CYBER RISK LEADERS

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

Issue 1, 2020

Coronavirus themed email attacks

– The 2020 Cybersecurity Threat Landscape

Rapidly evolving trends in cloud networking security and cloud-native security

The misperception of Multifactor Authentication

From fighting piracy to cyber security

Navigating the DARQ Decade to 2030

Managing risk in an enterprise security environment

Cyber Resiliency in 2020

THREAT LANDSCAPE ACROSS THE SUPPLY CHAIN

CYBER + COVID-19

Cyber Security Weekly Podcast

Cyber security weekly podcasts highlights

PLUS

NEW BOOK & REPORT REVIEW

14th Annual Tech in Gov

4 - 5 August 2020
National Convention Centre, Canberra

Co-located with:
CYBER SECURITY in GOVERNMENT
IDENTITY EXPO

Australia's largest ICT event for the government

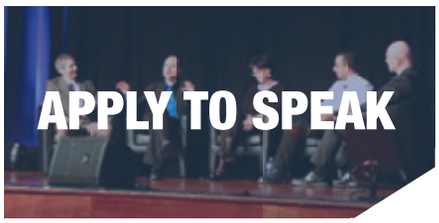
2000+ attendees • 120+ speakers • 3 co-located events

BOOK YOUR CONFERENCE PASS TODAY

EXPLORE
the role of next-gen technologies in executing strategy and enhancing service delivery

DISCOVER
how international governments are leveraging technology to better serve their citizens

NETWORK
with other government professionals, the private sector and entrepreneurial community



Exhibitor or Sponsor
techingov@terrapinn.com
+61 2 8908 8515

Apply to Speak
benton.ng@terrapinn.com
+61 2 8908 8527

Quote 'CSM10' and
SAVE 10%
REGISTER ONLINE

www.techingov.com.au | +61 2 8908 8555

MYSECURITY MARKETPLACE

EVENTS

Search and find all upcoming featured security events

Mon, Apr 06

3rd Innovations In Disaster Recovery And Rescue For Bushfire, Flood, Hurricane And Earthquake

Australia, Melbourne, Park Hyatt Melbourne

Thu, May 14

CRESTCon

Royal College of Physicians, London

Tue, Aug 04 — 10% Discount to Marketplace Users!

EmTech Asia 2020

Marina Bay Sands Expo and Convention Centre

Tue, Sep 29 — 15% Discount to Briefings Pass

Black Hat Asia 2020

Level 4, Marina Bay Sands, Singapore

Plus many more!

Contents

CYBER RISK LEADERS

Director & Executive Editor
Chris Cubbage

Director
David Matrai

Art Director
Stefan Babij

MARKETING AND ADVERTISING
promoteme@mysecuritymedia.com

CONNECT WITH US

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

AUSTRALIAN CYBERSECURITY MAGAZINE
www.australiancybersecuritymagazine.com.au

MYSECURITY MARKETPLACE
www.mysecuritymarketplace.com

AUSTRALIAN SECURITY MAGAZINE
www.australiansecuritymagazine.com.au

ASEAN Tech&Sec www.aseantechsec.com
www.aseantechsec.com

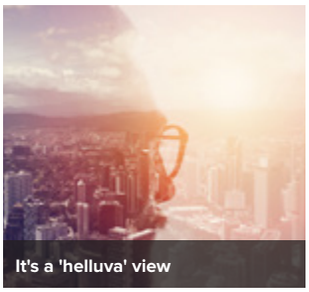
APSM ASIA PACIFIC SECURITY MAGAZINE
www.asiapacificsecuritymagazine.com

Drones & Robotics DRASTIC news.com
www.drasticnews.com

CHIEF IT TECHNOLOGY CHANNEL PARTNERS www.chiefIT.me
www.chiefit.me

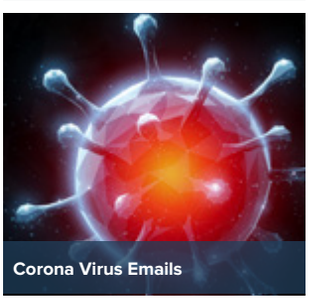
MySecurity TV
Entertain | Engage | Educate
www.youtube.com/user/MySecurityAustralia

SMART CITIES SURVEILLANCE CCTVBuyersGuide.com
www.cctvbuyersguide.com


It's a 'helluva' view


Cyber threat landscape


Cyber resiliencey in 2020


Corona Virus Emails


Navigating the DARQ decade

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


David **Stafford-Gaffney**


Annu **Singh**


Jane **Lo***


Lionell **Snell**


Scott **Raynovich**


Mohiuddin **Ahmed**

Also with Stewart **Hayes**

Editor's Desk

Welcome to the inaugural edition of Cyber Risk Leaders. As the name submits, this edition takes a broad gambit view across the domains of cyber, security, risk, governance and leadership. It remains the culmination of curated content from our security and technology channels.

As we all respond and adjust to the impacts of a novel coronavirus, COVID-19, the inherent nature of a globalised world, with interdependent supply chains, is being tested. “This is not a drill!”, warned WHO Director-General Tedros Adhanom Ghebreyesus.

As entire regions of China began to be shut down, so to were the levers on world supply chains, reliant on Chinese manufacturing. And with just as much speed and capability, cyber adversaries instantaneously spread Coronavirus themed phishing campaigns, including against Shipping companies.

A pandemic in the modern world still involves the weakness and frailty of the human race. The panic within populations to stockpile set in early in Singapore, Korea and Japan. In Australia, which showed great community spirit in the face of recent, catastrophic bushfires, is having it unravel with cases of ‘toilet paper’ confrontations and violence in stores – before even the full impact of the virus has arrived.

There remains broad speculation about the extent and duration of COVID-19. The most likely is it will stretch even the best healthcare systems and likely extend to the interruption of public services and key supply chains. As already seen with event cancellations, public institution closures and city-wide, and in the case of Italy - country-wide, shutdowns for quarantine and containment.

In contrast there will be a demand on IT services, on-demand online content and a rise in the short to medium term pace of digital transformation. The drive towards automation is likely as corporations seek to take the human element out of play and to get back to full production. As well as reduce the risk of similar interruptions into the future.

The complexity and sophistication of the cyber threat landscape, which continues to challenge government and industry is only going to grow as this migration occurs. A global economic slowdown is anticipated for the current quarter, with a best case scenario of returning to relative normalcy in the second half of the year.

Dr Richard Hatchett from the Coalition for Epidemic Preparedness Innovations, involved in efforts for a potential vaccine for COVID-19, appeared on the BBC Channel 4 news. Dr Hatchett said a vaccine will take up to 18 months to deliver at a cost of £1.5 billion. “It's the most frightening disease I've ever encountered in my career, and that includes Ebola, it includes MERS, it includes SARS. And it's frightening because of the combination of infectiousness and a lethality that appears to be manyfold higher than flu,” he said. Accused of scare-mongering, while it's crucial we take this virus seriously to avoid further spread, we may also need to avoid causing global panic, which could have far more devastating and dangerous consequences than had we just been dealing with a virus-led health crisis.

And that is why those in the security and risk domain should always take a broad view – facing a ‘black-swan’ event like a global pandemic, despite its predictability and with hind-sight, inevitability, the interdependencies of impacts and outcomes across a globalised, modern world can be beyond the reasonable or foreseeable.

In this issue, David Stafford-Gaffney contributes a timely piece, highlighting that “like computer viruses, it is a threat that some recover from, while others fall mortally ill. There are processes being followed to manage the coronavirus threat, from prevention, detection and containment through to recovery: and it’s clear we are not yet out of the containment and response phases. So how does this global health emergency help us with cyber resiliency” – my question is, ‘will it?’, because human-kind shows again and again we do not learn from our mistakes of the past. Hence, this won’t be out last issue. There is always so much more to touch on.

With thanks to our contributors, in this edition, we cover the readiness for 5G network roll outs, navigating the decade of DARQ, an acronym for Distributed Ledger Technology (blockchain, Cryptocurrencies, smart contracts), AI, Extended Reality (Virtual & Augmented) & Quantum computing and cyber security profiles of cloud computing, SD-WANs and digital video surveillance. Enjoy the read!

Chris Cubbage
CPP, CISA, GAICD
EXECUTIVE EDITOR

The Cybersecurity and Infrastructure Security Agency (CISA) warns individuals to remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19).

Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

CISA encourages individuals to remain vigilant and take the following precautions.

- Avoid clicking on links in unsolicited emails and be wary of email attachments. See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams for more information.
- Use trusted sources—such as legitimate, government websites—for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.
- Verify a charity’s authenticity before making donations. Review the Federal Trade Commission’s page on Charity Scams for more information.
- Review CISA Insights on Risk Management for COVID-19 for more information.

MEDIA CHANNELS

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

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

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

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

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

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

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

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

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

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

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

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

promoteme@mysecuritymedia.com
www.mysecuritymedia.com

THE 'GO-TO' TOOL FOR LEADING PROFESSIONALS

MYSECURITY MARKETPLACE

- ✓ UP COMING EVENTS
- ✓ COURSES
- ✓ WEBINARS
- ✓ WHITEPAPERS
- ✓ SOFTWARE

promoteme@mysecuritymedia.com
www.mysecuritymarketplace.com

“It’s one helluva view” – The 2020 Cybersecurity Threat Landscape

By Lionel **Snell**, Editor, NetEvents

The battle between organisation and chaos rages across the cyber universe. Whose side are you on? Business and Government will of course insist that they are the forces of stability and organisation, and the cyber criminals and saboteurs are the forces of chaos. But the irony is that in many ways it is business and government that are in chaos, while cybercrime grows increasingly organised – as we shall see.

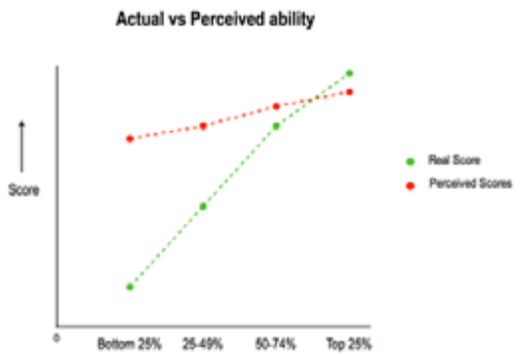
Let’s start with data from a supposedly reliable source: The World Economic Forum. In 2018 they estimated the global cost of cybercrime to be $600 billion. They estimate that it will reach $3 trillion by 2020. Meanwhile Gartner estimates that total global spending on cybersecurity in 2019 was $124 billion. Compare how much we are spending with how much we are losing and it looks like a very bad bet. Or, as analyst Vikram Phatak, Founder, NSS Labs points out: from an R&D perspective: “The bad guys are able to fund their research at a rate about five times of what the good guys are. This does not bode well for the future.”

Phatak also describes a serious skills shortage (heck! have the good ones gone off to work for the bad guys?) and how, for all the good intentions of DevOps, there are people doing rapid coding via Google search “grabbing an open source repository that may or may not have been backdoored by the North Koreans, Chinese, Russians, Iranians - pick your adversary. We're literally embedding the next attack vector in the code that we're developing today.” So that: “What's our current posture? If you ask most CSOs where do you stand, they probably can't tell you.” And that is before he has even got on to the perils of IoT, 5G and threats against the physical world of infrastructure.

Have you heard of the Dunning-Kruger Effect? That folks who are incompetent are so incompetent that they don't know that they're incompetent. They don't have the tools to judge their own capabilities. So, the data here, basically, the bottom 25th percentile, the actual performance is terrible, but they thought they did rather well – see diagram.

NGFW Failures - Evasion & Resiliency Misses

Vendor	IP Packet Fragmentation / TCP Segmentation	HTTP Evasions	HTTPS Evasions	RPC Fragmentation	URL Obfuscation	FTP / Telnet Evasion	Combination of Evasions	Advanced Evasions (HTML / Javascript / VB Script)	Resiliency
1	54	0	0	0	0	0	1	16	24
2	0	0	0	0	0	0	0	18	20
3	36	3	36	0	0	0	2	14	17
4	0	2	0	0	0	0	0	48	14
5	19	0	0	0	0	0	0	16	16
6	13	0	0	0	0	0	0	11	15
7	4	0	0	0	0	0	3	1	16
8	0	0	0	0	0	0	0	24	22
9	12	0	0	0	0	0	2	32	23
10	0	0	0	0	0	0	1	7	19
11	23	0	0	0	0	0	1	1	5
12	0	0	0	0	0	0	0	0	10



Conversely, people who are highly competent assume that, if things are easy for them, they will be easy for others. “This happens in Silicon Valley all the time, with software products in general – right?” The best minds overestimate the ability of others.

NSS Labs comes up with some revealing data on security products vulnerability to “evasions” – ie an attack is successfully blocked but the attacker just adjusts it slightly and the new version gets through unrecognised. Twelve Next Generation FireWalls were tested and 9 did well against simple, clear text attacks. But all 12 failed Resiliency (protection library depth) – NSS could trivially modify known / blocked exploits and bypass protection in all devices. Eleven of them failed to block exploits obfuscated using Complex App Layer Evasions(HTML / Javascript/ VBScript). Despite IP Fragmentation evasions been known and properly handled since the 1990s, they continue to challenge 8 of the vendors. Vendor 3 had big problems with evasions over decrypted HTTPS, but is now fixing the problem – see diagram.

It was not all bad news, however. Versa Networks’ FlexVNF did achieve the NSS Labs’ coveted “Recommended” rating on the strength of its 99% Exploit Block Rate and high scores in both SSL/TLS Functionality and Total Cost of Ownership criteria.

In summary Vikram Phatak says: “We're falling behind,

The World Economic Forum. In 2018 they estimated the global cost of cybercrime to be $600 billion. They estimate that it will reach $3 trillion by 2020.

and the bad guys have got the upper hand. We keep on making things worse. The tools that we rely upon are incredibly complex and are not getting any easier. Hopefully, with some of the AI stuff it will be, but that's no guarantee”.

As in any detective work, it helps to start with motive: what are the bad guys wanting to achieve? If you ask someone from the US Secret Service – part of the Department of Homeland Security – you might expect them to major on political threats and cyber war. But Tom Edwards insists that money is still the biggest driver: “the Secret Service has a dual mission. Not only do we protect our president and vice president, family and foreign heads of state, most people don't know that we also investigate cyber-enabled financial crime. We started investigating financial crime in 1865 with counterfeit currency, and we have evolved with the criminals all the way till today.”

