Cybersecurity Trends

UK edition n.2 / 2023

Secure Horizons:
The power of AI, Metaverse, Quantum & Blockchain

Global Cyberwatch:
Topical insights

Chain of Trust:
Tackling supply chain and Cyber Resilience

IN THE SPOTLIGHT

BlockAPT™

VIP Interview
with **Professor Lisa Wilson**

Contents

Foreword

In today's digitally connected world, cyber threats loom larger than ever. Malicious state and non-state actors continually seek to exploit vulnerabilities and compromise systems for their own gain. Meanwhile, rapid technological change introduces new attack surfaces and risks that we must move swiftly to address.

That is why I commend Cybersecurity Trends for its tireless efforts to promote cyber hygiene, raise awareness, encourage knowledge transfer and thought leadership, contributing to a more secure digital landscape for all.

In the face of increasingly sophisticated cyber threats, collaboration, commitment and proactive thinking are imperative. The Swiss Embassy in Romania supports since the first edition, in 2013, the Cybersecurity Dialogues Congress, organised by the Swiss WebAcademy in Sibiu / Romania. The Congress is an annual Central European dialogue platform that benefits from Swiss expertise and brings together security experts, both Romanian and international, to address cybersecurity challenges, solutions, strategies and behaviours.

Also, to raise awareness of the dangers of the online environment among the population, especially the young and elderly, who are digitally vulnerable, the Swiss Embassy has supported the dissemination in Romania of the Webster comics created by Swiss specialists. The comics address issues that any family member may face in the digital world: online scams, blackmail attempts, conspiracy theories, online behaviour, unpleasant content sites, screen addiction and all sorts of online scams. From the Webster family's adventures, readers are guided on how to behave responsibly in such dangerous situations. In addition, each story is accompanied by practical tips for avoiding Internet traps.

The comics can be used by parents, grandparents, teachers to initiate discussions with children about online traps and how they can be avoided. All 3 Webster seasons can be accessed and downloaded online from the website: https://www.websters.swiss/en.

I look forward to reading this and future editions of Cybersecurity Trends and watching the progress being made by Swiss WebAcademy.

His Excellency **Massimo Baggi**
Ambassador of Switzerland to Romania

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Editorial

Raj Meghani

Laurent Chrzanovski

Marco Essomba

The Path Forward: Inspiring Confidence in the Cybersecurity Landscape

The cybersecurity landscape around us continues to be in a constant flux of turbulence and opportunity in equal measure. Whilst emerging technologies like Quantum Computing, Artificial Intelligence, Blockchain, the Metaverse, and other technologies propel us to the digital landscape of tomorrow, they also open new avenues for cyber threats that could have severe consequences if left unaddressed.

Yes, emerging innovations introduce fresh vulnerabilities. Outsourcing and third parties create porous perimeters, allowing threats to infiltrate from all sides, multiply threat surfaces and increase risk exposure. But we see boundless opportunity - if we act now to build cybersecurity into these transformative innovations.

Quantum computing brings a new force to be reckoned with – a race against time. There remains confusion and a serious lack of understanding as organisations sit patiently to let others test the water on how quantum security will help fight the war against adversaries infiltrating data in motion and data at rest.

Staying resilient requires unity of vision, tight collaboration, and propping up fragmented defences across social, economic, political and geographic borders.

That is why the Cybersecurity Dialogues Congress in Sibiu, Romania last month offered a timely opportunity to bring together global security leaders and discuss solutions to harden systems against tomorrow's attacks, today. The discussions sent a clear message: We have the tools and insight needed to secure the emerging tech ecosystem. Now we must supply the will and act upon it.

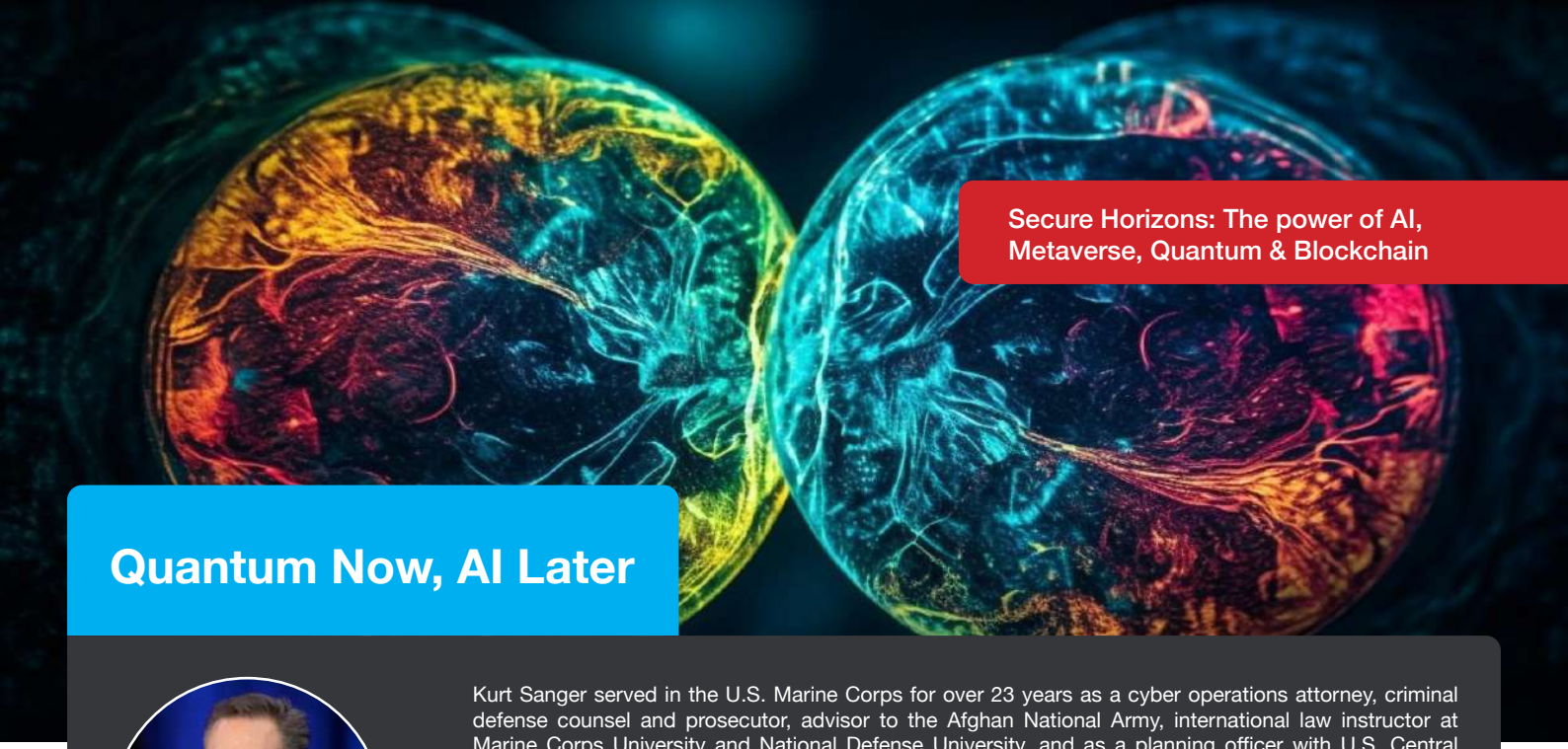
In the spirit of National Cyber Awareness Month and by pooling global insights and skills, we push the Public Private Partnerships (PPP) agenda forward. That is what we endeavour to do with this special issue of Cybersecurity Trends and our Global Cyberwatch section, bringing topics close to the heart of nations for all to share and benefit from.

