways to serve their customers better: "One of the new initiatives that we have, for example, will be shipping out some form of low-cost CPE," he explains. "That allows for pop up stores or a pop-up network. We are doing this for luxury brands. That is going to change the way they do business in the future. How will 5G replace Wi Fi at home? Will a home become the new subdomain of an office for example? These are the trends that we are watching. We remain flexible to make sure that we hear our customers and pursue the innovation that is necessary. New use cases are just exploding across all sectors."

Christopher of Standard Chartered looks forward to newer tools to allow workers to collaborate and to connect with each other and with customers: "They need the same or better ways to do what they were doing in the office previously. The way that organizations now adopt ways of working will be a talent differentiator, helping to attract better people in the future."

Links to the organisations participating in the CxO roundtable are as follows:

GlobalData
www.globaldata.com/covid-19-advances-business-continuity-planning-to-a-data-science-says-globaldata/

Lenovo
https://news.lenovo.com/pressroom/press-releases/lenovo-smarter-iot-solutions-to-help-retailers-improve-productivity-and-store-safety-in-new-normal/

Nokia
https://disruptive.asia/5g-can-provide-a-new-powerful-edge-for-industrial-iot-iiot/

Standard Chartered
www.sc.com/en/

Tata Communications
www.tatacommunications.com/blog/author/andrew-yeong/

For further reading/viewing on these themes:

www.youtube.com/watch?v=TTsrlt3qN9E

https://isg-one.com/docs/default-source/default-document-library/five-challenges-to-network-transformation.pdf?sfvrsn=0

www.networkcomputing.com/networking/driving-successful-digital-transformation-people-first-strategy

CYBER RISK LEADERS

MYSECURITY MEDIA APP

App now available on iTunes &

DOWNLOAD NOW!

Download on iTunes

GET IT ON Google Play

Cyber Security
WEEKLY PODCAST

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

Jenai Marinkovic & Jon Bradt

ISACA

Streamed May 28, 2021

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

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

Download on iTunes

GET IT ON Google Play

Cyber Security
WEEKLY PODCAST

Cyber influence and misinformation – a growing threat in cyber space

Dr Herbert Lin

Senior research scholar, Cyber Policy and Security, Center for International Security and Cooperation.

Episode 262 – CYBER INFLUENCE AND MISINFORMATION – A GROWING THREAT IN CYBER SPACE

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

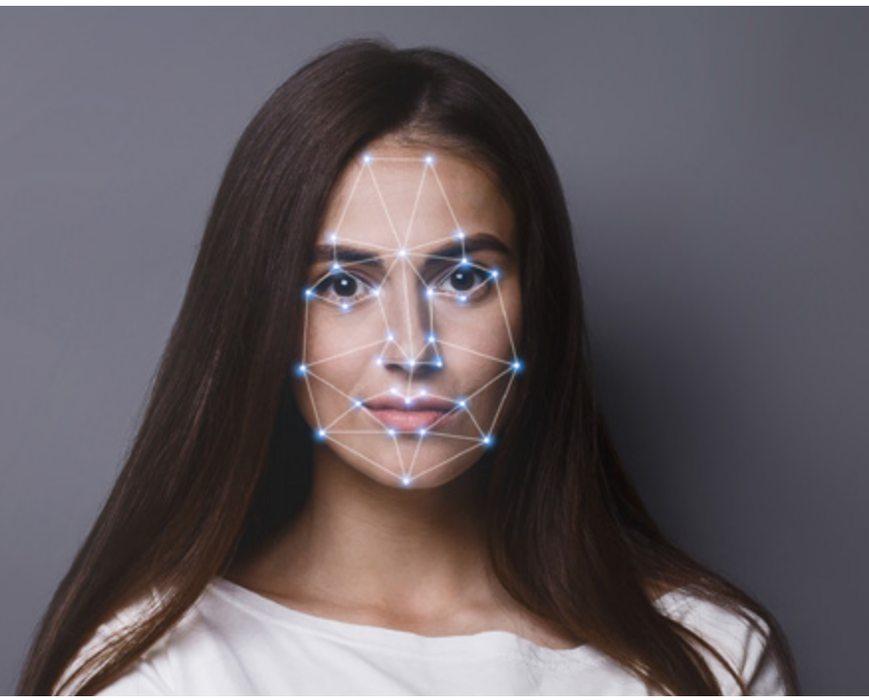
Download on iTunes

GET IT ON Google Play

00:00 00:00

LISTEN HERE

HRC calls for a moratorium on AI



By
Andrew **Curran**
Staff Writer,
MySecurity Media

The Australian Human Rights Commission (AHRC) has released a report calling for a temporary ban on the use of Artificial intelligence, such as facial recognition in high-risk decisions made by the government until new laws are in place.

The AHRC gave 38 recommendations to ensure human rights are protected in the use of Artificial Intelligence.