Tom says: “The cyber actors that we deal with are organised groups all over the world, and it's profit driven, whether public or private sector, through ransomware, through business email compromise. They're going after the money, they're going after credit card data, they're going after personal identifiable information, and then turning that into profit. The next thing would be credential theft. They get into cloud-based servers and steal that data so they can monetise it on the dark web or in other places.

“Ted Ross, CEO and Founder, SpyCloud, knows all

about this. He has a team of researchers that interacts with criminals, and social engineer data from them as they steal it, so they can turn that around to our customers and prevent account takeovers. “We started this company three years ago; we have over 13,000 breaches in our database right now. Almost 80 billion assets. Basically, if you have an online identity, we probably have it in our database – which means the criminals have it. They're highly organised. They build their own databases”.

People underestimate the criminal's ability to be creative. They assume that, once the information gets to the deep and dark web, companies like Akamai can detect it, and protect their customers. But actually they might continue to analyse that data for up to two years: “First thing they'll separate the data into high-value targets – a special category for very sophisticated targeted attacks. They leave all the rest for later, and run automated attacks.” One of his customers, a financial organisation that deals with a lot of crypto currencies, said that 10 per cent of the attacks into their network are targeted, and cause 80 per cent of their losses.

So what technical solutions point the way forward? Yes, there is much talk about AI and Machine Learning techniques for automating, accelerating and refining attack detection – but remember what Phatak said about R&D resources. The bad guys are probably already applying these techniques. Maybe a more obvious approach is to focus on visibility? This is a natural human instinct: if we hear a suspicious noise in our house in the middle of the night, most people instinctively switch on the light, even though it could make them visible to the invader. Once humans can see what is happening, we can act fast and often very effectively.

Paul Kraus, Vice President of Engineering for Cybersecurity at NetScout Systems, makes this point: “How do you know what to monitor, or how do you put value on the assets in your organisation, if you don't even know they're there? The first aspect is gathering up the inventory of actually what you have. Second of all, can you actually take statistics? Can you look at the changes? Can you monitor to the level that your organisation can accept the risk for that asset being compromised? ... I asked a group of security engineers ‘when the dev ops team in your organisation moves something to the cloud, are you involved?’ Out of 300 people, a half dozen raised their hand. Does the security team even understand what's out there? Does the IT team even understand what's out there? Let's go back to visibility. That's the key bit for understanding your risk posture. Without that visibility, you really have no way.”

This is a subtle shift in focus: from putting all our efforts into software or devices to protect us, to thinking more about what humans need to fight back. For a soldier, binoculars with night vision might be worth more than a gun.Ted Ross takes this up: “When you install a network, you install security with it. It's part of the install. Hopefully, that's happening in most places. When you start, to actually implement a security practice, I think most people forget about the human element. The weakest link is the human. I think we are all wired to start with the devices, but I think we should also be starting with human training and educating them on concepts like zero trust, and not to click on an email attachment. If you get an email from the CEO asking you to buy gifts at Apple, call your CEO. Just pick up the phone and call him, and see if he actually sent it. Really basic things”.

Phatak adds: “Cybersecurity has become like gym membership. People buy it, it makes them feel good, but they’re not really deploying and using it properly. They're not actually going in and doing what they need to do.”

Michael Levin, former United States Secret Service & Deputy Director, US Department of Homeland Security, is now CEO for the Centre for Information Security Awareness, helping organisations induce security into their organisation to create a culture of security. He emphasises that social engineering aspect: “This is one of the things that we educate companies and employees on. It's not just the phishing email, it's the different ways employees can be socially engineered. It could be over the phone, it could be in person, it could be through social media. You have to come up with mechanisms and reminders for the employees in the organisation on a daily basis to be on the lookout”.

This all paints a depressing picture. If we cannot offer cheer, we can at least offer advice:

- Forget the old idea that hackers favour low hanging fruit means they are lazy. As Michael Levin says: “what is the first thing that a smart car burglar should do? Check the door handle to see if it's unlocked. Many hackers are doing very good reconnaissance, finding all the open windows on our networks.” They are not only educated, they are highly motivated. For most employees security is a secondary issue, for hackers it’s their job.
- Think about the relationship between your social media and your business. One company CEO tweeted to his friends that he was heading to Beijing for a few days. A few days later, his CFO got an email - purportedly from him, saying he’d been arrested by the Chinese government and needed money. They sent the money because there was enough detail on social media to make it credible.
- Be suspicious if given any sense of urgency. As Levin says: “Nine times out of 10, it forces people to make decisions very quickly and it often results in a fraud.” If a message is saying “hurry, hurry”, don’t just click. Phone and check, or go to the original website.
- “Support an open culture about cyber threats” says Tom Edwards. If employers are too scared of the boss to confess to clicking on a phishing e-mail, then the company is in trouble. Michael Levin agrees: “There should be some way for them to come out and let the organisation know they might have done something wrong without being penalised.”
- If your security thinking is focused only on technology, you will be thinking mechanically. Think instead about the human factors, the hacker’s motivation and the victim’s weak points, and you will have a much broader view of the battlefield.

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. COMING SOON

OUR CHANNELS

MYSECURITY MARKETPLACE

MYSECURITY MEDIA

SMART CITIES SURVEILLANCE CCTVBuyersGuide.com

Drones & Robotics DRASTIC news.com

AUSTRALIAN CYBERSECURITY MAGAZINE

Cyber Security WEEKLY PODCAST

CYBER RISK LEADERS

MySecurity TV
Entertain | Engage | Educate

APSM ASIA PACIFIC SECURITY MAGAZINE

AUSTRALIAN SECURITY MAGAZINE

ASEAN Tech&Sec www.aseantechsec.com

CHIEF IT TECHNOLOGY CHANNEL PARTNERS
www.chiefIT.me

Cyber threat landscape demands more of the security supply chain – From the chip to the camera

Genetec™ Streamvault™ alliance with Intel and Dell Technologies creates a cyber-hardened ecosystem.

By Chris **Cubbage**, CPP, CISA, GAICD, Executive Editor

The current landscape and technical challenges of cybersecurity are largely being driven by nation-state actors and geopolitical tensions. With increasing warnings of foreign intelligence campaigns operating at unprecedented levels, the value of trust in global supply chains is now at the forefront. Within the context of a US and China trade war and reported compromise of hardware systems, including chip manufacturing, the supply chain demands a 'full life-cycle' security assurance. Apply this to the security systems supply chain itself, the concept requires securing the chip to the camera for the assurance of monitoring and surveillance systems.

Managing risk and the rapidly changing context of risk is the role of security professionals to mitigate. We need to constantly seek out ways to reduce and where possible, minimise the probability of a security event happening or its impact. There are a number of ways to mitigate risk but, in terms of impact, a critical one often underestimated in physical security is addressing the risk of cybersecurity breaches.

Cyber threats can be unforgiving. Operational disruption, theft of intellectual property (IP) and subsequent fines, and lawsuits are some of the known and measurable impacts. However, there is such increasing interconnectivity of systems, we also see human life potentially at risk, now and in the future. With business operations, IP, legal action and personal safety being put on the line, failing to manage any of these impacts will ultimately impact reputation standing with stakeholders and how significant the impact becomes.

Yet, the contemporary risk of an interconnected world is ever growing and continuous. Massive data breaches, government bans on technology supplies, political and military tensions have converged to make 'supply chain risk management' the 'hot topic' as we step into 2020 and the next decade. Super-microchip compromise, US bans on Chinese manufactured devices, and a global wave of privacy and cybersecurity regulations are unfolding at such a rapid, and somewhat unpredictable rate, the landscape of trade, trust, security, and privacy is shifting on a tectonic scale. We should anticipate that this trend will continue and will each be transformative, as symptoms of the digital revolution.

The estimated global cost of cybercrime is $5.8 trillion[1] with China reported to be responsible for up to 60 per cent of this activity, even to the extent of having privatised its cyber-attack capability. As security and risk professionals, being aware of these global trends, we want to help protect our companies, clients, customers, and country. In the context of security systems, such as video surveillance, it is not just the data and feeds from CCTV systems and networks. The cameras are essentially devices and network gateways that are deployed and intended for asset protection. To have them compromised and weaponised is an unacceptable derivative of their purpose. Yet in 2018, 90 per cent of IoT attacks were through routers and connected CCTV cameras.[2]

The traditional network of CCTV, being a closed-circuit TV system, has been an out of date concept for many years but we're stuck with the terminology to avoid public awareness confusion. But with the growth in corporate network capability, security systems are increasingly merged and aside to corporate networks, despite network segregation. But despite not being connected to the internet or externally accessible, even air-gapped systems can still be compromised via malicious attacks and patient, sophisticated lateral movement operations. Insiders account for 56 per cent of data breaches and if randomly found, 45 per cent of employees will still plug in a USB device. Now compound the risk across a supply chain, the vulnerability from principal network access by service providers, third parties, and malicious insiders, the challenge of managing and mitigating this risk domain appears overwhelming – hence why 100 per cent security can never be guaranteed.

Questions to ask of the supply chain?

- Stakeholders within the supply chain should be asking some fundamental questions:
- Who's liable if my equipment is used to access private information?
- Who owns the company that manufactures my software and hardware?
- Does foreign government ownership of a vendor matter?
- How transparent is the vendor with cyber vulnerabilities?
- Is there any security gap, including across its own supply chain, adding to a security gap to my security solution?
- Do I need cyber liability insurance?
- How Genetec is addressing supply chain risk within a security eco- system with Genetec Streamvault

A security risk mitigation model for security system deployment should have multiple layers of protection. These will be data encryption, authentication of users, auditing, third- party penetration tests, and coding vulnerability assessments. Ideally this is built around an ecosystem of trusted partners.

The strategic arrangement between Genetec, Dell Technologies, Microsoft, Intel, and Axis forms a shielded approach to technology delivery. Video is the biggest contributor to IP traffic and video analytics offer some of the most profound applications in the digital revolution — and some of the most adverse consequences if not protected. With human and critical infrastructure applications, such as MRI scans, driverless cars in real-time roadway assessments or for security of borders and across our utility services, the integrity and availability of these systems demand assurance.

There is a market driven need for standardisation and consistency across sites. The servers and workstations that are in the Operations Centre are part of the IT and corporate system. Technology, including security technology, needs to be repeatable across installations and predictable for maintenance and upgrades, as well as offering a reduced footprint and blended IT infrastructure environment.

As underlined by Philippe Ouimette, Director of Strategic Partnerships, Genetec speaking in Sydney at the Streamvault Solutions Day Seminar, "Genetec is particular about which organisations it accepts as part of its supply chain. They are all held to the highest of standards, especially when it comes to cybersecurity."

Integrators have a responsibility to ensure the systems they are installing are secure, but it takes an estimated 13 hours to fully harden a new IP CCTV system. The risk is some integrators may cut corners due to the time and granular configurations required. With Streamvault, Genetec is seeking to make it easier to harden these systems, whilst identifying system related risk, wrapped around a network of trust and supply transparency.

Streamvault provides delivery of a turnkey security infrastructure solution, with preinstalled OS and applications, certified performance, and a cyber-hardened supply chain.

The recommended approach for security consultants and integrators is to ask the right questions, choose security vendors and manufacturers you can trust, follow cyber best practice, and invest in solutions to prevent costs and liability. The cyber threat landscape demands it.

MySecurity Media attended a Solutions Seminar Day courtesy of Genetec. For further information visit: https://www.genetec.com/solutions/all-products/streamvault-

Cyber Resiliency in 2020

By
David Stafford-Gaffney

What does coronavirus and Cyber Resiliency have in common? Let's explore this concept and see how it helps us with cyber resilience. As you are likely aware, the coronavirus is a major global concern for businesses and individuals. Like computer viruses, it is a threat that some recover from, while others fall mortally ill. There are processes being followed to manage the coronavirus threat, from prevention, detection and containment through to recovery: and it's clear we are not yet out of the containment and response phases. So how does this global health emergency help us with cyber resiliency?

Resilience

The Oxford English Dictionary describes resilience as follows:
Resilience:

- the capacity to recover quickly from difficulties; toughness.
- the ability of a substance or object to spring back into shape; elasticity.

Human Resilience: Something that differentiates some people from others is their level of biological resiliency. Infections will occur, however, some who contract coronavirus will recover, while others will fall seriously ill and even die. The likelihood of death increases for the most vulnerable groups; the elderly, those with respiratory issues, and the very young. Those who recover quickly are considered more resilient, and they have specific attributes that afford them this prowess. They may be younger, have a good diet, are fit, are mentally active, and take dietary supplements to boost their immune systems. It might be that they are in tune to their body and detect subtle changes in state early enough so they can react quickly and cut out activity that is damaging and properly focus on recovery. The same patterns translate to systems.

System Resilience: Like people, organisations are susceptible to virus infections. And just like people, their systems may not recover quickly. System resiliency is key. If systems fail to recover in an appropriate period, organizational objectives can be impacted, so systems resilience is important to the organisation's health. We now know some systems recover more quickly than others, making them more resilient. Factors that make systems more resilient include up to date antivirus systems, good patching, well controlled access management, network segmentation, and security monitoring. When we look at the elements that make people and systems resilient, they appear to fall into broad categories:

- Anti-Virus / Dietary Supplements – Protect
- Monitoring / Detect subtle changes in the body early – Detect
- Patching / Allow the body to recover – Recover

Based on our dictionary definition, resilience could be the the capacity to recover quickly from cybersecurity-

Figure 1 - NIST Cybersecurity Framework - Nist.gov

based difficulties.

With cyber the ability to recover is not just a test on the processes and mechanisms in place after threat detection, because the spread and impact of the virus will be determined by other controls, such as protective and recovery controls. Resilience is therefore a broad topic that extends through the lifecycle of threat management.