We cannot do it alone. Policymakers must work closely with cybersecurity leaders to enact thoughtful standards that protect user rights. Organisations must invest in their teams through training, change their mindset and initiate forward-thinking upgrades now. And the industry must continue to come together across borders to share intelligence and build resilience.

The foundation is there. The motivation is strong. And the time for action is now.

Stay vigilant, but optimistic. Threats come and go; human resilience and imagination persist.

Happy reading!



Quantum Now, AI Later

Kurt Sanger

Kurt Sanger served in the U.S. Marine Corps for over 23 years as a cyber operations attorney, criminal defense counsel and prosecutor, advisor to the Afghan National Army, international law instructor at Marine Corps University and National Defense University, and as a planning officer with U.S. Central Command. He earned a degree in National Security Law from Georgetown University in 2015. From 2014 to 2017, Kurt was General Counsel for U.S. Marine Corps Forces Cyber Command. He served with U.S. Cyber Command from 2017 to 2022, first as the lead attorney for plans, policy, domestic and international partnerships, and legislative affairs, later as lead attorney for operations and intelligence, and finally as the Command's Deputy General Counsel. He retired from the Marine Corps in November 2022. Kurt is Founder and Director of Integrated Cybersecurity Partners, LLC, an information technology and national security consultancy. He is also a cybersecurity board member and advisor for Cowbell Cyber Insurance and Batten Safe Corporation, and a non-resident Senior Associate for the Strategic Technologies Program with the Center for Strategic and International Studies, a Washington, D.C. think tank.

Two technologies whose full promises and perils are largely to be determined are nevertheless dominating headlines on a daily basis, Quantum Computing and Artificial Intelligence. Few can predict their full potential; fewer understand how they work. They are the subject of speculation, debate, and prediction. Despite uncertainties, it appears organisations are taking immediate action regarding artificial intelligence but are not moving as quickly on quantum computing.

Any analysis of the technologies requires speculation, but for those who are keen to forecast, these variables should be among their considerations:

1) Are professionals taking immediate action regarding AI better served by a wait-and-see posture?

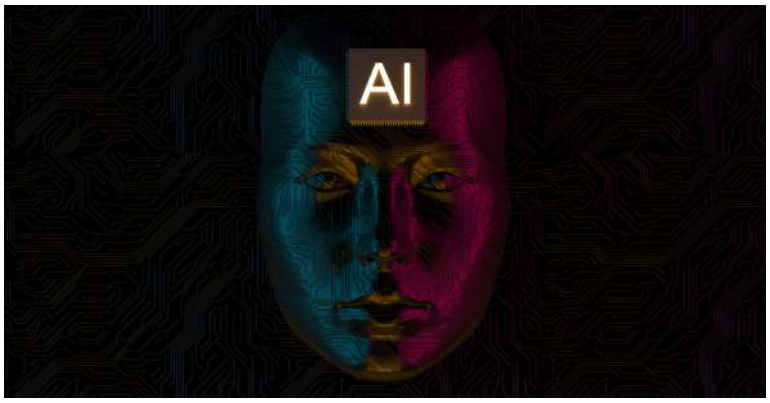
2) Are professionals taking a wait-and-see posture regarding quantum computing better served by taking immediate action?

AI's capabilities are becoming familiar to most through ChatGPT. While the tool is useful for personal and professional purposes, its work needs to be checked. When one calculates numbers using a traditional computer or presses print on a document, one can usually rely on a predictable result (even if the printing is unsuccessful!). With ChatGPT, one cannot necessarily rely on a result without independent verification, perhaps mostly vividly illustrated by a now-sanctioned U.S. lawyer who submitted a brief to a court using platform-generated cites to cases that did not exist. The effort needed to verify AI's work often defeats the purpose of using AI to begin with.

This issue may be compounded with time as the content generated by AI permeates other platforms and sources of information. Incomplete, poorly described, and entirely false information created by AI will make its way into databases, websites, and people's minds. These information sources potentially will deliver faulty information to each other and return it to AI platforms.

As a business model, AI faces separate challenges. It learns by taking in vast amounts of information and uses it to improve its own processes. Much of the information available to the public, and to AI databases, is protected intellectual property or regulated as sensitive information, such as personally identifiable or health-related information. Sometimes this information is available mistakenly.

When AI gathers information, whether through automated searches or user input, it often cannot distinguish information that is freely available for its use from information it should not use. Multiple copyright holders have filed suit against ChatGPT already (it has even come after the comedians!), with more almost certain to follow. Likewise, a class action lawsuit has been filed by individuals who believe ChatGPT has used their information without appropriate authorisation or compensation.



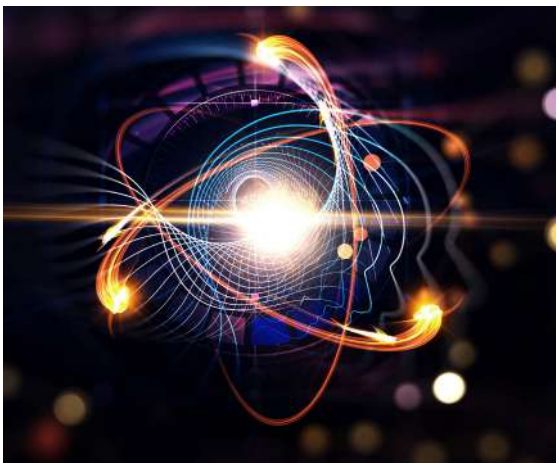
Beyond the scope of this article are the supposed threats that AI may pose to jobs, democracy, and all humanity, each of which have drawn significant speculation and fear. Though certainly worthy of exploration, and potentially far more disruptive than the issues described above, these considerations are not as immediate nor as tangible as current and anticipated litigation, flaws in AI's current outputs, and the time and effort required to check AI's work products. While there is risk in delaying the employment of new technologies, any organisation considering making use of AI should keep in mind its known and immediate perils, and anticipate unknown perils emerging in the years ahead.