The main recommendation from the AHRC is the "federal, state and territory governments... introduce legislation that regulates the use of facial recognition and other biometric technology."

"The unprecedented rise in AI presents a once- in-a-generation challenge to develop and apply regulation that supports positive innovation, while addressing risks of harm."

The report focuses on four main sections outlining recommendations informed by the Commission's expertise.

The AHRC said its aim is to foster a deeper understanding of the human rights implications for Australia of new and emerging technologies such as AI.

The AHRC said in a report The Commission recommends that the "Digital Australia Strategy promote responsible innovation and human rights through measures including regulation, investment and education. This will help foster a firm foundation of public trust in new and emerging technologies that are used in Australia."

The Commission said Australians should value human rights and it would be core to the government's approach to technology.

The Commissions aim is to promote and protect human rights in Australia.

After a three-year investigation, the Australian Hunan Rights Commission believe the federal government should pause the use of AI technology in important decision making, until there are safety measures in place.

The moratorium should remain until there is adequate legislation in place to ensure human rights are protected and there is proper regulatory processes in place for the use of these technologies

The AHRC said the use of biometric technology is a concern amongst the community especially regarding facial recognition.

"Where biometric technologies are used in high-stakes decision making, such as policing, errors can increase the risk of human rights infringement and have an impact on individual privacy" the AHRC said.

"The Commission recommends law reform to provide better human rights and privacy protection regarding the development and use of these technologies, and a moratorium on the use of biometric technologies in high-risk decision making until such protections are in place."

The report recommends there should be an Artificial Intelligence safety commissioner to help support regulators, policy makers government and business.

The AHRC said "Legislators and policy makers are under unprecedented pressure to ensure Australia has the right law and policy settings to address risks and take opportunities connected to the rise of AI."

The AHRC said the commissioner should be separate from the government including in its structure, operations and legislative mandate.

"It should be required to have regard to the impact of the development and use of AI on vulnerable and marginalised people in Australia and draw on diverse expertise and perspectives" they said.

The report also focuses on improving the design of technology to allow accessibility for those with a disability on things such as goods, services and facilities that use Digital Communication technology.

The AHRC said "The accessibility of new technology, and especially of Digital Communication Technology, is an enabling right for people with disability because it is critical to the enjoyment of a range of other civil, political, economic, social and cultural rights".

The Commission recommends creating a new Disability Standard and putting new government rules requiring access to goods, services, and facilities in place.

They also recommend putting in measures to improve private sector use of accessible Digital Communication Technology.

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

Prepare for Zero Trust Security Model at the organisation level: **Foundations and Implementation**

By

Ashish Shrivastava

The increasing usage of cloud-based services, mobile computing, internet of things (IoT), and bring your own device (BYOD) in the industry have changed the technology space for the enterprises. Secure architectures that rely on secure and careful design, access controls to isolate and restrict access to corporate technology resources and services, security perimeter, Security awareness, education & training and infrastructure security are no longer sufficient for a workforce that regularly requires access to applications and resources that exist beyond corporate network boundaries. The shift to the digital world as the network of choice and the continuously evolving threats, Industries led must adopt a Zero Trust security model.

The COVID19 pandemic accelerated Zero Trust model adoption since the beginning of the disease in late 2019. Since the after start of the COVID19 pandemic, most of the industries worldwide adopted the work-from-home model. The biggest shift of the workforce to work from home has resulted in an increasing number of security breaches and cyberattacks.

Consider the scenario, where a malicious actor comprises legitimate user's credentials and attempts to access organizational resources. The malicious actor is using an unauthorized device. In a traditional network, the user's credentials alone are often sufficient to grant access, but in a zero-trust environment, the device is not known. So, the device fails authentication and authorization checks and access is denied. The malicious activity is logged.

This article will talk about the foundation and guiding principles for implementing a Zero Trust security model and asses your Zero Trust readiness. It will help you to prepare the strong foundation and strategy to implement zero trust security model to protect against the ever-growing threats of cyber-attacks.

Foundation of Zero-trust architecture?

Organizations today are challenged in protecting resources (e.g., device assets, application services, business workflows, networks, and user accounts). A Zero Trust security model when implemented reduces external and internal threats in the organizations for their systems and data.

While preparing for a Zero Trust initiative, Zero Trust architecture reduces risk across in the organizations that are migrating to the cloud and/or transforming legacy network-based controls by establishing strong identity verification and authentication, validating device prior to granting access, and ensuring least privilege access to only explicitly authorized resources.

Zero Trust requires that every transaction in the organization between systems (user identity, device, network, and applications) be strictly validated, strongly authenticated, and authorized within organization's policy constraints before granting access.

When Zero trust effectively centralizes deployed and is applied to each data or resource access request, an organization's risk from data breaches, ransomware, and insider threats is minimized.

The foundational principle of zero trust is that trust should not be implicit "trust no user or device.", it must always be granted to a user or a system when accessing organizational resources or data.