In information security we base our approach on a list of requirements derived from risk management, regulations, contractual obligations, applicable laws, government policy, and business strategy. Cybersecurity has, however, pivoted somewhat over recent years to focus more on resiliency rather than security management. This is largely the result of the assume you're breached principle, which is attributed to several challenges organisations face:

- Rapid pace of technology change
- Transformation agendas, including cloud only, cloud first, etc.
- Ever expanding ICT boarders for organisations
- Skills gaps associated with transformation
- Growing cybercrime industry estimated at over ~ $1 trillion
- Increasing attack complexity

These challenges present opportunities for cyber events and incidents and although the focus is on resilience and therefore a quick recovery, it is important to understand that success in resilience is not just eradication. Whether it's coronavirus, Swine Flu, or Wanncry, threats are always present and protections from them will always be bypassed as they mutate and evolve. The question is, how do you achieve cyber resiliency?

The linkage back to cybersecurity is easily identified: to be cyber resilient, organisations need to ensure that they can recover quickly from cyber events and incidents. This is not a new focus for cybersecurity practitioners and doesn't alter how they operate. What it does is change the priority of activities and initiatives implemented. While the concept of cyber resiliency is new, our existing management systems based on known standards like NIST Cybersecurity Framework (CSF) or ISO 27001, provide the perfect foundation for a cyber resiliency approach.

Let's take NIST's CSF and the its five domains (see Figure 1).

Figure 1 - NIST Cybersecurity Framework - Nist.gov
If you look at the coronavirus analogy against NIST's CSF, it follows a similar pattern to the management of computer viruses, especially. The pattern looks like this:

1. Identification was most likely the first phase. Understanding things that should be protected from a virus (people, organisations, countries, etc.) and the processes in place to manage the risks virus infection poses.
2. Deployment of protective controls would have taken place. Those might include, vaccinations, boarder controls, even the establishment of the World Health

Organisation.

3. Detective controls are used to in airports, hospitals and GP surgeries which bear the load in this phase.
4. The ability to respond to an infection or outbreak is next. In the case of the coronavirus, we have seen this escalate, especially in China, as the assessment revealed its lethality. Response efforts are then tested as other countries detect new cases of the virus.
5. How humans, governments, and cities recover from the virus is yet to be seen. This is because we are not out of the respond phase yet.

The question remains as to what differentiates cyber resilient organisations from others? How do they achieve cyber resilience and what should be the board focus for organisations wanting to become more resilient?

If cyber resilience is about the capacity to recover from attacks, it is critical to focus on the security mechanisms that allow organisations to get back on their feet, through the stages of the NIST CSF.

- Protective controls reduce the likelihood of an incident and reduce infections from spreading
- Detective controls such as security event monitoring, help identify the threat when it first appears
- Rapid response and containment activities reduce overall harm
- Identification of critical assets helps focus recovery efforts where they matter

Managing your organisation's environment using an Information Security Management system (ISMS) based on a known framework will improve your overall level of resilience. However, this will only work if you are diligent and implement controls across the entire framework and don't focus only on the protective controls – which many organisations do.

Furthermore, not all organisations are equal and if you are facing the challenges mentioned before, or your current security posture isn't where it should be, you fall into one of the high-risk, are vulnerable groups (like the elderly and very young facing the threat of coronavirus).

Even having a strong incident response plan and associated processes are not the only thing resilient organisations focus on. You most definitely need to have a good incident response plan, but you should also focus and prioritise the following:

1. Before any priority changes, you should assess your critical assets, since it's they are what you are tasked with protecting. From there, you can review mitigating controls and understand your weaknesses or vulnerabilities. It sometimes helps organisation's to commission an independent reviewer of business and cyber risks, as this approach is unbiased and removes local emotion and politics from the findings.
2. Have a rehearsed cyber incident response plan that includes a post incident evaluation process to assure continual improvement and shows you can respond to changing threats. Ensure this plan is communicated to all stakeholders to foster buy-in and prepare for possibly unwanted response actions, like the call to request a system shutdown at 3 AM.
3. Formally manage security, based on a reputable framework. Cover all control areas and ensure all stages of the identify, protect, detect, respond and recover lifecycle are designed, industrialised and tested.
4. Ensure you have a cyber aware executive team who understand the relationships between cyber and information security and are prepared to invest. Leave technical jargon and operational transactions at the door as this activity must influence and build trust with those who pay the bills.
5. Employees need to understand cyber hygiene. Whether developed in-house or as a service, you should invest in user awareness. Evidence shows phishing as the leading method hackers use to gain entry to their victim's systems, and there is no better way to prevent this from being successful than to explain to users how to spot the attacks.

Even having a strong incident response plan and associated processes are not the only thing resilient organisations focus on. You most definitely need to have a good incident response plan

Transformation agendas, new technologies and the blurring of logical boundaries between IT and the business only introduce further vulnerabilities into our organisations. Just like the people who are resilient to coronavirus, simple protection is not enough, resiliency is also required. We must ensure our systems and organisations are both protected from threat and resilient once controls are bypassed. And the only way to do that is to approach it holistically, methodically, and with appropriate prioritisation.

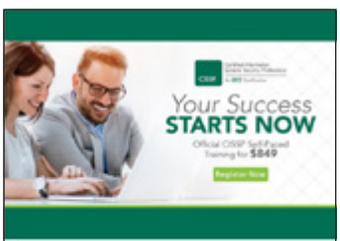
MYSECURITY MARKETPLACE

COURSES

Search and find all upcoming featured courses

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

(ISC)² CCSP Online Self-Paced Training



(ISC)² CISSP Online Self-Paced Training

Fri, Jun 07

EC-Council Masterclass
Multiple Venues

Plus many more!

Coronavirus themed email attacks

Viruses can be transmitted in various forms, through saliva, touch or even through air, and malware is similar in the sense that it finds different vectors to penetrate.

Right after the huge global attention around the Coronavirus, cyber criminals started using the interest to spread their malicious activity.

In addition to email campaigns, since the Coronavirus outbreak, a noticeable number of new websites registered with domain names related to the virus. Many of these domains will probably be used for phishing attempts.

An example of such a website is vaccinecovid-19\.com. It was first created on February 11, 2020 and registered in Russia. The website is insecure, and offers to sell “the best and fastest test for Coronavirus detection at the fantastic price of 19,000 Russian rubles (about US$300)”. The website also offers pieces of news and a heat map of the Coronavirus spread, but on closer look one can see that it is immaturely designed, providing instructions and comments such as “ a place for a beautiful subtitle” (in English translation).

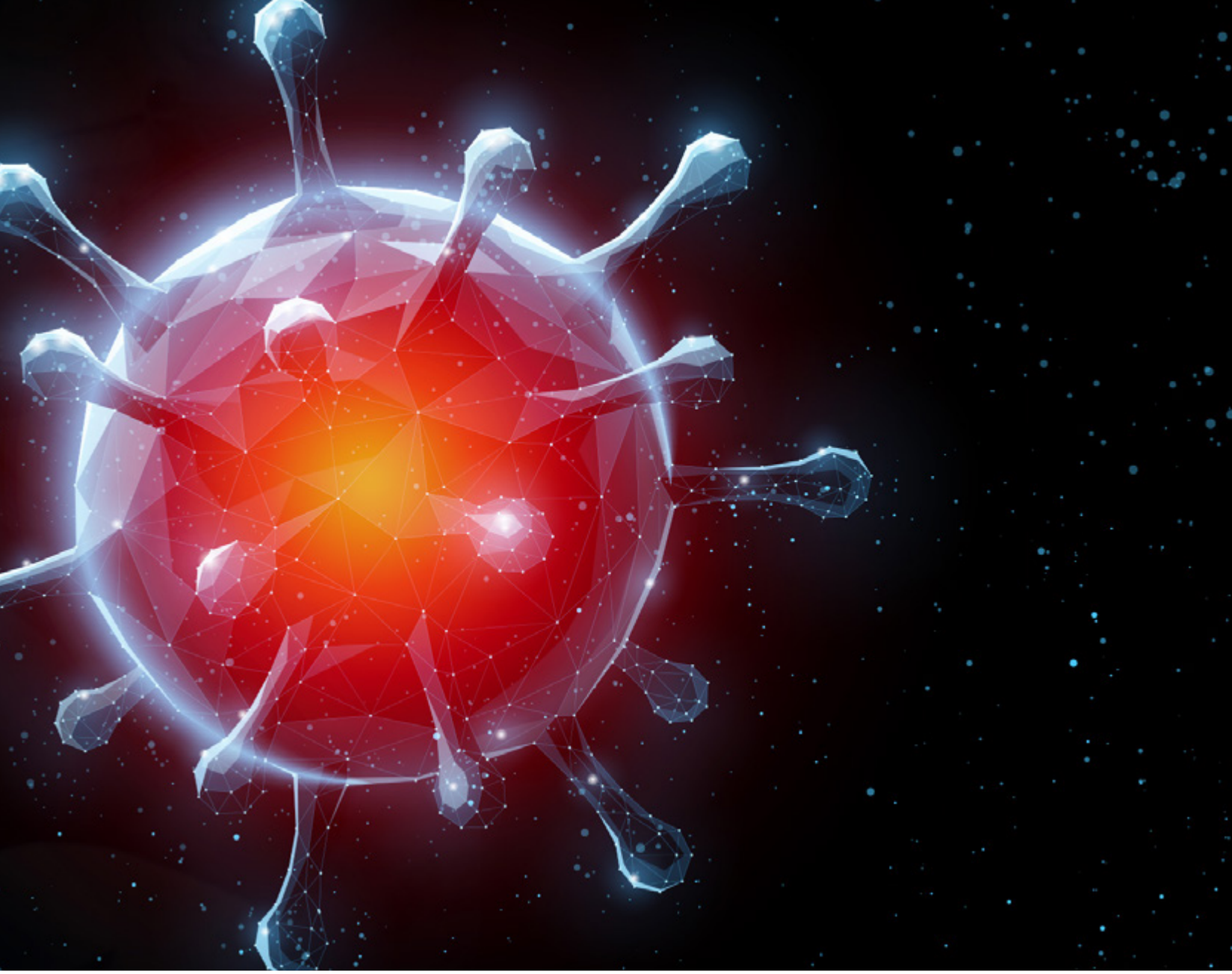
Proofpoint researchers uncovered Coronavirus themed email attacks that focusd on concerns around disruptions to global shipping. The e-mail campaign exploits a two and a half year Microsoft Office vulnerability, features malicious Microsoft word documents and installs an information stealing malware.

The industries being targeted by this email scam are those susceptible to shipping disruptions including manufacturing, industrial, finance, transportation, pharmaceutical and cosmetic companies.

A Coronavirus-related shipping supply disruption would negatively impact each of the company types listed above and there are genuine concerns globally about Coronavirus’ potential economic and international supply chain impact.

Check Point’s researchers reported an increase in exploits the ‘MVPower DVR Remote Code Execution’ vulnerability, impacting 45 per cent of organisations globally. The Global Threat Index for January 2020 reported that Emotet was the leading malware threat for the fourth month running, and was being spread during the month using a Coronavirus-themed spam campaign.

The emails appear to be reporting where Coronavirus is spreading, or offering more information about the virus, encouraging the victim to open the attachments or click the links which, if opened, attempt to download Emotet on their computer. Emotet is primarily used as a distributor of ransomware or other malicious campaigns.



January also saw an increase in attempts to exploit the 'MVPower DVR Remote Code Execution' vulnerability, impacting 45% of organisations globally. This rose from being the third most exploited vulnerability in December to the top position this month. If successfully exploited, a remote attacker can exploit this weakness to execute arbitrary code on the targeted machine.

"As with last month, the 'most wanted' malicious threats impacting organizations continue to be versatile malware such as Emotet, XMRig and Trickbot, which collectively hit over 30% of organisations worldwide," said Maya Horowitz, Director, Threat Intelligence & Research, Products at Check Point. "Businesses need to ensure their employees are educated about how to identify the types of topical spam emails that are typically used to propagate these threats, and deploy security that actively prevents these threats from infecting their networks and leading to ransomware attacks or data exfiltration."

Staying Protected

So how can you avoid falling victim to these scam attempts? Our recommendations for safe online behaviour are:

Ensure you are ordering goods from an authentic source. One way to do this is NOT to click on promotional links in emails, and instead Google your desired retailer and click the link from the Google results page.

Beware of "special" offers. An 80% discount on a new iPhone or "an exclusive cure for Coronavirus for $150" is usually not a reliable or trustworthy purchase opportunity.

Beware of lookalike domains, spelling errors in emails or websites, and unfamiliar email senders. Protect your organisation with an holistic, end to end cyber architecture, https://click.mlsend.com/link/c/

malicious threats impacting organizations continue to be versatile malware such as Emotet, XMRig and Trickbot, which collectively hit over 30% of organisations worldwide,

Navigating the DARQ decade to 2030

By Annu **Singh**

This new decade will be known as the 'DARQ' decade, as it's set to deliver on the promises of new and innovative technologies. DARQ is an acronym for Distributed Ledger Technology (blockchain, Cryptocurrencies, smart contracts), AI, Extended Reality (Virtual & Augmented) & Quantum computing. Let's explore how this next ten years could play out.

Introduction

2020 ushers in a new decade along with the apocalyptic headlines of devastating bushfires in Australia, coronavirus spreading the globe and rising tensions between U.S and Iran, raising the fear of worrisome military conflicts and political unrest. These headlines bring to centrestage the growing concerns relating to themes like climate change, protectionist trade wars amidst rising nationalism, data privacy and security, deep fakes and autonomous warfare. All these areas have grave potential to impact not only national economies but the everyday lives of citizens. With this bleak backdrop, it is interesting to appraise how technology will shape the next decade and take stock on how humankind can collectively exploit the emerging technologies to address some of these pressing global challenges.

From Disruption to Delivery

The last ten years were known as the teen decade as it was the decade of disruption brought about by digital transformation. We saw the fourth Industrial Revolution unfold with a focus on automation and connected technologies. This was supported by breakthroughs in technologies like Blockchain, Artificial Intelligence, Big Data and Analytics, Cloud and Edge computing, autonomous vehicles, IoT and 5G. As in the teen years, businesses and technologists experimented with all of these capabilities to see which of them might change their business model and boost their performance and market penetration.

The decade of the twenties is more about maturing these positions. While the AI hype has been in autonomous vehicals, image search, digital personal assistants, the next

decade will focus on bigger problems, like discovery of new drugs, semiconductor research, medical innovation, crop yield improvement, new materials development for optimal carbon capture, achieving sustainable developmental goals and achieving carbon neutrality.