Unlike AI, quantum computing is in development and unavailable to all but a few technical pioneers. Its eventual realisation is assumed but the arrival date of the first efficient and fully capable quantum computer is a matter of speculation. What quantum computing can achieve, and when it will be as ubiquitous as today's personal computer, is even harder to estimate.

What is known is that quantum computing will likely be able to decrypt many current forms of encrypted information. While this may seem like a threat that sits behind a distant horizon, in actuality it is already too late to protect many data sources. If encrypted information is stolen today and cannot be decrypted immediately, thieves can look forward to a day when quantum computing will be able to reveal it. This may still seem too far off for those making resource decisions regarding how to defend networks and their data, but thinking through the possibilities it is easy to see that investments must be made today to defend against future quantum capabilities.

Taking an arbitrary estimate of 20 years to achieve perfected quantum computing, a timeline significantly longer than many experts predict, information stolen today may not seem like it will be important or useful to a thief two decades from now. However, an individual's health data will certainly remain relevant, as will embarrassing information through which one can be extorted, as well as social security numbers, banking information for loyal customers, and transactions with government offices.

Regarding business organisations, if there is any doubt regarding the relevance today's data will have to malicious actors two decades from now, try this thought experiment: if a business' 2003 database were opened and made publicly available today, what information would it hold that could undermine the value of that business or negatively impact its reputation? It is likely that some 20-year-old emails attributable to current private sector leaders might prove embarrassing, and that an organisation's trade secrets and proprietary information of that era would still be valuable and worth concealing today, and old network configurations might reveal vulnerabilities that could be exploited now. Organisations holding valuable data, whether intellectual property, customer's personally identifiable information, or any other information worth stealing, should seek out quantum-resistant methods to protect that information now.



While the thrill factor of AI and its accompanying dangers have drawn the most attention, quantum computing and its potential to decrypt protected information on an unknown but impending date should be the priority risk that network defenders prioritise. AI's drawbacks are being realised daily while its ability to deliver useful outputs has been challenged. For those making resource decisions regarding their information technology budgets, quantum computing deserves as much if not more attention.

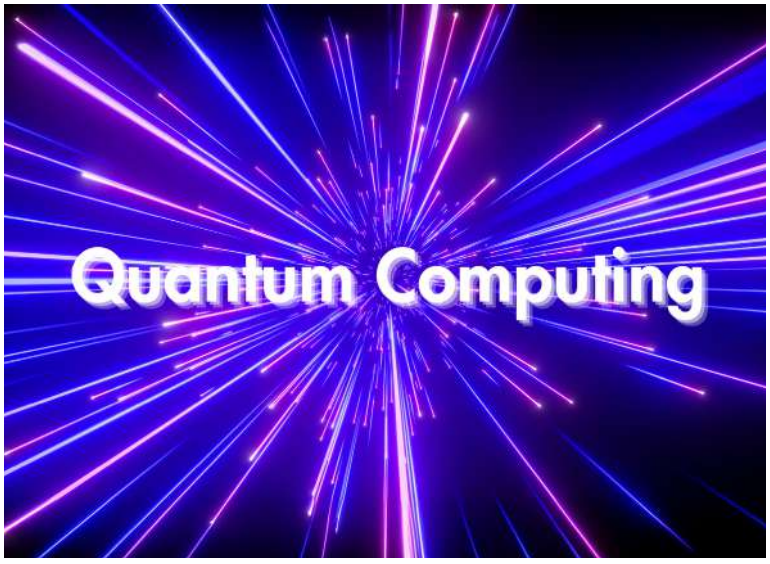
Blockchain Technologies and Quantum Computing in Cybersecurity: Friends, Foe or Happy Marriage?

Professor Lisa Wilson

DUniv., FBCS., FRSA., Grad. Cert Sc., Bch T&D, Dip. T&A Sys., Adv. Dip. OHS, BA (Economics, Geog., Fin. Mgt.) Dip. Ed.Professor Extraordinaire: Innovation, Digital Technology & Entrepreneurship Managing Director, XTCC Investments, Tallinn, Advisor, BondStream - Estonia, UK, Singapore, Dubai Advisor, Bedford Row Capital - UK, Estonia, Singapore, Dubai Academic Advisory Board: International Association of Trusted Blockchain Applications [INATBA] Legal Advisory Council - UK ICC Centre for Digital Trade & Innovation [C4DTI] Chief Research Officer, Global Foundation for Cyber Studies & Research [Washington DC] Fellow Royal Society of Arts, Manufacturers and Commerce [FRSA], London UK Fellow British Computer Society [FBCS], London UK Adjunct Faculty La Trobe University Adjunct Faculty SARChI Innovation Research Group [Tshwane University of Technology [South Africa]] Adjunct Faculty African Post Graduate Academy [APGA]

Blockchain and Quantum Computing are arguably two of the most extraordinary and game changing technologies of our time. However, the most common consensus is that fundamentally they are diametrically opposed to each other because they have core development principles that conflict. It's a little like coriander – you either love it or loathe it.

Advocates for quantum computing believe it will be the challenger that undermines blockchain and to the contrary blockchain advocates believe that quantum technology is a nascent player and improvements to blockchain will surpass any alleged challenge. It's a bit of a quandary because in reality there's always a middle ground, where instead of being foes, these technologies could play nicely together as best friends. It might be fanciful, but they could even become a happy marriage and produce huge benefits and impact to ensure our digital world is trusted and secure by design.



The conflict arises primarily in three areas, decentralisation versus centralisation, the security paradox and privacy as opposed to transparency.

Proponents of quantum technology highlight that it is computationally powerful enough to break the cryptography used within blockchain such as the Elliptic Curve Digital Signature Algorithm (ECDSA) for the creation of public-private key pairs and the SHA-256 which is used for the creation of hash functions. It's almost a gloat worthy feature that blockchain's core disruptive security features could be broken by quantum technology placing transaction and data security at risk and of course exposing crypto assets to the possibility of theft and unauthorised transactions. This thinking feeds perfectly into the hearts and minds of blockchain naysayers looking for ways to compete as foes rather than play as friends. This thinking can also blind us to the true value of working together and to realise that the greatest potential occurs when we see opportunity from strengths not weakness because of difference.

Blockchain's rely on a mechanism of consensus – or agreement - to validate and add blocks of data. These mechanisms rely on computational calculations and assessment and inefficiency is the very reason new consensus mechanisms such as Proof of Stake have evolved from Proof of Work used by Bitcoin, the first and still the largest blockchain. Quantum computing's strength is that it has the innate capacity to churn through computational calculations at unimaginable speeds. If that strength were applied to blockchain and the two worked together, blockchains could arrive at consensus in a faster, more efficient way, overcoming one of the barriers to adoption. Transactions could be faster, and more efficient and use cases of the technology could expand.