Defining principles of zero trust as per NIST, following are:

- Never trust, verify explicitly – Treat every user, device, application/workload, and data flow as untrusted. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies
- Run under the assumption of a security breach – Consider every digital asset is a resource (i.e., hardware, datasets, and applications). Access to resources should be controlled (i.e., authenticated, and authorized) on a per-connection basis and deny by default. All the resource should heavily scrutinize all the resource i.e users, devices, data flows, and requests for access. Log, inspect, and continuously monitor all configuration changes, resource accesses, and network traffic for suspicious activity. Communication channels should secure by default and all the hardware connecting to resources should controlled by the organization.
- Access based on least privileged- The principle of least privilege refers to an information security concept in which a user is given the minimum levels of access or permissions, needed to perform his/her job functions. Authenticate and explicitly authorize each to the privilege required using dynamic security policies. Limit user access with just-in-time and just-enough-access, risk-based adaptive polices, and data protection to help secure both system and data.

According to NIST Zero trust guide that no implicit trust is granted to assets or user accounts only based on their network location or based on asset they owned. Instead of assuming everything is safe behind the firewall, the Zero Trust security model assume all requests for access run under the assumption of a security breach and explicitly verifies each request. Zero Trust security model teaches

us to "never trust, always verify.", regardless of where the request originates or what resource it accesses, Every access request should fully authenticated, authorized, and encrypted before granting access to any critical resource. A Zero Trust security model relies on security policies, are used to decide whether to allow access, deny access, or control access with additional authentication challenges (such as multi-factor authentication), terms of use, or access restrictions.

Implementing Zero Trust Architectures

Developing an implementation plan and the need to understand technical requirements, how can zero trust be enabled in an organization's network and business applications?

These are all hard questions, especially when addressing legacy systems, on-premises environments versus in new deployments in the cloud.

Assess Your Zero Trust Maturity

Implementing of Zero Trust security model takes time and effort: it cannot be implemented overnight. For many networks, existing infrastructure can be leveraged and integrated to incorporate Zero Trust concepts, but the transition to a Zero Trust architecture often requires additional capabilities. Include Zero Trust functionality incrementally as part of a strategic plan can reduce risk accordingly at each step. As the Zero Trust implementation matures over time, enhanced visibility and automated responses allow defenders to keep pace with the threat.

The best approach to reaching a Zero Trust framework is to start with a single use case, or a vulnerable user group, for validation of the model.

As you consider security architecture transformation, it's important to benchmark your starting position to identify areas for improvement and measure Zero Trust maturity as you evolve.

Potential challenges on the path to Zero Trust

When implementing Zero Trust in enterprise networks, several challenges may arise that reduce the effectiveness of the solution.

The first potential challenge is a lack of full support throughout the enterprise, possibly from leadership, administrators, or users. If leaders are unwilling to spend the necessary resources to build and sustain it, if administrators and network defenders do not have the requisite expertise, or if users are allowed to violate the policies, then the benefits of Zero Trust will not be realized in that environment.

Security Domains of Zero Trust Architecture

Zero trust architecture is based on the assumption that attackers are already present in a network.

As NIST (the U.S. Department of Commerce's National Institute of Standards and Technology) describes it: "Zero-Trust Architecture is an enterprise's cybersecurity plan that utilizes zero-trust concepts and encompasses component relationships, workflow planning, and access policies."

Using the NIST SP 800-207 document as a reference point, we can classify these Zero Trust Architecture under three major security domains and managing access to resources can be considered in three distinct domains – granting access, controlling access, and continuous monitoring.

Granting Access Domain: What factors should be considered in allowing access? How does one determine and verify the identity of an accessor, what is the integrity of an accessor, and the current state of an accessor? The three major security control and factor within this domain are "Authentication and Authorization," "Integrity," and "State." If these factors are not properly implemented, unauthorized or compromised users or devices may get access when they shouldn't.

Controlling Access Domain: How much access should be granted, and for how long the access is allow in terms of both time and activity? This domain fall under the principle of least privilege. The factors within the "Controlling Access" domain is "Minimal Access in Size" and "Minimal Access in Time." If these factors are not implemented correctly, an enterprise risks granting too much access, which could lead to a security breach.

Monitoring and Securing Access: When zero trust access protocols are established, access must be continuously monitored and secured. If these factors are not followed, the zero-trust architecture could be vulnerable to network, infrastructure, and environment attacks.

Building Zero Trust into your organization

Implementation can be approach by implementing Zero Trust security controls and technologies spread across six foundational elements: identities, devices, applications, data, infrastructure, and networks.

As you begin to assess Zero Trust readiness in your organization and begin to plan on the changes to improve protection across these fundamental identities such as devices, applications, data, infrastructure, and networks, consider these key factors to help drive your Zero Trust implementation more effectively.