Going DARQ

In the post-digital era, transformation has become the new steady state. Innovation now must move beyond digital and this is where the DARQ technologies come in. DARQ will provide the platforms for the next wave of disruption and differentiation, which are expected to enhance and alter user experiences and impact the core of how businesses operate. The next ten years will have a profound impact on the lives of billions of people, some for better and some for worse.

Distributed Ledger Technology (DLT) will move beyond exploratory proofs of concept, towards practical applications. The focus will be on integration and interoperability, as businesses move from pilot implementions to production solutions. Governments are already using blockchain technology for social welfare distribution schemes, digitised land registries and identity proofs in employment records, tax identification records, government records, certificates and healthcare records, and reputation scores. As cryptocurrencies gain acceptance, they are expected to become a de facto standard (estaimated by 2030) like the US Dollar, which is widely accepted today. Blockchain can rapidly scale to over 2 billion people who today have no access to financial services and are considered unbanked.

What's the Destination?

Alphabet and Google CEO Sundar Pichai at Davos 2020 said 'Nature at a fundamental level works in a quantum way,' while highlighting the impact that AI and Quantum computing combined can have on the lives of billions of people. With data explosion fueling the AI algorithms, the AI supremacy race is on. China and the USA currently lead this race. Machine learning and deep learning programs can analyse an unprecedented volume of data and train systems on these large databases. This capability to analyse data and make a prediction based on it in ways scientists never imagined before, can make innovation and research more economical and affordable, at a time when investment in research is on the rise with no proportionate results to show.

Quantum Computing and AI are expected to bring breakthrough innovations in the field of health and medicine, new drug discoveries, farming, agriculture, genetics, and security. Traditional encryption systems could crumble as quantum computing allows parallel processing and security will need to be reconsidered from a fresh perspective.

Drug research is another complex and capital-intensive area that takes years to get results. It is estimated that there are as many as 10 60 potential drug molecules, which is more than the number of atoms in our solar system. Quantum computing, coupled with machine learning and deep learning solutions will open doors to explore all possible molecules, capitalising on the ability to analyse existing molecules and their properties and discover revolutionary drugs.

Decarbonisation: Moving from Molecule to Wlectron

Green technologies and investments are gaining traction as consumer awareness and behaviors now demand businesses to reduce carbon footprints and adopt environmentally friendly practices. Carbon emissions from fossil fuels account for 30% of the world's greenhouse gas emissions. The future for energy is renewable and nuclear. As a sign of the future, earlier this year, the eighth largest oil producer, Abu Dhabi opened the world's largest individual solar power project with a peak capacity of 1.18 gigawatts generated by 3.2 million solar panels. But, as the world explores electrification to move away from fossil fuels, most storage solutions are still lithium ion-based batteries. The race is on to invent new materials for a clean

tech application to improve batteries for storing power on the electric grid and organic solar cells, which can be more economical than today's bulky silicon-based batteries.

AI will also be used for intelligent electricity distribution of energy. Scandinavia uses the concept of district heating to exploit the excess energy from data centres and thermal power plants to heat their resident's homes. Denmark uses wind power to meet its energy needs, reducing carbon print significantly. Bangladesh is using solar power technology for rapid electrification in rural areas, changing the lives of its citizens.

Feeding the Five Billion

500 million tons of food is wasted each year due to planning and handling issues. When, the UN Food and Agriculture Organisation estimates 800 million people go to bed hungry every night across the world and malnutrition is expected to affect half the world population by 2025. Solutions like Connected Containers that share data with an AI backend, have the potential to plug in to such supply chain problems and bring logistical improvements that can reduce food waste to a single percentage point. 39 million people faced acute food shortages due to extreme climate conditions in 2017/18.

Crop scientists are using AI to help create crops that require less water and disease resistant pesticides, while trying to improve crop yields through precision farming. Inari is one such company that uses machine learning to analyse which genes can help a crop thrive by making it disease tolerant or drought-resistant. Inari makes changes to the natural genes of the same species of plants and breeds plants that can cope better with extreme weather conditions. They use technologies like computational crop design to understand the genome of the crop and the interaction of each gene to one another. Genetic technologies like gene editing tools digital crosses or epigenetic tools are used to put the genes back together into the system, so they can actually be more tolerant to challenging environmental conditions. These technologies can help reduce farming costs, grow more nutritional food unlike genetic mutation methods and develop sustainable agriculture practices.

Yuval Noah Harari author of 'Lessons for the 21st-century' highlights the need to act now to distribute the benefits & power of AI between all humans. He warns how AI will create immense wealth in a few high-tech hubs, while other countries run the risk of becoming exploited data colonies of these forerunners. While the next decade will be tech-driven, the human element would still stay centric, skills like creativity, collaboration, specialised caregiving roles, HR cannot be replaced just yet by automation!

Preparing Tomorrow's Workforce

The number of technoloy and automation jobs is expected to increase to 1.1 billion over the coming decade. 133 million of thes jobs are expected to be created by 2022. While convergence of SMAC (Social, Mobile, Analytics and Computing) technologies in the last decade helped move ebusiness to become digital and brought solutions closer to users; it also highlighted the need for training to help users benefit and avail the advantages of these solutions.

Skills gaps and widening income inequality threaten the readiness of humans to tackle the changes brought forth by the fourth Industrial Revolution. According to the European Commissions' survey on the digital skills gap across the EU, 43% of people in the EU don't know how to perform even basic tasks like to search for information online. The focus needs to move to life-long learning and government and businesses need to collaborate to create one-stop shop avenues and community platforms that offer taxonomy, skills, certifications for reskilling and upskilling. Moreover, the government & businesses will have to focus on the redeployment of these resources for newly created jobs.

The gig economy or freelancing market is a growing segment of the workforce, which acts as a new leveling mechanism for global markets in digital outsourcing. Freelancing includes everything from computer programming, web design, tax preparation & search engine optimisation. As digitalisation spreads to grass root levels, many countries are focusing on the digital economy. This has opened up opportunities for people in developing countries, giving them access to global markets that did not previously exist. Asia is a world leader in providing outsourcing services to the rest of the world. Bangladesh is a rising power in the freelance worker market. It now owns 16% of the total freelance worker market and earns $100 million annually in revenues through gig-economy.

Frontier 2030

To look beyond the frontier of 2030, several ethical and governance questions with regards to DARQ need to be answered. Can we stop technology from fostering police states, where individual rights and privacy is impacted, while our data is commercialized and used to sell to us. AI is already being weaponised, so this also needs to be addressed if we are to counter the narratives of the dooms sayers. A cumulative effort is required by tech companies, governments, and policymakers, citizens and consumers to create a constructive framework that favours ethical choices and to harness the DARQ power for the greater good of mankind. And for all of us on this exciting voyage, in the words of Captain Jean-Luc Picard 'to continue this mission to explore strange new worlds, to seek out new solutions, to boldly go where no man has ever gone before.'

MYSECURITY MARKETPLACE

WHITEPAPERS

Search and find all upcoming featured security whitepapers

Tue, Feb 25 Free Direct Download

Advancing Cyber Resilience in Aviation: An Industry Analysis

World Economic Forum

Thu, Feb 27 Free Direct Download

Physical to Digital: A Revolution in Document Security

Reconnaissance

Thu, Feb 27 Free Direct Download

Kr00k – CVE-2019-15126

ESET

Mon, Mar 09 Free Direct Download

The National Security Agency's recommendations for cloud security

Plus many more!

5G: Are we cyber ready?

By
Mohiuddin **Ahmed**,
PhD
Academic Centre of Cyber Security Excellence,
School of Science,
Edith Cowan University, Australia

Surely 5G has been able to draw our attention from a plethora of other things. But it does not mean that we are going to be able to keep up with the pace of 5G. The telecom operators are going to allure mass population with mind-blowing TVCs. And surely, we are going to fall for it. But in 2020, we are responsible for the consequences of 5G even as user and cannot just play the consumer rights card. So, what makes 5G so special and how it supersedes its predecessors.

For mass users, the Internet speed is going to be the primary selling point. 5G offers dramatic bandwidth expansion and believed to be 100 times faster than 4G! The video streaming and heavy file downloads are going to be two of the key observable differences in redefining user experience of it. For example, to download a two-hour film over 3G network it takes 26 hours, for 4G, 6 minutes and 5G network requires only 3.6 seconds according to Consumer Technology Association: https://www.cta.tech/.

It's just not the Internet speed that is going to be upgraded, the response time is also going to be 400 times faster than 4G as per MICROCOMMS: https://www.microcomms.co.uk/. Therefore, the mass users will experience a far better Internet of Things. For example, the autonomous vehicles such as drones, cars require continuous stream of data, therefore the faster the data is communicated, the better and safer the vehicles can operate. Consequently, the defence, finance, governance, healthcare, educational and many other sectors are going to be enjoying the benefits of 5G.

So, what is the secret sauce in 5G? Unlike its predecessors, 5G is software driven, i.e. the physical infrastructure will not be affected for any upgrades. Just like our smart phones, we only need to update our apps, driver software etc. not the phone every now and then. 5G is going to significantly reduce the maintenance and upgrade costs for the service providers.

To dig a little deeper, the traditional enterprise network requires hardware-based core networking components. These components such as hubs, routers securitize the network traffic and ensure smooth routing operation. However, in 5G, these components are replaced by software driven approaches and follows digital routing. Additionally, the concept of network virtualization is also well accepted in 5G to offer the benefits mentioned earlier. In a nutshell, 5G is going to provide a more engaging and richer web experience.

Despite these mind-boggling amenities, the cyber security issues raised by 5G should not be an afterthought. The velocity of 5G is indeed a threat to us if not handled well. A hasty 5G deployment will create a catastrophe and haphazard cyber space! Let us consider the dark sides of 5G as we do not live in a perfect world and cyber criminals

are not in Mars!

Since the Internet speed is going to be hundred times faster, the cyber-attacks of any kind will exploit this speed! The exponential growth in bandwidth is going to be a nightmare for the personnel in security operation centres. As of now, the real-time cyber threat intelligence and detection has a significant correlation with the bandwidth. The traditional signature-based intrusion detection systems are struggling to keep up with the notion of Big data! Most of the Internet-based applications are streaming in nature and a source of Big data. In this scenario, 5G is going to challenge the real-time cyber intrusion detection approaches and existing solutions are going to be of no use! Rather, these traditional cyber threat intelligence tools are going to create lots of false alarms due to not being able to accurately segregate normal traffic from anomalous traffic!

Although, 5G is going to reduce the costs associated with maintenance and upgrades due to software driven networks, any vulnerability, bugs or malware will have consequences beyond imagination at this stage. The switch from hardware-based networking operations to software based will allure cyber criminals more than ever as we know these criminals prefer to launch attacks from a remote location. It is also possible that rogue nation-states will exploit 5G for malicious intents. It has not been long

'Sadly, 5G is going to be a game changer for the cyber criminals. The hundred times Internet speed and 400-times faster response time will surely facilitate much more complicated cyber-attacks.'

ago that Australian parliament was under cyber-attack and 5G without proper governance will create more digital nuisance. Which may lead to mayhem in international affairs and trade situations. The threat landscape is much wider in Internet enabled healthcare devices. The software driven network and hundred times faster Internet are not only going to bear good news for the healthcare providers but also going to widen new highways for creepy nightmares!

Well, the 5G network is not unwelcomed but failing to address the cyber risks is totally unaccepted. In recent times, there has been an exponential growth in cyber-attacks, and we have observed some of the notorious attacks such as Ransomware which crippled many organizations and among them law enforcements and healthcare are most notable. All these happened in 4G networks. Sadly, 5G is going to be a game changer for the cyber criminals. The hundred times Internet speed and 400-times faster response time will surely facilitate much more complicated cyber-attacks. The software driven 5G network will encourage malware authors (criminals) to develop more sophisticated and impactful virus. The possibilities are endless if we put ourselves into the shoes of a hacker!

Surely, 5G sounds exciting and expecting to serve us better till we hear about 6G! To capitalise the benefits of 5G, it is imperative that a synergistic approach is taken for strategic management among all the stakeholders: Service providers, Business, Government and obviously the consumers. Australian service providers such as Telstra and Optus have adopted 5G in limited areas and by 2020 all the service providers will go live. Therefore, it cannot be stressed enough that cyber security issues must not be overlooked and should be addressed now or never!

Rapidly evolving trends in cloud networking security and cloud-native security

By
Scott **Raynovich,**
Principal Analyst, Futuriom

Our sense of security is deeply ingrained. For centuries we understood that, if a house has doors, you lock them. So, if your business network has an entry point, you install a firewall. But BYOD, wireless connectivity, and cloud applications have exploded the number of entry points. In today's connected world, every single device or application expands the attack surface. If the network periphery goes fractal, where do you put security?

The cloud has changed everything on the network. It's changed traffic patterns, behaviours, and network architectures. Shortly, if not now, the bulk of enterprise traffic exiting the LAN will be heading for the cloud. It used to be a self-contained world of a corporate LAN or WAN. This is creating more bandwidth demand and it requires a more flexible architecture. You can't just install a firewall – you have to have security apps distributed wherever your users are going.

Kevin Deierling is Senior VP of Marketing, Mellanox Technologies and he sees the same problem: "They used to say 'secure the network against attacks from outside', but more and more in the cloud model they're coming from inside – because the cloud model invites third parties that are potentially untrusted right into the middle of your datacentre. So, that old security model of perimeter protection is not adequate. It's still important, but it's not adequate".

Another rising challenge is appliance sprawl. Enterprises have racked and stacked appliances for a variety of networking applications that should be native to the network itself. In the beginning, there were a few internal switches and then a router to connect with the outside world. Now there hundreds of different kinds of devices with different characteristics and different protocols, ranging from WAN optimization to application delivery control. It's going up the stack into the software layer: we have orchestration tools and visibility tools and so on. These are the things that network and IT managers are struggling with.

The way that the enterprise is interacting with the cloud is now changing the game. This has a vital bearing on security policy: is it MPLS or Internet? Private cloud or public cloud? Is the end users coming from a private MPLS

'So where should we put security? The answer is to put it everywhere: Security is going to be pervasive across every environment.'

network, business quality internet, or home broadband? For a larger organisation the picture becomes more complicated as this diagram suggests.