With growing use of IoT, sensor technology and AI, it's difficult for a human mind to think how fast information could be processed. From a cybersecurity perspective, it could mean that the potential quantum efficiency in the wrong hands could expose a risk for malicious actors to carry out a 51% attack where they can disrupt the recording and approval of new transactions. It's important to understand that technology can be friends but there'll always be enemies trying to rattle the cage of harmony and cause conflict in our digital world. That isn't a technology issue – that's a human ethics, integrity and honesty problem. Criminal minds look for weakness to exploit so the advantage is that if technology can think and work faster than they do, we might edge ahead in the race for digital trust.

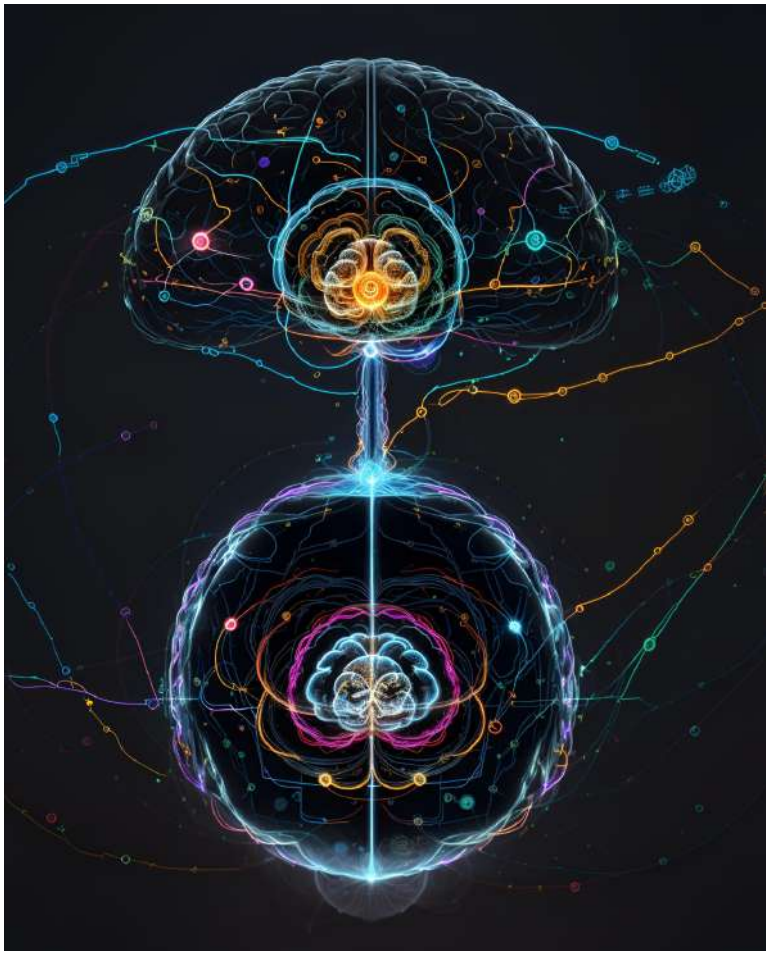
These potential threats have led to a great deal of work on post-quantum or quantum-resistant cryptographic algorithms and systems that by design will retain blockchain security making them immune to security threats posed by quantum computers. If you think about it, it's like working together to create a vaccine to overcome an unwanted predicted outcome. Transaction visibility and provenance is another core principle of all blockchain technology. Having gatekeepers and developing systems in different ways such as private and permissioned blockchains affords enhanced security access and availability for sensitive environments but the transparency still remains at the heart and soul of blockchain. To the contrary, quantum computing is fundamentally driven by ultra-privacy. It uses complex encryption methodology such as Quantum Key Distribution (QKD) where any attempt to observe a quantum system inherently alters that system. As a result, the transparency of blockchain conflicts with the concept of perfect secrecy of quantum communication.

But again, the real opportunities lay with how these two opposites attract. Quantum secrecy can certainly work in harmony when blockchain systems require access to the outcomes of a central source of highly sensitive information and data subsets and that is required quickly such as political, health, financial or digital trade information. This profoundly expands the 'secure by design' principles that cyber and digital experts often discuss. If we really want to shift our minds to 'what's possible' overlaying AI into the mix for both blockchain and quantum computing could exponentially increase secure data processing to the point that cyber risks, trends, breeches and reputational challenges could be identified in moments rather than months or years that it takes now. For any CISO, this could be game changing relief.

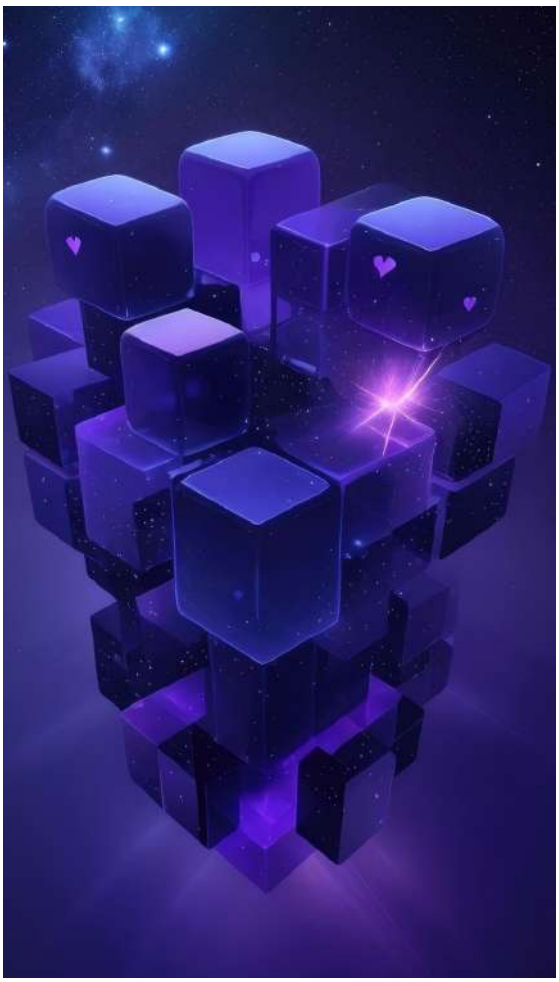
There is already work being conducted on marrying the benefits of blockchain and quantum technology to produce quantum blockchains. This can be easiest described as a decentralised, distributed, encrypted database that is built with quantum computational technology and information theory. In essence, in a quantum blockchain network, each node stores a copy of the blockchain – encrypted by quantum theory. Researchers from several companies and countries are exploring the concept of quantum blockchains, that would be able to maximise the potential of QKD properties that prohibits cloning and intrusion giving maximum digital security and digital trust by design.

The future of a trusted digital society through a marriage of what many believe are foes into quantum blockchain will be beneficial for all technologies that have a foundation based on distributed storage and consensus mechanisms. An obvious use case would be electronic voting systems and international collaboration systems such as pandemic, terror and natural disaster warning systems. Also critical systems, where development of these is often held back because stakeholders have no trust, data movement is limited by nationalistic regulatory mechanisms and data sources are highly sensitive.