- Identities: When an identity attempts to access a resource, we should verify that identity with strong authentication, ensure access control in placed and compliant, and follows principle of least privilege access. User, device, location, and behavior should analyze in real time to determine risk and deliver ongoing protection. Password-less authentication should enable.
- Devices: Once an identity has been validated and granted access to a resource, then data can flow to a variety of different devices, from IoT devices to smartphones, and on-premises workloads to cloud hosted servers. This flow can create a massive attack surface area, it require monitoring of the device and

enforce health & compliance for secure access.

- Applications: Applications and APIs provide the interface for the data consumption. System can be legacy on-premises, cloud workloads, or SaaS applications. Security controls should be applied in-app permissions, allow access based on real-time analytics, monitor for malicious behavior, monitor and audit of user actions, and secure validation of critical configuration. All apps should be provided with least privilege access with continuous verification along with in-session monitoring and response for all the apps.
- Data: Where possible, data should remain secure even if it leaves the devices, apps, infrastructure, and networks under the organization controls. To ensure protection, data should always be classified, labeled, and encrypted, and access should be restricted. Access decisions should govern by a security policy.
- Infrastructure: Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services), should assess for configuration, and then automatically block and flag for any malicious behavior and should take protective actions. User and resource access should segment for each workload. Unauthorized deployments should always be block and alert the system. Granular level access control should available across all the cloud workloads.
- Networks: All data is ultimately accessed over network infrastructure. Networks should be segmented, enable real-time threat protection, end-to-end encryption apply, monitoring, and analytics should in placed.

As you start to assess your Zero Trust readiness in the organization and begin to improve protection across fundamental elements such as identities, devices, applications, data, infrastructure, and networks, you should consider these key fundamental is help drive your Zero Trust implementation more effectively.

We can build the following security control and tools to drive Zero Trust implementation:

1. Strong Authentication System: The explicit ability to verify the identity of a process or device. Along with multi-factor authentication, roles for employees need to be tightly controlled, and different roles should have clearly defined responsibilities that keep them restricted to certain segments of a network.
2. Authorization System: Implement access management along with strong identity verification. The ability to grant or deny device access to data, assets, applications, or services by a policy enforcement point. Enforce the principle of least privilege when determining who needs access to what.
3. Data classification and protection. Discover, classify, protect, and monitor sensitive data to minimize exposure from malicious or accidental exfiltration.
4. Privileged and policy-based Access Management: The ability to secure, control, and manage privileged access to critical assets and applications via defined security policies.
5. Software-Defined Perimeter or Networking: Move beyond simple centralized network-based perimeter to comprehensive and distributed segmentation using software-defined micro-perimeters
6. Device Compliance: The ability to validate that policy engine decisions are enforced on device endpoints.
7. Network Segmentation: Network traffic can be segmented at either the macro or micro level depending upon the organization's application and data resources. Move beyond simple centralized network-based perimeter to comprehensive and distributed segmentation.
8. Automation. Invest in automated alerting and remediation to reduce your mean time to respond (MTTR) to attacks.
9. Intelligence and AI. Utilize cloud intelligence and all available signals to detect and respond to access anomalies in real time.
10. Data Loss Prevention Systems: The ability to inspect network traffic and application-based traffic and apply rules to allow or deny it.
11. Security Information and Event Management Systems: A security information and event management system provides network and application traffic visibility and supports the notion of continuous monitoring and reporting on the success and failure of the enforcement of policy engine rules.

Summary

A zero-trust is a technology that helps organizations mitigate data breaches by removing the concept of automatic trust from network architecture. By adopting the zero-trust model, organizations can enhance their ability to fight advanced threats such as ransomware through leveraging micros-network segmentation and multi-layered access controls.

Zero-trust is not only used to enhance data security; it proves helpful to improve your organization's data management efforts and helps you to have complete visibility over your data flow between your endpoints devices and connected networks.

Remember, "Never trust, always verify."

Reference:
https://csrc.nist.gov/publications/detail/sp/800-207/final
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST. SP.800-207.pdf

About the Author

Mr. Ashish is a Cyber Security Architect and security blogger. He has been working in the computer security industry since the early 2004, having been employed by R&D division such as Novell, Samsung and Philips, where he conducted cyber security research and a position in Healthcare's Security & Privacy division to protect the data of over a billion users.

Ashish has achieved CISSP, CEH and AWS Solution Architect Associate certifications.

Migrating MPLS networks to the cloud age

By Guy **Matthews,** NetReporter

MPLS has served enterprise network needs well for the past 20 years. But there is no getting away from its negatives. MPLS is expensive, complex to deploy and inflexible, which makes it ill-suited for the cloud-first requirements of next generation enterprise connectivity. So what should we all be thinking about as we start to embrace a future of cloud networking?

There comes a tipping point every once in a while when one technology makes way for another that is better suited to contemporary needs. In early 2000s, for example, there was a big transition in enterprise networks where the world migrated in short order from the likes of ATM, Frame Relay and private line networks towards MPLS which was far better tooled up for the transport of Internet-based traffic. MPLS, and the dedicated IP VPN market, has had a great run of it, but now the time has come for another shift. And this time it's all about things like cloud networking and connectivity defined by software.