Look closer at the diagram and it begins to fragment into complexity. Kelly Ahuja, the CEO of Versa Networks points to the need for data-center segmentation in order to isolate applications that can become threat vectors, and in a branch office even the printers could be vulnerable to capture – unless, like HP Enterprise printers, they can detect and self-heal from malware.

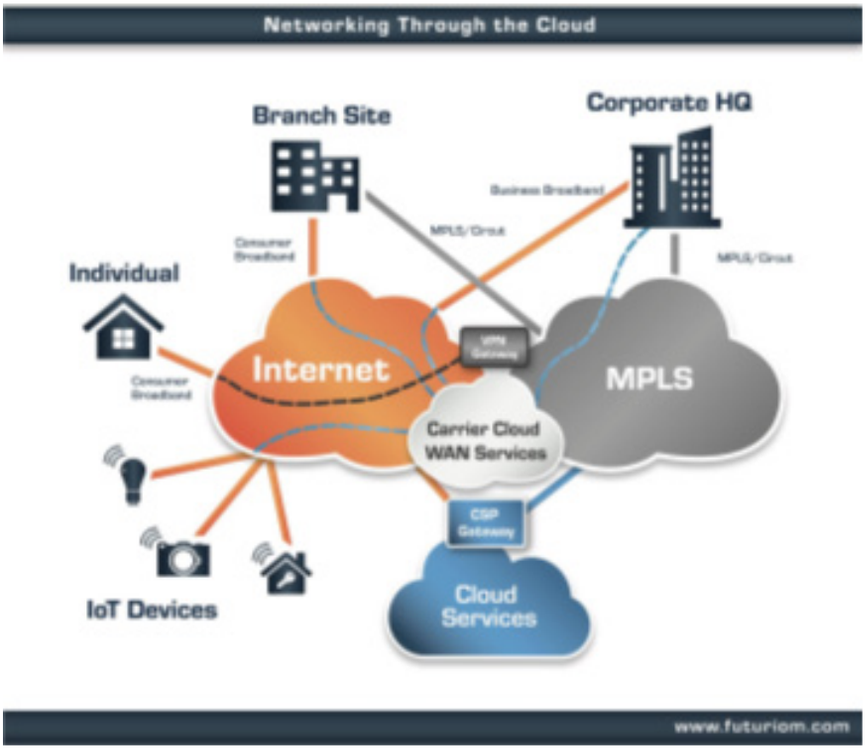
So where should we put security? The answer is to put it everywhere: Security is going to be pervasive across every environment. The edge as we knew it, the network perimeter as we knew it, was really about the external edge. In the future, it's going to be about internal perimeters – and everything is going to have to get protected in every possible way.

There is no shortage of security tools available, and that becomes another part of the problem. There are end-points, there is container security inside the datacentre, and firewalls at the edge. Drill down, and there are literally hundreds of tools for CISOs to look at and evaluate to attack specific problems. From the end user perspective, it's overwhelming. It is not just about the technology now, it's the human management problem these solutions generate: If you look at all the major breaches, whether it's Target or Chase or the IRS or Equifax, it almost always leads back to a human error. Either there were things flagged that weren't paid attention to, or there were decisions not to patch web servers and so it's really an organisational issue as much as a technology issue.

The human problem must be solved with automation. And network security challenges need to be solved with native security built directly into the network.

Given such uncertainty, and so many possible leaks, encryption becomes a more interesting solution: if you cannot stop the data getting into enemy hands, you might at least make sure they cannot read it. Encryption has a key role in the traditional closed model, as Deierling explains: "Normally you have an encrypted secure tunnel from the client into the datacentre and the cloud. But once it's in the cloud, then people assume that's a trusted model and inside it's not encrypted".

But with today's internal perimeter model you cannot seal the cloud, but is it practical to encrypt within the data center? Won't ubiquitous encryption slow everything down? Not so, says Deierling: "We have introduced a new network adaptor product that performs encryption at 200 gigabits per second line rate. We do this for point to point encryption with Ipsec, we do it for TLS [Transport



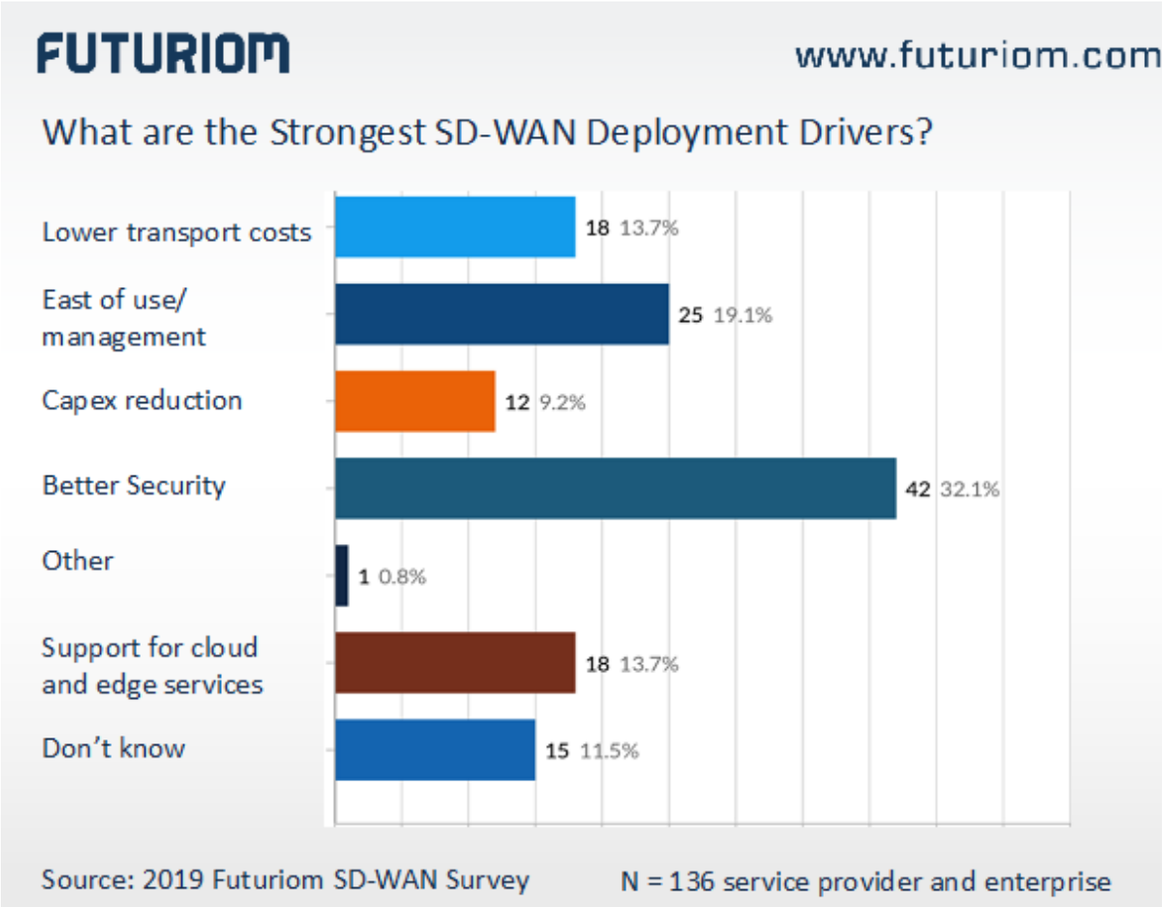
Layer Security], so that's sort of the transport layer, and we encrypt data at rest on the hard drives. This is going to become ubiquitous... two of our major customers now adopt encryption inside of their datacentres."

MK Palmore is a Field CSO of Palo Alto Networks and he too sees encryption as a security fundamental: "Encryption certainly has risen to the level of best practice, both for data at rest and data in transit." Indeed its value is increasingly recognised by the general public, with nearly half the buying public recognising its importance when buying tech devices and services – according to a Christmas 2019 survey by nCipher Security.

Kelly Ahuja agrees that encryption will happen everywhere, but how is it best delivered: "Our job isn't to determine where encryption has got to be used. Our job is to be able to provide ability to encrypt wherever a customer needs it." For example: "If you look at Wi-Fi 6, there is a WPA3 standard that's coming out which has WPA3/OWE that stands for Optional Wireless Encryption. They are actually going to use encryption in the wi-fi domain."

More contentiously, Palmore recommends hardware assist: "Clearly when you're in a datacentre at a 200-gig interface, you do need hardware assist. If there is hardware assist available, every system should use that to do it because that's going to give you the best performance."

Here Deierling does not agree: "Hardware assist is extensions in the Intel CPU that can do the decryption in software and it accelerates that. However, if you look at all the other things – overlay networks, virtual machines, hypervisors that switch between the virtual machines – all of that is done in hardware today... If you use software to encrypt the packet, all those things break. All of the hardware accelerators that companies like ourselves have put into the network interface cards over the last 20 years, all break. Because when you have an encrypted connection, all of the information we need to look at – overlays, TCP/



IP headers and checksums – all of it becomes encrypted because there's a giant IPsec tunnel. We don't see any of it. All of our accelerations break. So, I actually think [the acceleration] needs to be inline in the network adaptor."

Another way to install security everywhere is as a secure overlay. Futuriom's 2019 SD-WAN Survey asked 136 service providers what's driving their SD-WAN implementation, and security came out way on top – see diagram above.

All of these factors are driving a convergence of tools at the enterprise tools. We don't need routers, firewalls, and WAN optimization devices anymore – we need a converged enterprise edge. SD-WAN vendors are sounding more like firewall vendors these days: talking about their security stacks and their next generation firewalls.

Palo Alto, known for its second generation firewalls, does not disagree: "Palo Alto Networks has acquired several best of breed entities over the past 18 months to align our vision of the future, and it does involve a bit of consolidation" says Palmore. "We think firewalls will remain present both in physical and virtual form, but we think firewalls should deliver a number of services to our customers... The cyber security of the future involves a tremendous amount of automation, because most enterprises cannot scale from a workforce standpoint to what's needed in the cyber security industry... We are also doubling down on cyber threat intelligence. The idea that no one entity sees the entirety of the threat landscape but, if you use a patchwork approach and cobble together visions of the landscape, you can extract data and information that enables you to provide security services from a wide variety of sources".

Speaking for the SD-WAN vendors, Kelly Ahuja says "When a market is hot, everyone tries to go for it." The company's approach has been to give the customer an option: "We're an open platform. We can sit beside a physical Palo Alto or we can put a virtual Palo Alto VNF and service chain that together. We can do that with Fortinet, Riverbed, Silver Peak, Cisco – you name it. The key thing is to solve the customer's problem and most of them have an existing environment where you have to fit in and enable a smooth migration. Whether they move to a cloud or stay on-prem, it's really going to be their call and every customer is going to be different. You've got to have versatility, and that's where the name Versa comes from."

Security has to be everywhere – that is the conclusion we come away with when talking to the industry's top experts. It needs to be a coordinated net of many approaches and that can be managed with a lot of automation.

One final point following this technology discussion: "security everywhere" must include security in the workforce. When bored, or distracted under pressure, humans can be the weakest link in the security chain. On the other hand, alert, informed and disciplined employees add up to the network's strongest security overlay.

The full session transcript is available now.

MYSECURITY MARKETPLACE

REPORTS

Search and find all upcoming featured security reports

Fri, Mar 06 — Free Direct Download

2019 Internet Crime Report

IC3

Thu, Mar 05 — Free Direct Download

2020 Global Threat Report

Crowdstrike

Thu, Mar 05 — Free Direct Download

2019 Cyber Threatscape Report

Accenture

Tue, Mar 03 — Free Direct Download

Australia's new Consumer Data Right: What's not to like?

LexisNexis

Plus many more!

From fighting piracy to cyber security

- Singapore's journey towards smart nation

By
Jane **Lo**
Correspondent

2019 commemorates 200 years since Sir Stamford Raffles's landing on Singapore, the historic event many Singaporeans fondly associate with his sighting of a lion and the naming of the island as "The Lion City" or Singapura.

Travel accounts and early maps also mentioned "Barxingapara" (1502), "Sinca Pora" (1607), Sincapura" (1690), reflecting the shifting references - from a gateway, a strait, to a settlement.

The varying etymology stemmed from the significance of Singapore's waterways as a maritime artery in the region, very much vulnerable to pirate attacks, political and military incursions.

The Anglo-Dutch Treaty in 1824 settled the long-running territorial and trade disputes in South East Asia between then maritime superpowers Great Britain and the Netherlands.

Tackling the threats of pirates, who were "absolutely swarming" (according to historic records) and highly organized, to kidnap, raid, and plunder, incurred considerably more time and efforts.

Choosing a route was a security decision.

Today, this strategic location that connects the Indian Ocean to the South China Sea is now an international financial, shipping and aviation hub, housing critical systems that transcend national borders, such as global payment systems, port operations systems and air-traffic control systems.**

****Singapore's Cyber Security Strategy**

"Just as the pioneers faced danger and adversity on the seas to bring wealth and prosperity to this corner of the world, so shall we continue that journey in cyberspace," said David Koh (Commissioner of Cybersecurity and Chief Executive Cyber Security Agency of Singapore) in his Welcome message to the 5th edition of the Singapore International Cyber week.

Today, Cyber is the new frontier and "like the pirates of old, there are those who would exploit cyberspace for malicious purposes," he said.

"Cities around the world have ushered in the era of digital transformation. Singapore is no different, as we work towards our vision of a Smart Nation," he added.

Mr Teo Chee Hean (Senior Minister and Coordinating Minister for National Security) speaking at the SICW2019 Opening Ceremony. Photo Credit: SICW 2019

David Koh, CEO of Singapore's Cyber Security Agency, and Ciaran Martin, Head of the UK's National Cyber Security Centre. Photo Credit: British High Commission Singapore.

"This brings about the phenomenon of manufacturing every type of device to be "smart". From traffic cameras to lamp posts and even the most mundane of devices like rice cookers and baby monitors are now part of the "Internet of Things" or IoT." he explained.