The final primary conflict between blockchain and quantum technology is decentralisation where authority and decision-making processes are distributed to all participants or nodes. It is democratised by design. Over the years, blockchain technology and its costs have lowered much the same as the Internet, WiFi and data have. Quantum technology is still nascent, few in numbers, very high-cost, and requires super specialised environments with expertise to operate. These parameters inherently lead to a centralised model because it is not something that is yet accessible to many. This conflicts with the core principle of design of blockchain – that it is available to all.



In reality though we know that education and understanding of blockchain technology is still limited despite it being foundational technology.



We know that less than 3% of our global decision makers have knowledge about blockchain and that fear and misinformation still drives adoption. We are really only now starting to see institutional and broad adoption throughout business sectors. It could therefore be argued that blockchain, a decentralised technology, has knowledge and adoption that in many ways is still centralised. In part, this is more about the fact that each is at a different place in their development curve rather than centralisation is in conflict. Is that any different than being a friend with someone of a different age or level of experience?

Technology advances are happening at an exponential rate of change. Blockchain is a foundational disruptor in the way we engage in business and life digitally whereby trust by design is its core principle. Quantum technology can think and process information at speeds that are unimaginable. And AI can read information from vast sources as humans we would take a lifetime to read. All these do have core conflicting elements, as do people. We are all different. But our strength for a secure by design future sits with our ability to see how our weaknesses can be bolstered by playing as friends with technologies that can harmoniously complement and support challenges.

The world becomes our oyster - provided our thinking includes ethics, integrity and acceptance that people, not technology, are innovative.

A Trio of Technological Paradigms: AI, Metaverse & Blockchain

Erik Alfonso Nilsen

Erik Alfonso Nilsen, PhD, is a physicist with advanced degrees in electrical engineering and mathematics. He has co-founded multiple companies since 2000, including TauTuk Cyber and Bio-Signal Technologies. Nilsen has a passion for signal/image/video processing, weak signal monitoring, analysis, and prediction, and has developed novel methods derived from chaos theory, fractal geometry, topology, electromagnetics, DSP, neuroscience, and nonlinear dynamics in his work. A strategic startup consultant for high-tech and med-tech startups, he also performs technology due diligence for PE/VC firms' portfolio companies. He is the author of numerous peer-reviewed publications in the physical and medical sciences, patents, and two books. Erik is a proponent of the decentralized internet and has recently been focused on out-of-band analogue and digital methods to help reduce hackers' success rates.

In our progressively digitised society, we are witnessing a compelling trio of technological paradigms that are profoundly shaping the current era: Artificial Intelligence (AI), the Metaverse, and Blockchain technologies. While these may initially appear as ephemeral novelties or even transient trends, their potential and burgeoning significance are triggering a sea-change across our Internet landscape. They are pushing boundaries and expanding the realms of possibilities in ways that were once unimaginable. Nonetheless, as these avant-garde innovations mature and become increasingly embedded in our daily lives, they bring with them a bountiful of challenges – ones that necessitate nuanced understanding and proactive measures. Among these pressing complexities are those related to cybersecurity and system performance.

Pillars of the Digital Transformation:

1. Artificial Intelligence: Bridging the Chasm between Humans and Machines

Artificial Intelligence (AI), the audacious ambition to reproduce human-like intelligence through machines, made its embryonic beginnings around the mid-20th century. Its early iterations were ensconced in simple algorithmic computations, intended to mirror, albeit in a rudimentary fashion, certain facets of human cognition. Fast forward to the present day, AI has morphed beyond recognition, thanks to a confluence of forces such as complex mathematics, the ability to process staggering amounts of data, and rapid advances in computational horsepower. Today's AI exhibits extraordinary abilities ranging from ingenious pattern recognition to intricate decision-making. This sophistication is largely owed to the evolution of AI into neural networks or advanced systems capable of complex computation and analysis.

Over the past decade, the tentacles of AI have reached into almost all sectors of life, prominently in healthcare and finance. In healthcare, AI systems play a pivotal role in detecting diseases at their early stages and aiding in drug discovery. As we journey further into this digital age where abundant data reigns supreme, AI steps into the breach to support data-heavy tasks such as diagnosing patients remotely, thereby facilitating telemedicine. In the financial domain, AI assists in forecasting stock market trends with remarkable acuity and plays an invaluable part in credit scoring. Notably, AI brings to the table a highly potent combination of increased efficiency, greatly reduced error rates, and intelligent data management.

2. The Metaverse: Beyond the Virtual Veil

The concept of the Metaverse is straight out of the pages of science fiction, projecting visions of a breathtakingly vibrant digital universe that overlaps with our physical one. When broken down to its bare bones, the Metaverse introduces a unified digital-physical experience that engrosses all our senses, generated by a convergence of assorted technologies. At its foundation are Virtual Reality (VR), Augmented Reality (AR), alongside rapid strides in networking, computer graphics, and most importantly, enhanced connectivity ensuring real-time interactivity.

While path-breaking initiatives like META's fantastically devised Metaverse are beginning to take shape, it remains a work under construction. As a consequence, despite its grand expanse of possibilities such as virtual concerts, digitally-curated business meetings in extravagant virtual conference rooms, and an educational avenue with virtually revamped campuses, it brings its shadowy challenges. Any conversation surrounding the Metaverse would be fragmentary without acknowledging the elephant in the room - privacy and data security concerns, along with establishing authenticity in digital identities and managing socio-economic disparities.

3. Blockchain: The Trust Backbone of Digital Transactions

Blockchain technology has been a game-changing addition to the contemporary digital vocabulary. Initially associated primarily with Bitcoin, blockchain has transcended its beginnings since its birth in the late 2000s, evolving into an evergreen technology used far and wide today. At its core, blockchain provides a decentralised ledger that enables recording transactions with utmost transparency and verification processes accessible to all parties involved.

4. The Cybersecurity Concerto: Encryption-free Security and Performance

Paradoxically, as we plunge deeper into the digital era, cybersecurity subsequently escalates in importance. Traditional safeguards, although offering secure blankets against penetrative threats, also tend to throttle system performance due to the substantial computational resources requisitioned for the encryption-decryption process. Cutting-edge research is thus par for the course in devising advanced mechanisms and sophisticated hardware for data protection without compromising performance.

Encryption-free cryptography poses an innovative alternative to traditional encryption techniques, offering exciting new vistas towards higher processing speeds and greater efficiency without relinquishing data security, privacy, and integrity or user confidentiality. Recent research heralds an ambitiously formulated solution set which not only promises to combat cyber threats effectively but also enriches users' experience by enhancing performance metrics.

Gravitating Towards the Horizon: A Unified Perspective

With these three technological marvels marching apace towards maturity, the digital landscape is ripe for a revolution. Visualise a vibrant Metaverse buzzing with AI-curated avatars, interacting and conducting transactions verified through blockchain underpinned scaffoldings. Imagine this not as a scene from a glossy sci-fi blockbuster but as an imminent reality about to be navigated daily.