MPLS is still heavily embedded and will take time to shift into the history books. Newer markets, such as that for carrier managed SD-WAN services, have been growing fast, points out Erin Dunne, Director of Research Services with independent analyst firm Vertical System Group. But MPLS alternatives like this represent only a tiny part of the overall market opportunity, maybe around 5%. "Carrier-managed SD-WAN is certainly moving faster than certain other types of services," she points out.

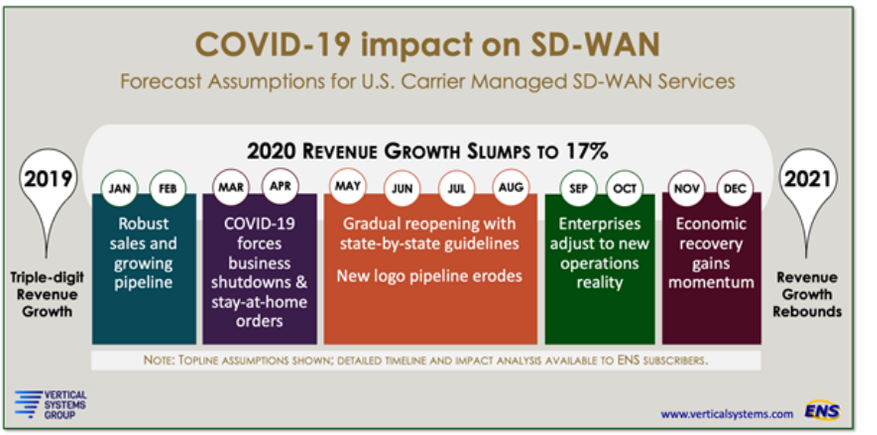
Figure 1: A timeline for SD-WAN adoption

So where did carrier-managed SD-WAN get to after a year of lockdowns and work from home? Figures from Vertical System Group show triple digit growth for 2019, while those for last year reveal a slump of 17%. "Despite a tough year, carrier-managed SD-WAN has been one of the bright spots for the overall networking market. Growth is rebounding, we're seeing that already."

Figure 2: Challenges for managed service providers

So what are the big challenges for managed service providers as they seek both to emerge from a pandemic-driven slowdown and also transition to a post-MPLS world? "COVID was a major trigger that forced a lot of transitions," says Dunne. "The first is migration to the cloud. And the second is 'work from home' and 'work from anywhere' solutions. Service providers that were just dipping their

Figure 1: A timeline for SD-WAN adoption



feet into this market had to manage this transition for their enterprise customers. With the pandemic subsiding we hope we're starting to see a movement back to longer term planning. Service providers need to deal with backlogs, address multi-cloud, refocus on transformation, and think about the customer experience again."

To help clarify this issue, Dunne questioned a number of stakeholders in the connectivity market to ask how the global pandemic has impacted the demand for network services, and get a feel for the longer term outlook.

Tata Communications serves enterprises around the world with managed network services. Song Toh, Vice President, Global Network Services with the company says it entered 2020 with great plans: "Then the world turned upside down," he says. "It has impacted some enterprises and put some plans on hold. Now they're continuing with digital transformation, which requires the network to transform as well. The long term outlook is positive. Infrastructure needs to be refreshed, network bandwidth needs to go up for the IT systems and cloud migration that has been planned."

Ashwath Nagaraj is Co-founder and Chief Technology Officer with Aryaka, a provider of software-defined network connectivity. He believes what has emerged from pandemic is nothing less than a new networking topology: "A user can be at home, at a branch, at a data center, at headquarters. Your data can be in a data center in the cloud, and can be at home. This has made the web far more important than it ever was to the enterprise business. And this change is here to stay. Not everybody is coming back to the office. So where is that office budget going to go? It is going to help transform your business, deliver the killing blow to some older networks while empowering the IT organization to deliver productivity to employees."

Mike Frane is Vice President Product Management, Windstream Enterprise which delivers security and managed services to businesses across North America. He agrees that networks and connectivity are now more important than ever: "We saw many customers accelerate their deployments to deliver on the flexibility and adaptability that they knew they would need to weather the uncertain times ahead of them. I've seen a resurgence in the last half of 2020 and our enquiries and sales of SD-WAN continue to build. Customers see SD-WAN as a highly agile option that lets them rightsize their network and their bandwidth as they shift their business and operational models. Customers are going to look for a network solution that easily provides flexibility and reliability for their physical locations."