The threats of this rapid proliferation are multi-fold:

The connected devices, as origins of compromise, expand the surface vulnerable to attacks; acting as carriers, they enable the propagation of viruses; and as connectors, their integration with the physical world raise the potential to cause direct physical harm.

We hear more at Singapore International Cyber Week (SICW 1st Oct – 3rd Oct 2019, Suntec Convention and Exhibition Centre) and Singapore International Energy Week (SIEW 29th Oct –1st Nov, Marina Bay Sands Convention Centre).

Cyber Security of Devices in Smart Nation

An example of an IoT threat was the Mira malware that launched the DDoS (distributed denial-of-service) disrupting the internet for 8 hours in 2016.

This incident was cited in a "IoT Security Landscape" study report (IoT or the Internet-of-Things), commissioned jointly by Singapore and the Netherlands, launched at the SICW 2019.

Mirai compromised hundreds of thousands of devices to jam the servers at Dyn's data centres. Unable to respond to legitimate requests, the servers forced the shut- down of 80 websites, including Amazon and Google.

Some may argue that Mirai or the SingHealth incidents caused no real damage – only, for example, mere inconveniences from completing an Amazon transaction, or breach of personal sensitive information.

Or even in the case of fingerprint spoofing for illegitimate authentication of biometrics, a mere case of identity theft.

But there are genuine safety threats:

It was executed under the MoU between CSA and the National Cyber Security Centre (NCSC) of the Netherlands signed 14 July 2016 in Singapore.

Authored by Dr Mark van Staalduinen and Yash Joshi of TNO (the Netherlands Organisation for applied scientific research) with TNO and CSA (Cyber Security Agency of Singapore) experts, the study was developed by as an outcome of the bilateral IoT Security Workshop between Singapore and the Netherlands in The Hague on 18 May 2017 and the Global Forum on Cyber Expertise (GFCE) meeting in Brussels on 30 May 2017.
It was executed under the MoU between CSA and the National Cyber Security Centre (NCSC) of the Netherlands signed 14 July 2016 in Singapore.

David Koh, CEO of Singapore's Cyber Security Agency, and Ciaran Martin, Head of the UK's National Cyber Security Centre. Photo Credit: British High Commission Singapore.

- FDA's (U.S. Food and Drug Administration) recall of a pacemaker manufacturer in 2017, for potential cybersecurity issues which would allow an unauthorized user to "modify programming commands to the implanted pacemaker, which could result in patient harm from rapid battery depletion or administration of inappropriate pacing" (that is, abnormal regulation rate of the device);
- Smart Cars with "vehicle-to-anything" connectivity (vehicle-to-vehicle/ consumer/ infrastructure/ pedestrian) where safety necessitates robust cybersecurity measures to mitigate dangerous navigation caused by unintended bugs or hacking attempts;
- The "Triton" malware which infiltrated a Middle Eastern oil and gas petrochemical facility in December 2017 and triggered a safety system shutdown.

Healthcare, transport, energy sectors are part of the 11 Critical Information Infrastructure (CII)

that are responsible for the continuous delivery of essential services in Singapore – the others include government, infocomm, aviation, maritime, banking and finance, water, security and emergency, and media.

As these sectors are digitally transformed to build a Smart Nation, devices are being networked for planning and tracking, remote operation, surveillance, predictive maintenance.

This digital fabric increasingly powering our daily interaction can be easily disrupted by a communication breach or a malfunctioned program.

Security-by-design

Security-by-design, in which device manufacturers and developers embed security measures during the design phase, aims to mitigate threats that cause such disruption.

This principle was highlighted in the Operational Technology (OT) Cybersecurity Masterplan, announced by Mr Teo Chee Hean (Senior Minister and Coordinating Minister for National Security) at the SICW 2019 Keynote.

Besides boosting training and establishing an OT Cybersecurity Information Sharing and Analysis Centre, the plan also encourages OT equipment manufacturers and service providers to adopt cybersecurity-by-design in the developmental phase.

The principle was also referenced in the Joint Statement on bilateral cooperation between Singapore and the UK on the IoT during the SICW 2019:

"... we want to ensure that internet-connected devices have security built in by design and the public and industry are protected against related security threats, such as cyberattacks, theft of personal data and risks to physical safety... "

Implementing this principle requires harmonized standards for the plethora of devices independently developed by different manufacturers. For example, Miria's exploitation of devices' simple default passwords could have, to some degree, be mitigated with pre- agreed a "no default password" standard.

ISO/IEC 15408, or the Common Criteria ("CC"), a gold standard for IT security evaluation for over 20 years, remains today "the de facto

standard for IT security product certification around the world", said Dr Janil Puthucheary (Senior Minister of State (SMS), Ministry of Communications and Information, and SMS in-charge of Cybersecurity) at the International Common Criteria Conference (ICCC) during SICW 2019.

"It advocates for devices to be secure-by-design, taking cyber

Mr Boris Balacheff (HP Fellow & VP,

"... we want to ensure that internet-connected devices have security built in by design and the public and industry are protected against related security threats, such as cyberattacks, theft of personal data and risks to physical safety... "

Chief Technologist for Security Research and Innovation, HP Labs Security Lab) at ICCC 2019.

security considerations into the product design and its subsequent life cycle, allowing customers and companies to identify products that have been rigorously tested, verified and certified", he said.

A labelling scheme deriving from a scheme such as CC (or other international standards) would promote users' awareness of vulnerabilities of their devices. This could influence better buying decisions, and in turn could reduce the surface vulnerable to attacks such as Mirai.

Recognised as a Common Criteria Certificate Authorising Nation in January 2019, Singapore joins the other 30 nations in the Common Criteria Recognition Arrangement whereby CC certificates issued by an authorised nation are mutually recognized across all member nations.

Dr Puthucheary also stressed that "better product assurance, especially for network-connected devices, is going to be important. If we can adopt these product evaluation and certification regimes, such as CC, it will give the kind of assurance benchmarked at internationally-recognised standards, to strengthen IT security for our government, Smart Nation as well as the digital economy."

"Choosing a device has become a security decision"

For sure, we rely more and more on personal devices such as medical implants and mobile phones, or business printers and computers for collection, analysis, transmission and storage of information.

Moreover, the traditionally isolated Operational Technology systems are increasingly linked to internet with industrial sensors, routers, and more. At the Singapore International Energy week, Faud Al-Ansar (VP IT Division Abu-Dubai National Oil Company) noted, for the energy sector, that Operational Technology (OT) and Information Technology (IT) are converging so rapidly that mitigating security flaws could become main concerns in this race to integrate systems.

As we journey towards Smart Nation, security is paramount to protect the confidentiality, integrity and authenticity of the devices underpinning our critical infrastructures.

Indeed, as pointed out by Mr Boris Balacheff (HP Fellow & Vp of HP Labs- Security Lap HP Inc.) at the SICW 2019, ""organizations have not traditionally included cyber-security requirements in IT equipment procurement, but this is to change, because we clearly see a rise in attackers focusing on exploit lower layers of device hardware and firmware. Indeed, we can say that in the

21st century, choosing a device has become a security decision."

The misperception of multifactor authentication

If you want to prevent unauthorized access, multi-factor authentication (MFA) is one of the most effective measure your organization can implement. The reality is that without MFA, the other security measures you have in place can be circumvented.

One of the most potentially dangerous threat to a business today is poor login security. Actually, a recent report shows that 81% of breaches leveraged either stolen or weak passwords. The problem with these attacks is that they are very hard to detect. The attacker is in possession of valid credentials, why would any security tool detect anything uncommon? When a user logs in, your security solutions assume that the person who's logging in is who they claim to be.

Despite knowing the threat, many businesses still don't take password security seriously enough. According to a survey we conducted a couple of years ago, only 38% of organizations used MFA. What's worrying is that according to some recent research, we can see that things haven't really changed today.

Four misconceptions about Multifactor Authentication

1. "My organization is too small to use MFA"
   First misconception, most organizations think that MFA is only for large enterprises not for small-to-medium sized businesses (SMBs) and that's wrong. MFA benefits all companies, regardless of size and should be part of any business' security strategy. When you think about it, it's only logic, whether you're an SMB or a large enterprise, the data you're trying to protect is as important and sensitive. MFA can be adapted, and doesn't have to be complex or expensive!
2. "I don't have privileged users so I don't need to use MFA"
   The second misconception about MFA is to think that it should be used only to protect privileged users. Based on that, many organizations decide not to use it because they believe their users are not privileged so MFA seems too much. Well, let me tell you something: even if you don't consider your users as having access to critical data, they still have access to enough data to harm your company. To illustrate this, think of a nurse selling information on a celebrity's patient to a journalist. You can easily see the value of the data being inappropriately used and the harm that can be done.

Furthermore, it's very rare for a hacker to start with a privileged account, most of the time they just start with any account that falls for phishing scams and move laterally within the network.

3. "MFA can be bypassed so it's not perfect"
   That's true, MFA is not perfect, but no security solution is. MFA is actually pretty close. According to last month's warning issued by the FBI, recent attacks show that hackers were able to bypass MFA. They founds two main authenticator vulnerabilities: 'Channel Jacking', involving taking over the communication channel that is used for the authenticator-and 'Real-Time Phishing', -using a machine-in-the-middle that intercepts and replays authentication messages. However, expert agree to say that this type of attack requires high costs and effort. Habitually, cybercriminals who encounter MFA will rather switch to their next target than try to circumvent this measure. Certain vulnerabilities can be avoided by choosing MFA authenticators that do not rely upon SMS authentication. (The National Institute of Standards and Technology (NIST) discourages SMS and voice in its latest Digital Identity Guidelines).

The FBI still recommends using MFA as it is highly effective and it's a simple step to improve your security.

4. "MFA is disruptive so it will impede users' productivity"
   This is also a misconception in the sense that it doesn't have to be true. Let me explain. Every time your organization wants to implement a new technology, it comes with a challenge: how do I implement it without impeding my users? Obviously, if the solution is too disruptive, it won't be adopted as quickly or not at all. This is the reason why you need to choose an MFA solution that offers flexibility. This solution needs to be customized to your own needs. To do so, contextual controls can be used in conjunction with MFA to further verify users' claimed identity. Contextual factors don't disrupt employees and can include time, location, session type, machine and number of simultaneous sessions.

Anyone can be victim of stolen credentials – privileged and non-privileged users, working in an SMB or a large enterprise. This is why MFA should be part of your security strategy to better protect your users' access.

About the Author

François Amigorena is the founder and CEO of IS Decisions, and an expert commentator on cybersecurity issues.

IS Decisions is a provider of infrastructure and security management software solutions for Microsoft Windows and Active Directory. The company offers solutions for user-access control, file auditing, server and desktop reporting, and remote installations.

Its customers include the FBI, the US Air Force, the United Nations and Barclays — each of which rely on IS Decisions to prevent security breaches; ensure compliance with major regulations; such as SOX and FISMA; quickly respond to IT emergencies; and save time and money for the IT department.

CYBER RISK LEADERS

MYSECURITY MEDIA APP

App now available

on iTunes & Google Play

DOWNLOAD NOW!

Download on iTunes

GET IT ON Google Play

What's on the cards with SD-WAN and MPLS?

By
By Lionel **Snell,**
Editor, NetEvents

SD-WAN was one of the hottest topics of 2019. It will be even bigger in 2020.

Erin Dunne, who directs the research practice for market research and consulting analysts Vertical Systems Group launched a discussion on the current state and future of SD-WAN and MPLS. She invited three of the industry's leading players – with experience embracing every aspect of WAN development: from services to the enterprise side, buying, selling, development and standards.

Prashanth Shanoy, VP of Marketing for Enterprise Networking, Cisco and Kelly Ahuja, Chief Executive Officer, Versa Networks – represented two of the world's top four SD-WAN suppliers. The third member was Conrad Menezes, Vice President, Industry Initiatives, CTO Office, Aruba HPe – a company that, along with Versa, promotes the increasingly influential "software defined branch office" concept.

The discussion began with Erin Dunne reflecting on the changes since the 1980s private network: through X.25, frame relay, ATM, private lines, to Ethernet and dedicated IP VPNs, mostly based on MPLS. "We've had 20 solid years of really good growth in MPLS and VPNs. Thousands of organisations worldwide with millions of sites trust this technology and depend on managed VPNs for connectivity. This is a $40 billion market and yet revenue for MPLS is down. We're losing sites, there's a lot of price compression and the number of enterprise sites at T1 and below is dropping through the floor". She added: "However, the connectivity to MPLS at above T1 or E1, is still growing. We're not seeing those connections drop off at all".

So what is replacing all those slower speed MPLS connections? According to Erin the market is moving to "some sort of SD-WAN implementation", which can mean a carrier-managed service. She also points out that the top carriers selling managed SD-WAN services – AT&T, Hughes, Verizon, Windstream and Aryaka – are the same top MPLS providers: "So this is a pretty tight market right now between the MPLS providers and the emerging SD-WAN market."

What other changes are we seeing in the market? Kelly Ahuja, speaking for Versa Networks, sees the market splitting into two main segments: a DIY segment of large enterprises building and managing their own WAN; and a mass market of smaller companies that might prefer a managed service. The former want to disaggregate the underlay, so they can use multiple providers, and build their own network. He also sees a hybrid model, where the provider supplies the underlay, devices and maybe also monitoring, while the customers set the policies themselves.

Ahuja also refutes the "death of MPLS" rumour. Whereas a customer with two or more MPLS connections might reduce their number: "a bank's not going to get rid of MPLS any time soon". Prashanth Shanoy agreed: MPLS will still hold its own in large scale or critical situations demanding high performance and reliability. In particular Cisco is seeing how traffic steering and application awareness enable better, optimized use of the remaining MPLS links.

On cost grounds, Conrad Memezes for Aruba HPe is less confident about the future of MPLS: "MPLS metro ethernet isn't cheap. For a 100 Mbps access circuit with 20 Mbps bandwidth, the average cost in the US is around $2000. Compare that with the broadband circuit that's 100 Mbps down speed and 20 Mbps up, that's $200. So $1800 difference, a little over $21,000 on an annualised basis". For an organization with a thousand sites, it means a year one saving of $21 million. He did not see latency as an issue, at least not in the US, so much as the need to gain confidence as they migrate from a dual MPLS system to single MPLS plus broadband: "and then a year later they're moving to dual broadband". He does admit that most prefer a dedicated internet access rather than an average consumer service.