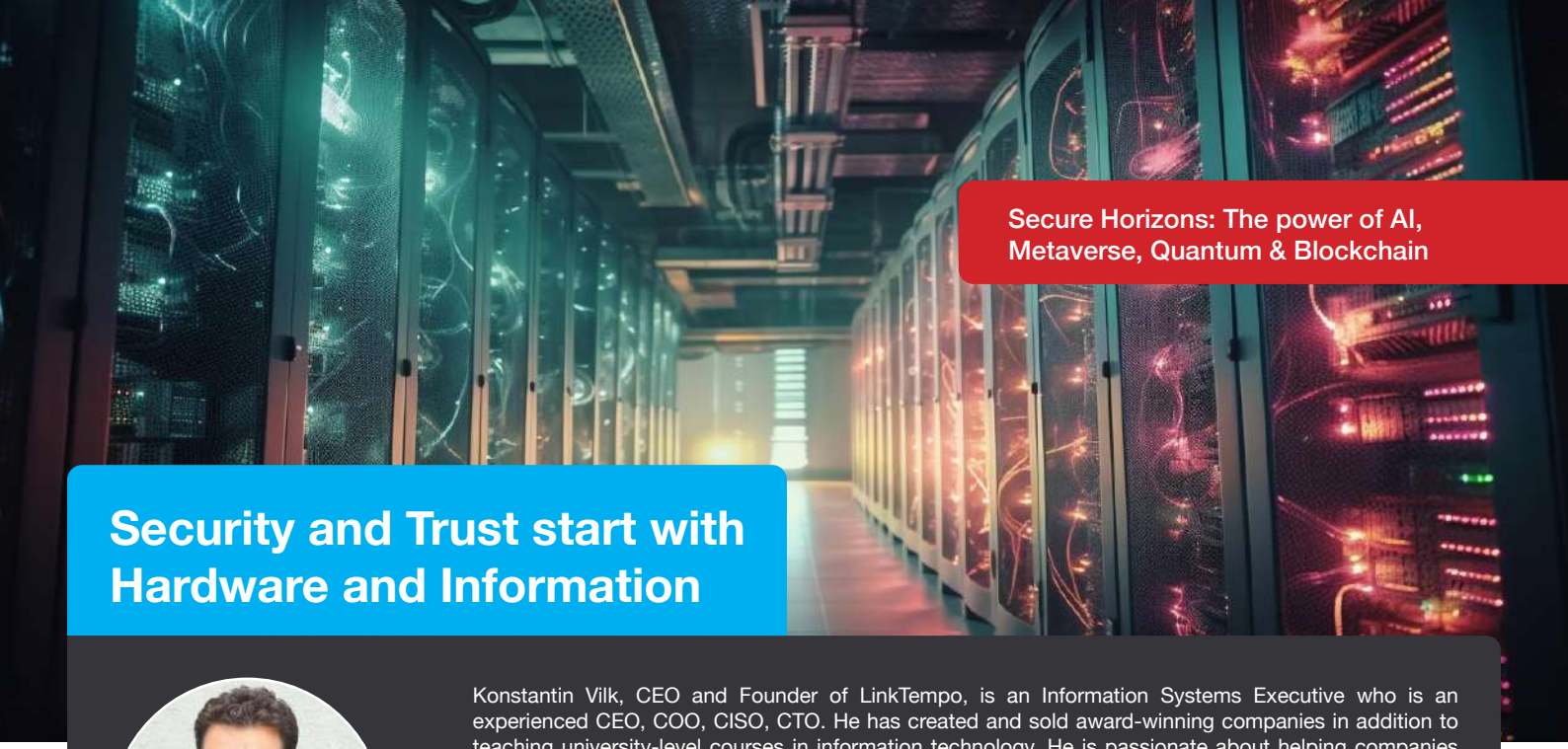
As we hurtle towards this future, the significance of balancing robust security protocols with performance standards becomes paramount. On one end, are ingenious metaverses demanding lightning-fast transaction speeds verifying micro-transactions spanning milli-seconds; at the other end are soaring computational demands by complex AI algorithms necessitating high-performance computational capabilities to deliver real-time results.

Conclusion:

As we inch ever so closely to this new dawn, it becomes unequivocally critical to understand these lofty digital constructions and their synergies for an inclusive digital future.

We need to adeptly navigate these panoramas while keeping our sight reserved for not just the glorious sunrise but also the deepening shadows it casts. Harnessing these technologies' potential presciently and responsibly necessitates an uncompromising commitment towards fortified cybersecurity practices. Only then can we ensure a promising future illuminated by AI, the metaverse, and blockchain technologies' brilliance, harmoniously humming a symphony of secure horizons on the power grid of a digitally transformed world.

Hence, the burgeoning marriage of AI, the Metaverse, and blockchain holds an optimistic promise of a secure, fast-paced universe that elevates user-centric experiences and convenience to unforeseen pinnacles. The tantalising vision of encryption-free systems contributing to a digital future with enhanced performances, even under greater data security and privacy configurations, is within our grasp. With this projection in sight, the importance of traversing this evolution wisely, with due heed paid to cybersecurity and efficiency measures, is a call to action we must take seriously going forward.



Secure Horizons: The power of AI, Metaverse, Quantum & Blockchain

Security and Trust start with Hardware and Information

Konstantin Vlik

Konstantin Vilk, CEO and Founder of LinkTempo, is an Information Systems Executive who is an experienced CEO, COO, CISO, CTO. He has created and sold award-winning companies in addition to teaching university-level courses in information technology. He is passionate about helping companies create incredible products and has extensive experience in Quantum Computing, Quantum Cryptography, Artificial Intelligence, Cyber Security, Cloud, Innovation, Marketing, Sales, M&A and implementation of enterprise-wide systems. Prior to founding LinkTempo, Kosta founded QuSecure, an award winning and fast-growth Quantum Computing Cyber Security company and Quantum Thought, a premier quantum computing launchpad for the founding generation of quantum computing companies. He also created an award-winning company named I-Span which became a leading partner in the transformation of corporate systems to the Cloud. After his exit from I-Span he headed Technology and Cyber Security in the financial services sector. He is recognized as one of the top CTOs in the quantum computing field and a thought leader in quantum computing, data management and compliance.

Over the past two decades and through evolutions of technology including the growing maturity of AI, growth of IoT, Blockchain and Quantum, we are consistently drawn back to the fundamental concept of Trust. It's the evolution of our conversation on cybersecurity, our latest developments and our push for improved resiliency and safety as we connect digitally. Irrespective of whether we discuss Web3, Quantum Computing, Identity and Access or even Blockchain, to name a few, trust is the pervasive part of this conversation because it is the fundamental aspect of how we connect before we even begin to communicate. Yet, defining what is Trust, and importantly Zero Trust, has become a source of confusion in many ways.