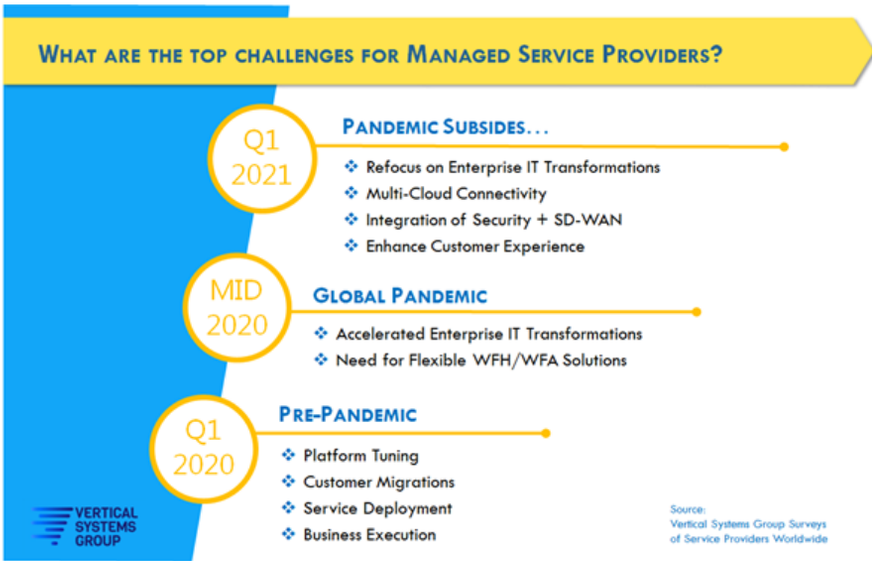
Frane however believes it will be the business, not IT departments, that will be the driving factor behind network transformation: "It'll be the busines that sets the direction from a network perspective. Businesses and their operational model, and how they reach their customers, is going to change in the future."

Nagaraj of Aryaka challenges Frane's position: "Sure, businesses need the transformation, but where's the money coming from? It has to come, I think, from the IT department coming up with creative ideas on how they can really transform the needs of business. That's how I see it."

In either instance, there is a job to be done by service providers, supported by vendors, of supporting enterprises where MPLS is still the VPN of choice. MPLS might be somewhat inflexible, but on the plus side it meets the 'five nines' needs that a lot of enterprises have for their applications. What is to be done to help those MPLS devotees to move on?

"The reality of the market is that MPLS has a long tail," says Frane of Windstream Enterprise. "There are still customers out there who rely on TDM connections for

Figure 2: Challenges for managed service providers



the functioning of specific applications. And there are many reasons for that. In some verticals the regulatory environment may necessitate the use of MPLS. Some applications have been specifically designed to work over the MPLS network and might not be readily portable to the cloud. In others, there may be a strong emotional attachment to the way that the network has always worked. MPLS is going to be around for a long time."

There is, believes Frane, no easy button for transition, not least because migrations take careful planning and time to execute: "It's not just about simply swapping out one network technology for another," he points out. "It can also require a shift in mindset, an application model, as well as in some cases the operational model of the business. There is a growing comfort with enterprises and organizations of moving to an Internet model with SD-WAN as the overlay, but we still see that the predominant model is a hybrid one with MPLS."

"The King is dead, long live the new King," adds Nagaraj of Aryaka. "What MPLS brought to companies was reliability, stability, quality and security. And so the hybrid network remains. But what's killing MPLS is that you can't put an MPLS connection to everybody's house. The home worker is going to be 40% of all the total number of hours of work. So you have to incorporate this 40% into your network, and I think that is really where MPLS struggles right now. This means that the world has to move to a new network, now."

Toh of Tata Communications points out that migration will naturally happen at different rates in different organisations: "Some will start off pretty aggressively, going 80%, 90% to cloud. In that situation the hybrid network will have a lot less MPLS in it. The reason why MPLS stays is because some applications are still very sensitive to jitter and latency. If you have a globally distributed operation, you cannot switch straight over to Internet and hope that everything works perfectly. I'm not actively killing off MPLS for my customers, but if they are ready, and they're looking for the agility, then that will be SD-WAN plus a mix of underlay that's probably more Internet and MPLS."

So what are the experiences of those who have made the move and find themselves free of legacy constraint? Are they noting, for example, cost savings after a move from MPLS to SD-WAN?

"There's a lot of hype from vendors about how much SD-WAN is going to save you," acknowledges Frane of Windstream Enterprise. "In reality we find customers spend about the same or maybe even a little bit more, and the conversation is really about the value that they are getting moving from a 100Mb MPLS connection to SD-WAN with maybe Ethernet at 50Mb and a broadband connection. It's going to cost you about the same, but you've got 10 times more download than you had before. You've got resiliency built into it, you've got your dynamic multipath optimization so your applications will run better. The value that the network is bringing is also a piece of the education."

"The most important thing that happens when you move out of MPLS in my mind is security," says Nagaraj of Aryaka. "You can get peddled snake oil with security. But unfortunately the consequences of that are very severe."