What are the key use cases for SD-WAN? asks Erin Dunne. For Shenoy and Menezes it is all about the cloud and flexibility. According to Shenoy: “The whole reason why SD-WAN even exists today is because of the emergence of cloud”. Then: “As applications and workloads started moving to clouds, it was all about a guaranteed application experience, no matter where my applications are and no matter where my users are. So SD-WAN was meant to provide consistent, reliable application experience for a public or private cloud environment”.

Menezes adds: “When you think about the speed at which you can spin up services in the cloud space, it's drastically different from what you can do in the data center.” Also: “You don't need to haul all of your data traffic back to your data centre in the traditional style using a MPLS network”.

There is another company, NetFoundry, that takes the cloud agility argument a whole stage further in a world where companies like Netflix and Walmart can deploy code thousands of times a day. NetFoundry offers a “Connectivity-as-Code” solution that abstracts application developers from the underlying network, enabling them to specify in code the network policies, performance and security required by the app over any network infrastructure. The company argues that, while SD-WAN is a great solution for connecting sites, Connectivity-as-Code allows the secure-by-design apps to control the network automatically without manual configuration.

Shenoy emphasises the need for security in Software as a Service applications: “That's why you see so many security vendors coming into the SD-WAN space, like Fortinet or Palo Alto or Zscaler etc. It's now all about providing SD-WAN and security as a single stack”.

Kelly Ahuja is not so sure about the desire for disaggregation of underlay and overlay, seeing disaggregation of software from hardware as the real issue. “Most of the industry is actually selling hardware defined solutions, so that's another thing that differentiates us: we are software only and will work on any CPE appliance that we've certified”.

Bearing in mind that SD-WAN includes an entire market of hardware, software, service providers, equipment vendors, security, cloud-based offerings and much more – what are the key capabilities or differentiators offered by Versa, Cisco and Aruba?

According to Prashanth Shanoy, Cisco’s customers want to upgrade from a traditional WAN environment: “We provide a really simple, elegant, seamless solution to move from the traditional network to a fully advanced SD-WAN solution, while providing investment protection on their existing infrastructure. A lot of our customers migrate with literally zero CapEx, just a software upgrade on their existing WAN infrastructure”. A second demand is for maximum control and flexibility with choice of managed service, do-it-yourself, or working with the channel partners. “It's not one size fits all”.

While a lot of SD-WAN pioneers focused on replacing MPLS with lower cost yet secure VPN through the Internet, Versa has promoted what they call “the software defined branch” to eliminate hardware at the branch, while providing full contextual visibility across users, security and applications.

Aruba HPe too major on what they call “SD Branch” as: “a unified view of the wireless side of the network, the wired side of the network and the wide area network” according to Conrad Menezes. “The ability to manage the wireless and wireline network from a single pane is, I think, the single biggest benefit”.

The full session transcript is available now.

CYBER RISK LEADERS

Cyber Security
WEEKLY PODCAST

Download on iTunes

GET IT ON Google Play

www.CyberRiskLeaders.com

PODCAST HIGHLIGHT EPISODES

Cyber Security
WEEKLY PODCAST

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

Interview with Sharon Hiu, APAC Channel Analyst with Canalys, based in Singapore.

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

Episode 193 - Bitdefender set to release Digital Identity Protection service for consumers

Interview with Bogdan 'Bob' Botezatu, Director of Threat Research and Reporting with Bitdefender whilst visiting Australia from Romania.

Pre-release discussion about Bitdefender's new Digital Identity Protection (DIP) service. Scheduled for release in April 2020 the DIP scans the internet and dark web for background to give awareness to consumers on what personal information of theirs is for sale or available that they're not aware of.

Bob also shares insight into the background of Bitdefender and the trends shaping cybersecurity in 2020.

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

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

Episode 187 - INTERPOL CYBER CRIME OPERATIONS & IGCI SINGAPORE - Interview with Craig Jones, INTERPOL Director for Cybercrime

Mr Sathish Ashwin is the Head of Research and Operations at the National Podcast interview by Jane Lo, Singapore Correspondent with Craig Jones, Director, Cybercrime, INTERPOL IGCI (Interpol Global Complex for Innovation).

A national and international expert in the field of cyber and digital crime investigations and capabilities development, with over 27 years of law enforcement experience, Craig Jones is recognised as a strategic leader and thinker. Craig has an ability to identify and shape policies that deliver outcomes and results against international and national cyber strategies. This experience allows INTERPOL to anticipate and predict the long-term impact of national and international developments, including economic, political, environmental, social and technological specific to the cyber threat.Craig demonstrates extensive expertise in cybercrime investigations, regionally, nationally and internationally at a senior level within UK law enforcement.Committee chaired by Honorable Justice Dr. S. Mohan, Former Judge, Supreme Court of India.

Episode 190 - Space 2.0 and why Space is important to Australia - Interview with Professor Russell Boyce at the Global Space & Technology Conference 2020

Jane Lo, Singapore Correspondent interviews Professor Russell Boyce at the Global Space & Technology Conference 2020.

Professor Boyce holds the position of Chair for Intelligent Space Systems and Director of UNSW Canberra Space (Australia's largest space capability), at UNSW's campus at the Australian Defence Force Academy. His role there, leading the growth of Australia's largest space mission and research team, leverages the first part of his career – 25 years of research and teaching in the field of hypersonic aerodynamics and scramjet propulsion. Boyce chaired the Australian Academy of Science's National Committee for Space and Radio Science from 2011-2017; was a member of the Expert Reference Group that paved the way for the establishment of the Australian Space Agency; and has co-authored over 200 international journal and conference papers on hypersonics and space research. He sits on the Executive Council of the Space Industry Association of Australia, and has recently been named a Fellow of the American Institute for Aeronautics and Astronautics (AIAA). Professor Boyce is only the third Australian to become a Fellow of the AIAA which is the peak professional body for the aerospace sector globally.

the cybersecurity industry. Magda founded Women of Security (WoSEC) and launched a WoSEC CTF For Girls Competition Day

Episode 189 - ECU launches new Security Operations Centre with RSA Security - building renewed tertiary focus on cybersecurity skills training

IInterview with ECU Executive Dean of School of Science, Professor Andrew Woodward and Dr. Paul Haskell-Dowland, Associate Dean for Computing and Security, School of Science, Academic Centre of Cyber Security Excellence.

Edith Cowan University (ECU) has opened the southern hemisphere's biggest Security Operations Centre (SOC) within a university. The cutting-edge, $3 million SOC will offer Perth students firsthand experience in cyber operations and technology and responding to cyber security threats.

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

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

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

Managing risk in an enterprise security environment

By Stewart **Hayes**

Security has different meanings for each organisation depending on their business sector, operational locations and operating model. These may influence their view on what is important - cyber, physical or personnel (insider threat) security and, as a result, how they approach security management. This has tended to influence their choice of staff and skillset required to oversee their security infrastructure. However, nearly all organisations are now faced with a multitude of threats which could impact their ability to operate effectively, meet their business objectives and protect their stakeholders' interests.

Converged Security is a topic that has been around for a number of years. The Alliance for Enterprise Security Risk Management formed by ASIS, ISACA and ISSA used to issue an award for the best approach to delivering security convergence. Unfortunately, this alliance disbanded after 2007; however their publications and principals remain applicable. In 2012, along with some very experienced colleagues, I published a paper on the advantages of a fully integrated security ecosystem - The Changing Face of Cybersecurity (ISACA Journal) that considers business risk first. Essentially this promoted the provision of a single focus for security issues; IT systems, Physical infrastructure and Personnel.

This should now be extended to cover other related areas including key aspects of Personally Identifiable Information which is typically handled by the Legal Department; OH&S and the working environment – usually the domain of HR or Health and Safety; Payment Cards – Finance; and Political threat if they are operating in hostile regions is usually outsourced to specialist agencies. All represent a potential source of security risk to the organisation and should be managed consistently and effectively. The problem for the Executive however, is deciding where they spend their security dollar. They must consider these security risks alongside investment, market and regulatory risks.

Developing and establishing a framework for the converged security model is difficult. Typically, the various security disciplines have different skill sets, different modus operandi and different threats to address. As a result, the security dollar often gets spent on fixing the last problem that occurred or the 'issues' identified by an auditor. These may not address the key business risks.

Technology relevant security threats continue to emerge. Having established approaches to securing a Cloud environment with massive data stores and transient servers and applications, we now have another field approaching the security ecosystem like a steam train. Integrated Operational Technology (OT) and 'Internet of Things (IoT)' components within the corporate infrastructure. We have aged Building Management Systems (BMS) with unprotected control systems enabling unfettered access to corporate networks and even sensitive operational networks beyond the corporate environment. Similarly, IoT devices having greater autonomous intelligence than OT systems are being plugged into the operational infrastructure in increasing numbers. These are now gathering large amounts of potentially sensitive information to be stored in data lakes and analysed by artificial intelligence (AI) systems. The current separation of security duties across all these environments is not sustainable and is comparable to a balloon in a box of pins; at some point the security bubble will burst.

The role of the Security Manager must now be to understand the growing number of threats to the organisation's operational infrastructure and ensure the risks to the business success are managed effectively. Being skilled in one discipline - IT Security, Physical Security or OH&S is no longer viable. The new breed of Security

Convergence of the Security disciplines can provide massive business benefit. These should be identified as part of any business case for infrastructure improvement programmes.

Manager must understand enterprise risk and business enablement. They do not need to be experts in the various disciplines but they must be able to gain the confidence of those that are and be able to promote the concept of a fully integrated security model.

The benefit of a converged approach can be seen in an example from the Telecommunications Sector. The challenge for the authors was to provide an effective solution to manage physical access to facilities, racks and roadside boxes across sites in Australia, in a way which provided accurate audit of access. A manual system would be error prone and involve significant overheads, but by integrating the physical access with the Identity and Access Management system it was possible to for users to have a single identity to manage access to both their IT services and the physical environment down to the physical rack keys. This made the business processes highly efficient, required minimal effort, and delivered a full audit of all system and facility access. This integrated approach saved many millions of dollars in establishing and managing the security ecosystem.

The Health Sector also presents opportunities for converged security to make a significant difference. In a number of hospitals, the author was able to integrate physical access control with the IT systems and, importantly, the patient management system. This enabled end to end tracking of a patient episode through the facility and reduced the risk of mistaking a patient's identity. Using a wristband-based RFID (Radio Frequency Identity) tag, the patient could check themselves in, be verified before any procedure and, along with the clinician tag, could enforce dual control on records access.

There were also missed opportunities. A large multinational bank used the physical access card to carry a chip that would act as a Visa approved wallet. This has a cost. When the systems that this wallet could be used on were removed, the chip became useless. Had the physical security team worked with the IT Security team, the chip could have been used for password-less authentication and provide a secure store for encryption keys. As it is, the chip, whilst expensive, now serves no purpose and passwords continue to be used.

Similarly, with the increasing use of corporate infrastructure to carry OT and IoT traffic and the increasing risks from connectivity that comes with IoT, traditional siloes of operational activity are increasingly turning to the security manager for help. As a result, the security manager must now not only help deliver integrated systems but must be able to monitor for operational protocols, not just those in the IT spectrum. While the 2016 Dyn denial of service attack from IP-enabled cameras is a well publicised example of these forms of risk, there are many others which have had more severe ramifications. In 2016, the Ukraine power grid was disrupted by a cyber-attack with quarter of a million people left without power for some hours.

There have been numerous reports of rogue IoT and OT devices being used to compromise the corporate infrastructure, many of them successful. These systems should be subject to the same rigour as other IT systems within the organisation's operational infrastructure to manage the potential risk; that is their vulnerability to compromise and ability to impact sensitive systems.

The approach to qualifying this risk is the same as any other risk assessment process, however it must now be considered on an enterprise scale. Mitigation controls should likewise be addressed on an enterprise basis; that is, can one solution address risks across different operational areas. These issues may also be relevant on a global scale for multinational organisations; however the different operating environments and regional influences may need to be managed differently.

Technology continues to evolve and as we see the continue evolution of IoT plus the next wave of 5G-enabled solutions and artificial intelligence driven systems, the need for a holistic approach to managing security risk will become even more critical. Furthermore, the cost of not addressing risk is also increasing. A breach could affect the organisation's ability to deliver services, may cause direct financial loss or affect their reputation in the market place. As legislation such as GDPR comes into force, the penalty for allowing a breach to affect customers is becoming increasingly severe.

Cyber security is no longer an isolated domain, it is part of the wider enterprise and risks must be considered alongside the other business issues. Threats may manifest differently in the various disciplines however the business impact is comparable; it could affect the organisation's ability to deliver services, may cause direct financial loss or affect their reputation in the market place. Whichever area or discipline of the wider security environment, the approach taken to quantifying and assessing the risk is the same. Similarly, the approach to mitigating these risks may be common, at least in part.

In conclusion, security risk management is an enterprise issue and contributes to the success of the business just like with any other form of risk management. The modern-day security manager and their team must now be cognisant that security management is a multi-disciplinary skill and operational security must now observe a convergent approach to enable business benefit. All aspects of the security ecosystem are related and require a common approach rather than the current siloed verticals.

Acknowledgements:
My thanks to many colleagues in Industry and Academia who have reviewed this paper and provided invaluable input.

Deep learning enriches digital video analytics

Genetec™ Streamvault™ with an Intel core set for growth in 2020 and beyond

By Chris **Cubbage**, CPP, CISA, GAICD, Executive Editor

Consider the world's technical mega-trends: the proliferation of cloud computing, the cloudification of networks, edge computing with artificial intelligence (AI), and analytical capability. Consider over half of the world's data was created in the last two years and less than 2 per cent of that data has been analysed. [1] Increased compute demand and diversifying workloads are driving growth and applications of AI, high-performance computing (HPC), multi cloud computing and orchestration, networks, databases, virtualisation and cyber- security.

Higher compute performance and lower network latency is overlayed by the biggest trend of them all – the decreasing cost of computing. In just five years, between 2012 and 2017, the cost of storage plummeted 77 per cent and compute costs dropped 56 per cent. While in the same period, computer processing performance increased a whopping 370 per cent.