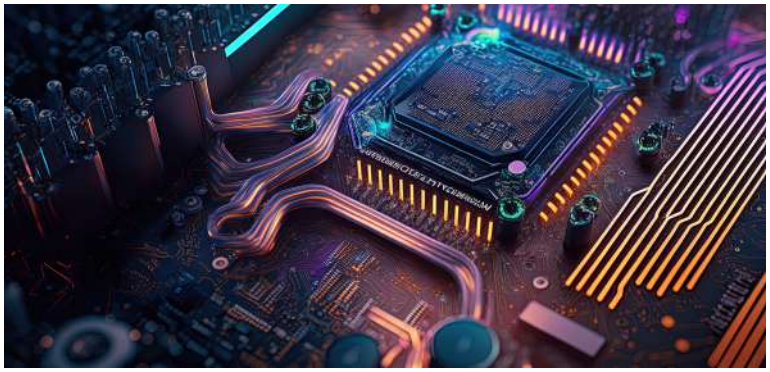
As we look at John Kindervag's Zero Trust framework as extended into NIST Zero Trust Architecture, we assume that none of the devices, identities, systems and users are trusted by default. As such, we need to continuously validate that identity of account or device, execution of the connection and the connection is still secure, after all, things change and often in real-time. As these changes occur, we need to continue to monitor and manage that trusted relationship even after the baseline connection is established via the initial authentication and authorisation.

If we look at tools we use to ensure security and resilience of our data and communications, or specifically their marketing, we are inundated by the confusion created around what that Zero Trust actually is and how it is managed and operated in the real world. AI and Behavioural Analytics messages seem to play a role in the conversation, as well as Identity Governance and so many other messages. However, they play only a part of what true security is and tend to focus less on the importance of hardware, cryptography and adaptable management capabilities as an integral part of that conversation.

Let's unpack.

We have known throughout history that any one defence tends to be a minor speed bump in the attacker's initiative. Success and actual results lie in the orchestration of how all defences play together to drive the outcome we really want, safety. Assets are valuable to us, but we don't have to protect all of them the same way, what's good for one is not necessarily effective for another. Generally speaking, the most effective defences for safeguarding data, in the market right now, leverage protections up and down the stack and deflect the attack to sandboxes to divert the attack or by logically segmenting endpoint hardware and prevent the attacker from leveraging their capabilities effectively. By segmenting assets and resources against rogue processes or even bad application code by applying preventative controls they effectively sandbox bad processes, resource misuse and applications trying to perform unauthorised actions.

Hardware is that integral element. One that's been historically unmanaged, non-resilient and accessible to well-resourced attackers. Now there is a growing industry push for hardware to be more connected, more secure and more resilient. Naturally, it means that hardware needs to be managed, monitored and updateable, even at the processor and sub-controller level. How else will we respond to zero-day and APT threats as they evolve towards other "softer" targets easier to attack like the CPU, Board, Wireless card or Memory. Keep in mind, we are constantly creating those softer targets by defending our assets better and forcing the attacker to pivot their attacks to what we forgot to defend in our rush to plug higher priority holes in our security.



With that continually increasing and evolving attack surface against hardware, spurred on by a greater number of IoT, Endpoint, Edge and AI devices and their increased compute capability, we need a method of better aggregating data to manage these assets at a much more granular level.

By aggregating data, we have an opportunity to process it into better information that drives actionable insights at scale to inform our understanding of use, our ability to be compliant, and of course our defences.

As we look to have comprehensive and scalable security, tools like BlockAPT are there to defend systems and information by enforcing Quantum Resilient protection and data aggregation from other security devices. These tools work in concert with ZTNA from companies like Cyolo, when we access our vital data, or GarbleCloud for quantum resilient data protection. When these are superpowered by secure data processing and persistent compliance mechanisms developed by LinkTempo to address the growing informational needs well beyond the security tools alone, they combine to become our informational footprint.

The use of Cyber-Mercenaries in the Economic Warfare of Artificial Intelligence

Stéphane Mortier

Stéphane Mortier is currently deputy head of the Centre for Economic Security and Protection of Enterprises (CSECOPE) within the General Directorate of the French Gendarmerie and a member of the Gendarmerie National Research Community (CREOGN). He is assiciate lecturer at the University Gustave Eiffel. He has a degree in political science, sociology and international relations from the Université libre de Bruxelles (ULB), in strategic management and economic intelligence from the École de Guerre Économique, and a doctorate in management at Paris 1 Pathéon Sorbonne. He is also the representative of the foreign sections of the ULB Alumni Union and chairs the French section (UAEF). Within this framework, he develops cooperation projects in Africa. He is a lecturer at the Ecole de Guerre Économique (Anti-Money Laundering), at the University of Likasi – DRC (Stategy, Business law). He is a founding member of the Cercle K2 and an active member of the Association pour l'Unification du Droit en Afrique (UNIDA). He is the author of some publications on economic intelligence.

Artificial intelligence requires vast quantities of data to develop. It's no secret that GAFAM, BATX and NATU collect data from their users in order to develop new tools based on it. Nobody is fooled by the fact that Tik Tok was created to collect data, for example[1].

At the same time, cyber attacks seem to be increasingly focused on stealing data: health data[2], data from research laboratories, financial data, personal data... and even casino data! In short, any type of data can be stolen... and sold to whoever needs it.

Apart from the case of espionage (mainly economic or military), it's a safe bet that this stolen data can be used as training data for future artificial intelligence tools. Cybercriminals are either thieves and/or receivers of stolen data sold on the darkweb or elsewhere, or they are "mercenaries" acting on behalf of a client (foreign powers, industrialists, laboratories, etc.).

In both cases, AI is at the heart of the problem: as a tool for obtaining data or as a requester of data for its development.

So we have belligerents (States, digital industries, laboratories), combatants (cybercriminals), weapons and ammunition (IT tools and data), and a strategic objective (artificial intelligence). In short, all the elements needed for a real economic and technological war.

Artificial intelligence as a tool for cybercriminals

Cybercriminals are making increasing use of artificial intelligence tools to commit their crimes. Just take a look at the main modus operandi:

1. Phishing:

Traditionally, users have been able to detect phishing mainly by identifying the poor quality of the message contained in the email they received (spelling or grammatical errors, poor quality images and logos, bizarre signatures, etc.). Nowadays, cybercriminals use extended Large Language Models (LLM) to draft their messages. Such models generate texts that are virtually indistinguishable from those written by a human. Technically, this is a transform-based neural network[4] . These basic models use generative AI for Natural Language Processing (NLP[5]) and Natural Language Generation (NLG). This makes it almost impossible for a user to tell the difference between an email written by a writer or by artificial intelligence. This greatly increases the cybercriminal's chances of success.