Perhaps the biggest upshot of the current transitional phase we are in is that the topology of the network has changed, says Nagaraj. "The WAN is now the centre of your enterprise business. That's partly because of the home working. As the CEO of a company, you are now empowered to transform the business much more than you were before because you have the tools to really change the structure of your business. If you are looking for reliability, security, stability, that's where people like Aryaka are interested in talking to you. We feel that all of those are critical, and we want to address that."

Operating models across industries have changed dramatically due to the last 12 months, agrees Frane of Windstream Enterprise. "SD-WAN and cloud security are going to give enterprise organizations the ability to adapt to the new normalcy of uncertainty. Whatever happens with workforce shifts, you're still going to need connectivity at home and you're going to need the connectivity in the branches. It's not an 'either or' model going forward. In fact, in many ways everything becomes much more complex for the enterprise to manage."

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

PROFESSIONALS

BUSINESSES

SEARCH THE MARKETPLACE

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

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

SEARCH

www.mysecuritymarketplace.com

CYBER RISK LEADERS

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

Foreword by M.K. Palmore, Retired FBI Assistant Special Agent in Charge, FBI

★★★★★

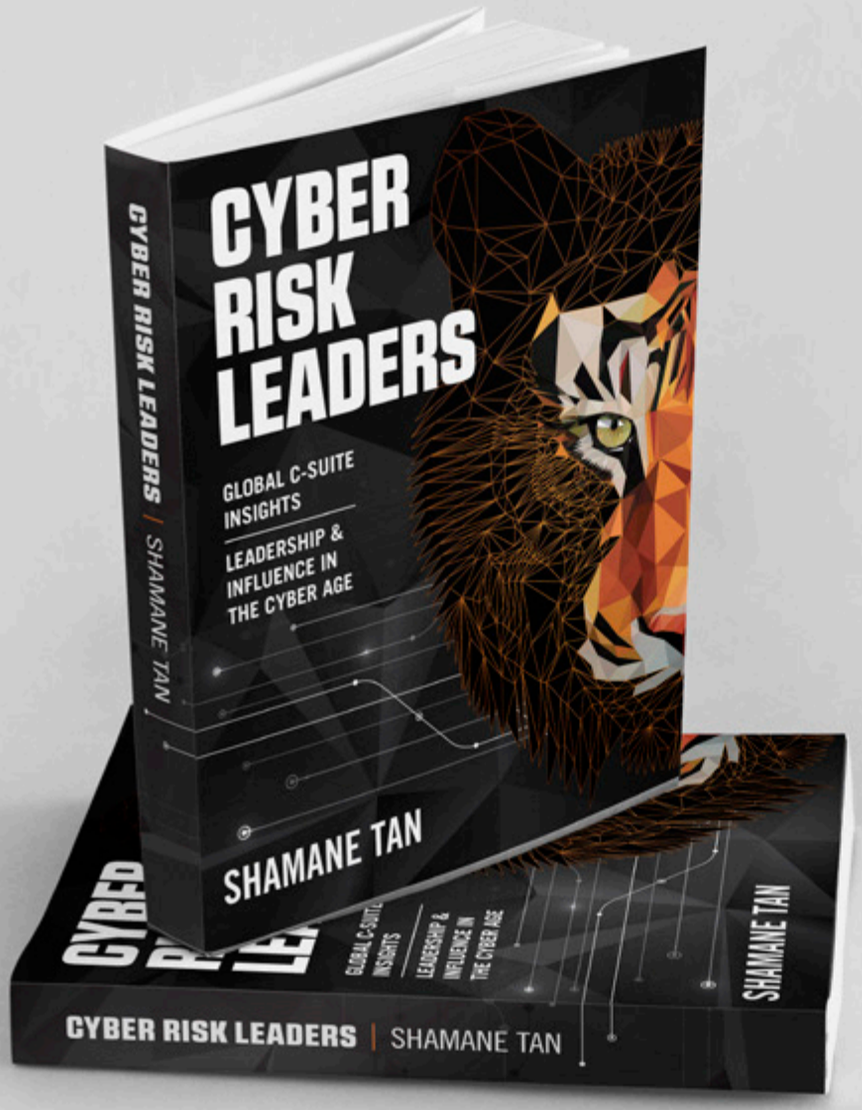
"With experience and insight, Shamane has written a really useful book for existing and aspiring CISOs. I loved her unique voice, highly readable style, and wholeheartedly recommend this book."