Data processing is rapidly moving from descriptive and diagnostic analytics to predictive analytics, giving foresight; prescriptive analytics, for simulation-driven, improved decision making; and cognitive analytics, with self-learning and automated action capability.

The transition from operational to advanced analytics will overcome bandwidth limitations and storage costs by the analytics processing moving to the network edge. This delivers near real time response needs, from what has been a forensic and review application to now more predictive and cognitive application. This shift also creates greater accuracy and addresses privacy concerns, with less data moving around vulnerable networks. For video analytics, systems are now achieving 97 per cent identification accuracy, which is better than any human can sustain in an operations room.

AdDigital_EN_Genetec-Steamvault-to-paradise_325x325pxHPC technology is giving rise to high performance video systems. The digital video landscape will contribute 82 per cent of all IP traffic by 2021 and security video will naturally be a big part of that. By 2025 deep learning revenue is forecast to be worth $40 billion and growing at 11 per cent CAGR (calendar annual growth rate)[2]. Deep learning enabled video systems and NVRs (network video recorders) have many use cases, such as public surveillance, transport monitoring, crowd monitoring, region of interest detection and intrusion detection. Market verticals are vast; across cities, financial services, robotics and drones, home, retail, and health services.

Cloud proliferation is happening and data analytics is a strategic business tool with an ability to create value from

predictive insights. As of 2020, the emerging 5G networks will begin to connect billions of devices and the cost of compute and storage will continue to drop, dramatically. With digital video driving much of the IP traffic, the opportunities for video analytics are endless.

Intel's product portfolio spans the spectrum from edge to datacentre and cloud, including a large eco-system of developers and development tools that share common algorithms across the portfolio which can significantly speed up development cycles.

It is therefore not a coincidence that Genetec is converging its software with hardware from the likes of Intel and Dell Technologies, creating new product series like that of the Streamvault portfolio. Intel technologies can be found across the stack from smart edge devices with analytics capabilities enabled by the Movidius VPU, through to gateways, cloud and Datacenter servers and appliances built on high performance 2nd Generation Xeon processors

Optimising the software stack and deploying capabilities on modern hardware can have a profound effect on overall solution performance and throughput. For example, by utilising modern Intel technologies and the Intel distribution of OpenVino, Philips was able to achieve a 38X increase in image throughput on x-ray analysis,

ability to scale up to 416TB in a 2U with cost-effective internal storage and scale-out to 7.2PB in a 42U rack. This allows the management of thousands of hours of videos or Exchange mailboxes in one location and as a streamlined server,

and GE saw a 14x improvement in inferencing speed over their baseline solution with a clinical diagnostic scanning implementation. The combination of OpenVino and 2nd generation Intel Xeon processors mean developers do not require expensive third-party accelerators to enable high performance video analytics.

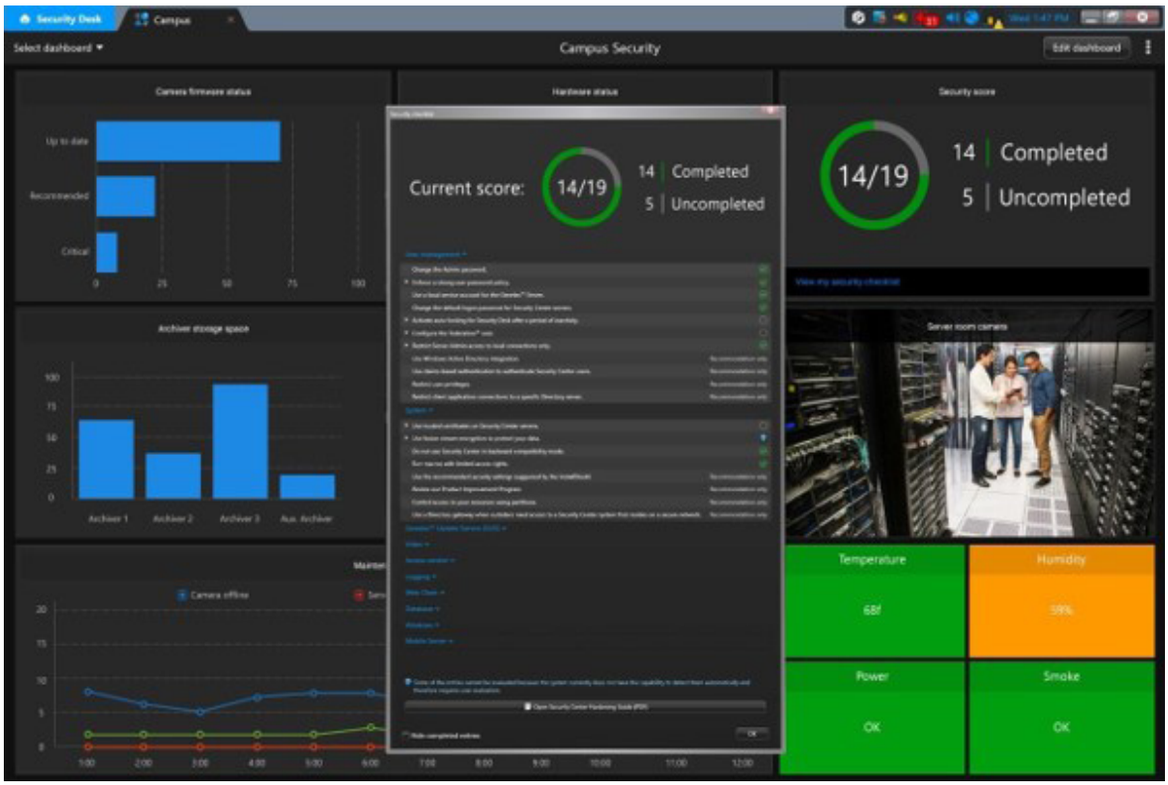
Genetec has been in business 22 years and their video systems are generating 15,000 petabytes (PB) of data. Having the ability to granularly analyse all of this data is clearly a business enabler. The R&D focus is becoming "how do we dig into the data our systems are collecting," said Philippe Ouimette, Director of Strategic Partnerships, Genetec. Hence why, again, it makes sense for Genetec to be working with Intel and Dell Technologies.

Daniel Corney, Solution Architect – Industry IoT, Surveillance and Computer Vision, APJC, Dell Technologies, walked through the Poweredge R740xd2 enterprise content server, which is the platform on which Streamvault operates. Built to provide scalable business architecture, with flexible internal storage, intelligent automation, and integrated security, the features include targeted workloads for media streaming (video surveillance and content delivery networks), Microsoft Exchange Mailbox and software-defined storage (like WSSD or vSAN).

Corney highlighted the ability to scale up to 416TB in a 2U with cost-effective internal storage and scale-out to 7.2PB in a 42U rack. This allows the management of thousands of hours of videos or Exchange mailboxes in one location and as a streamlined server, and comes with intelligent automation and integrated security.

The Dell EMC VxRail design principles provides turnkey experience, lifecycle experience and highly differentiated for full stack integration, networking automation, and advanced analytics. The VxRail comes with the iDRAC9 controller for agent free embedded server management and the OpenManage application to manage, patch and monitor server fleets. The cybersecurity approach is based on NIST guidelines to develop the Cyber Resilient Architecture, starting with silicon roots of trust and end to end supply chain assurance. There is a BIOS and iDRAC9 dual authentication to verify system integrity.

Genetec has thought strategically about the business proposition for integrators. This protection and verification



extends security across the server ecosystem and thereby the supply chain, proposing to be the world's most secure server against physical intrusion. It includes multiple layers of protection aligned to the iDRAC Credential Vault and Chassis Intrusion Alert, malware injection with Dual Silicon Root-of-Trust, 'tamper in transit' protection with Dell EMC Supply Chain Assurance, malicious firmware update via Root-of-Trust + Cryptographically signed and validated firmware, and rogue configurations attack (back to the iDRAC) and data breach protection with system erase and user authentication.

"We've eliminated the need to deploy Genetec software onto hardware before installation, providing pre-configured appliances that are essentially plug and play, with cyber security baked in — potentially saving days of precious time per project," said Ouimette. "Systems integrators and end users can deploy fully hardened systems, with automated updates based on regular testing and vigilance against threats built into the solution."

Lee Shelford, Sales Engineer for APAC, Genetec outlined how Streamvault is designed to secure the system deployment, increase margins via reduced installation times and therefore delivers enhanced business continuity. Cybersecurity is included by default. The system's connectivity allows monitoring and maintenance, with automatic patching. Hardening is by custom group policy, configured registry, set Windows firewalls, anti-virus, NetBIOS, forced custom passwords and verified Windows update status. Blackberry Cylance is deployed as the chosen malware detection tool and third-party penetration tests with letters of completion are also provided. Staying connected and updated includes the camera firmware, Windows updates validated by Genetec and real time notifications in the configuration tool.

The Streamvault portfolio includes 100 series to 300 series, bundled with all licences including number plate recognition and access control. The 4010e-R4-H provides Raid5 or JBOD up to 52TB and up to 570mbps on 1RU. For 4010ex – R26-H – up is suitable to 1000 cameras and 2.2gbps and 355TB based on 16TB HD and Perc740.

There is a 730 per cent performance improvement on offer over the 'off the shelf' hardware alternatives. This is calculated based on the standard 'customer off the shelf' or COTS server with 300Mbps recording and redirection and playback, all coming out of the 300Mbps. For the Streamvault, the 4011e, gives 2200Mbps, with 1300Mbps recording, 750Mbps redirection, and 150Mbps playback. For Federated systems they need to ensure systems can be redirected and have adequate throughput. This offers a 14RU to 2RU improvement or the calculated 750 per cent.

Genetec's Streamvault Dashboard

Finally, the analytics. Analytics appliances are built to run KiwiVision and working with Dell and Intel, the sva-1010e-h and Nvidia and running up to 80 video streams and the sva2000 will do up to 150 streams. Genetec has also recently announced the sharpZ3 PR mobile licence analytics with Intel Movidius myriad x VPU for high performance at the edge with deep learning capabilities. There is much more to dive into.

Over the last 18 months, Genetec reports that the transition to Streamvault in government, transport, and local government has been increasing. With a sound business case built on a trusted and security supply chain, this transition is likely to continue and is a platform all security consultants and integrators should have insight into. Not just for technical comparison but to be benchmarked against current designs and platforms on the market.

CYBER RISK LEADERS

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

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

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

★★★★★

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

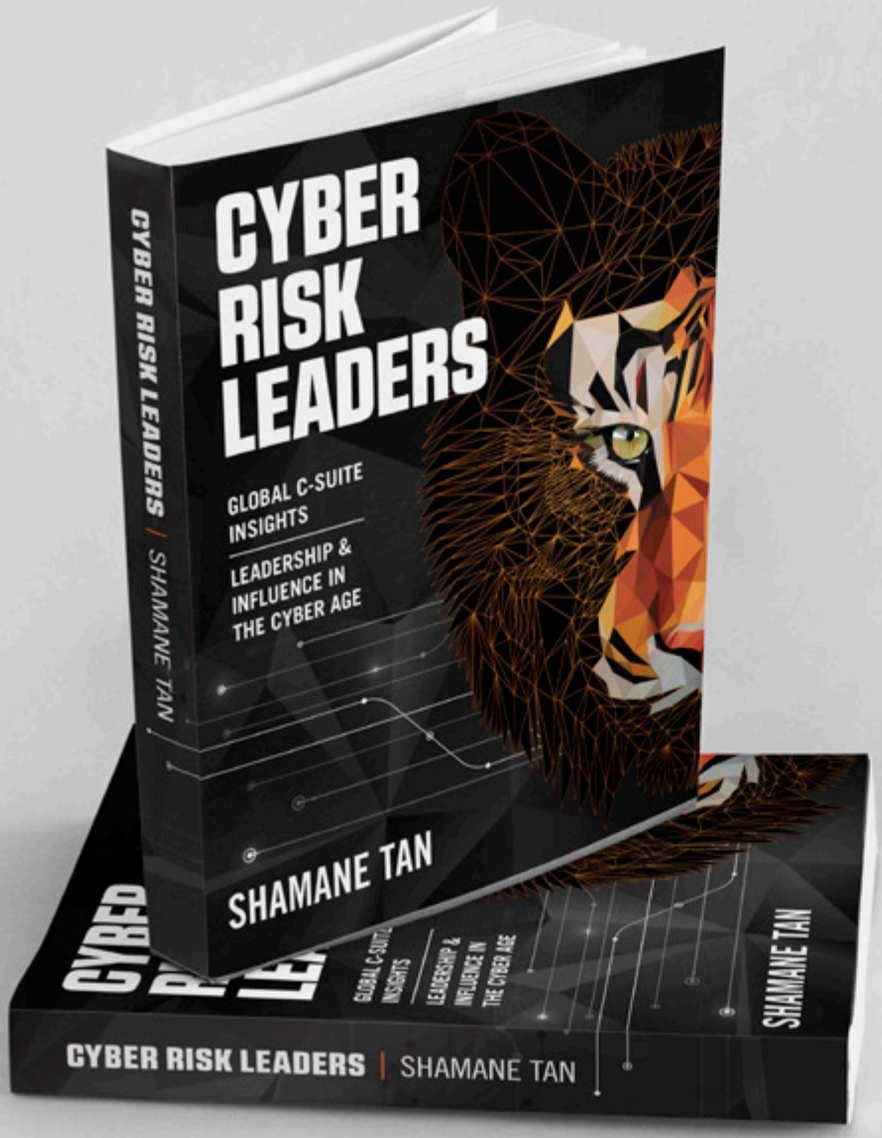
CEO, Cyber Security Capital (UK)

★★★★★

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

CISO, Telstra APAC

★★★★★



ABOUT THE AUTHOR

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

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

GET YOUR COPY HERE!

Proudly Published by

MYSECURITY MEDIA

www.mysecuritymarketplace.com

THE 'GO-TO' TOOL FOR LEADING PROFESSIONALS

MYSECURITY MARKETPLACE

- ✓ UP COMING EVENTS
- ✓ COURSES
- ✓ WEBINARS
- ✓ WHITEPAPERS
- ✓ SOFTWARE

promoteme@mysecuritymedia.com
www.mysecuritymarketplace.com