★★★★★

"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

MySec.TV

NEWS & INTERVIEWS

WATCH NOW

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

Interview with

Evan Davidson

Vice-President, Asia Pacific & Japan

And

Kelvin Wee

Director for Security Engineering, APJ for SentinelOne

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

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

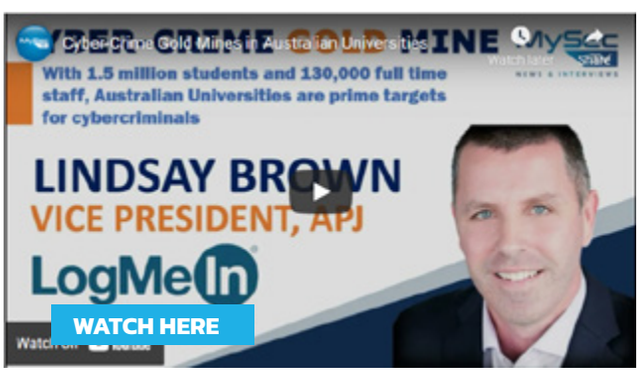
SentinelOne

MYSECURITY MEDIA

MySec.TV
NEWS & INTERVIEWS

TECH & SEC WEEKLY

AEROSPACE, DEFENCE & SECURITY TRENDS



MYSECURITY MARKETPLACE

EVENTS

Search and find all upcoming featured security events

Tue, Jul 27

Rotorcraft Asia and Unmanned Systems Asia 2021

Tue, Aug 03 — 10% Discount to Marketplace users

AI for Business Summit 2021

Tue, Aug 03 — Free Registration

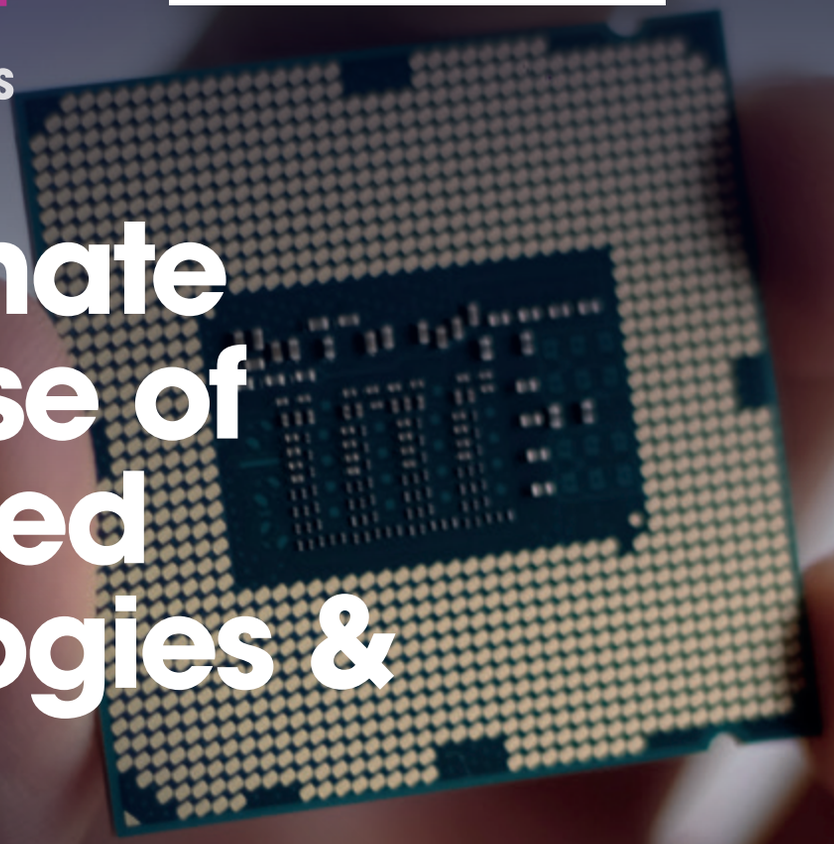
Datacentre & Cloud Infrastructure - DCCI Summit: ASEAN

Plus many more!

Embedded Technology Convention 2022

SINGAPORE • LAS VEGAS

19-20 January 2022	8-9 June 2022
SINGAPORE EXPO SINGAPORE	LVCC LAS VEGAS, USA



The Ultimate Showcase of Embedded Technologies & Systems

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

WANT TO KNOW MORE?

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

ASIA

Carson Liu

Event Director
Tel US: +1 914 639 6564
Tel UK: +44 203 026 3765
Email: carson.liu@prysmgroup.com

USA

David Miller

Event Director
Tel US: +1 702 707 7627
Tel UK: +44 203 026 3765
Email: david.miller@prysmgroup.com

www.**EmbeddedTechConventionAsia**.com | www.**EmbeddedTechConvention**.com

MYSECURITY MARKETPLACE

RESOURCES - PRODUCTS - EVENTS

EXCLUSIVE SECURITY & TECHNOLOGY

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

PROFESSIONALS

BUSINESSES

SEARCH THE MARKETPLACE

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

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

SEARCH

www.mysecuritymarketplace.com

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.

PROFESSIONALS

BUSINESSES

THE HUB

Everything about your favorite companies in one convenient place.

CHECK OUT THE LATEST PRODUCTS

Access Control, Network security

Enable Zero Trust with RSA

Access Control

YubiKey 5C NFC

UTM

10% Discount to Marketplace Users

Crystal Eye UTM Gateway Series 30+

Endpoint Protection

Malwarebytes Endpoint Detection and Response

www.mysecuritymarketplace.com