2. Bypassing anti-spam filters and creating email addresses:

Artificial intelligence can also enable a cybercriminal to bypass anti-spam filters and create apparently legitimate email addresses. Spam filters are based on machine learning to assess the reputation of the sender and the content of the email and thus assign a degree of threat to the recipient. Cybercriminals use a multitude of techniques to fool the artificial intelligence filtering spam (use of public services with a good initial reputation such as Gmail, Dropbox, etc.; use of warm-up solutions[6] ; multiplication of sending IP addresses; cascade compromise of accounts to benefit from the reputation of the first account; hiding the content of the message behind a reliable site or URL redirection or shortening; hiding the content behind a captcha; use of sandbox evasion malware[7]). As for the creation of reliable e-mail addresses, this is simply a matter of generating an address that will have a "good reputation" and will therefore bypass the detection capabilities of anti-spam filters.

3. Ransomware and encryption:

Ransomware attacks are becoming more effective by the day. Cybercriminals use AI to encrypt files while evading anti-virus software and, above all, identifying the most sensitive and strategic files for the victim. Most victims of ransomware are companies or institutions holding strategic or sensitive data. Artificial intelligence can be used to identify files with high added value for the victim, putting particularly strong pressure on the victim, who will be more likely to pay the ransom.

4. Social engineering:

In a social engineering cyber attack, where the attacker exploits the vulnerabilities of the victim through social interaction, the confusion between fiction and reality, made possible by AI, is unstoppable in achieving the set objective. The victim, deceived by a "false virtual reality", then finds himself in a situation where, naturally, his behaviour will unconsciously lead to the compromise of an information system or, more simply, to being extorted. This abusive use of AI can be practised at various stages of a cyber attack using social engineering: from the search for information on the target to the execution of the attack, via the approach phase[8].

5. Deepfakes:

Deepfakes are commonly generated by artificial intelligence. Cybercriminals create fake videos, images and audio recordings that are realistic enough to deceive any user or recipient (see social engineering above). These deceptive and manipulative media are used to set up scams (fake president fraud, for example), to spread propaganda and false information, etc. AI makes it possible to manipulate facial expressions, voices and gestures in images, videos and soundtracks, blurring the line between reality and illusion.

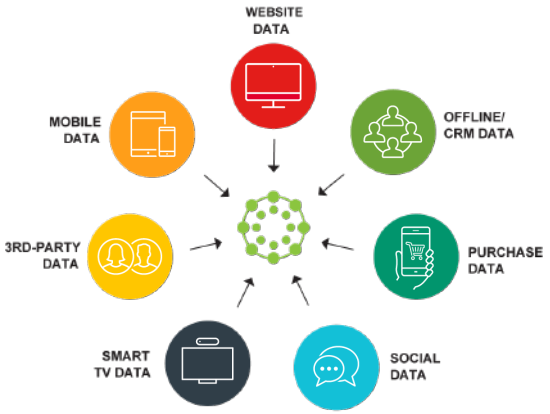
Botnet creation and management:

AI plays a central role in the creation, management, streamlining, coordination and optimisation of botnet activities. These can be used for DDoS attacks, spam distribution and, of course, data theft.

Added to these modus operandi is the fact that cybercriminals can attempt to exploit AI by reverse-engineering AI engines. If they can simulate AI systems, they will know whether an attack they are planning will be detected by a system.

In short, AI is becoming a tool in the service of cybercrime and the modus operandi. Although identical for many years, it is becoming more complex by the day and increasingly difficult to thwart. Most of these attacks are ultimately aimed at capturing data and possibly falsifying it. The question is: "What is the final destination of this data? Is it only "marketed" on the darkweb, or does it have a more strategic purpose? Could it be used, in one way or another, to fuel the development of new artificial intelligences such as training data?

A need for data to develop artificial intelligence tools



Let's take a step back a few years: at the Web Summit 2016, Facebook's Chief Security Officer said that his company was buying login data available for sale on dark web markets[10] , a practice that had been in place since...2013[11]. Facebook buys compromised login data in order to identify which of its users are using weak passwords. These users are then invited to change their passwords to something more complex and unique, to ensure tighter controlled account security. So what is the situation today? Will data obtained in this way be used as training data for future artificial intelligence tools? The question remains open, but the hypothesis has been put forward.

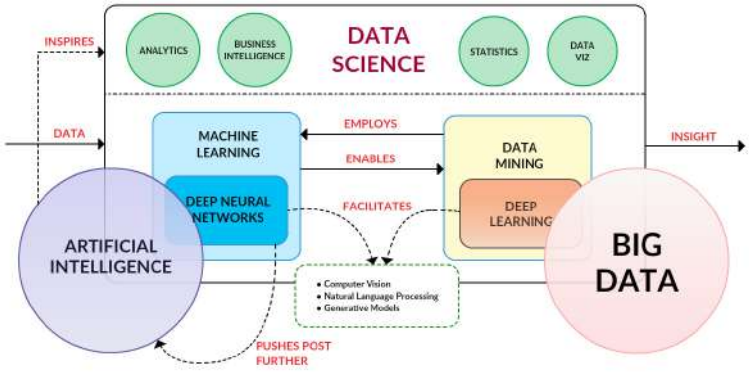
While it is acknowledged that the United States is best placed to win this AI race, thanks to its impressive pool of highly qualified engineers, its particularly dynamic innovative companies and its army, which is already beginning to integrate certain technological applications, China nevertheless seems well positioned to overtake it. This ambition is clearly visible in the "Next Generation AI Development Plan (AIDP)", unveiled by the Chinese government in July 2017. It envisages China becoming the world's leading AI power by 2025, and the world's leading innovation hub by 2030[13]. The AIDP sets out three key milestones, each containing a series of goals, some of which are narrowly defined, while others are more vague :

1. By 2020, China intends to remain competitive with other major powers and optimise its AI development environment. In monetary terms, China intends to create an AI industry worth more than 150 billion yuan (around $21 billion). Finally, it is seeking to establish initial ethical standards, policies and regulations for vital areas of AI;

2. By 2025, China aims to achieve a "major breakthrough" (as stated in the document) in basic AI theory and to lead the world in some applications (some technologies and applications reach world-leading levels). China also aims to increase the value of its core AI industry to more than 400 billion yuan (about $58 billion), and plans to develop and codify in law ethical standards for AI;

3. By 2030, China aims to become the global centre of AI innovation. By then, the growth of the core AI industry is expected to more than double again and be valued at 1 trillion yuan (around $147 billion), and further improvements in laws and standards are also expected, in order to meet new emerging challenges.

In other words, the Next Generation Artificial Intelligence Development Plan is intended as a blueprint for a comprehensive AI ecosystem for the country[15]. In short, China is striving to create AI systems capable of analysing and reacting to geopolitical changes, giving it a competitive advantage over other states[16].



There are also the raw materials (rare metals in particular) that are essential for electronic components, including the semiconductors needed for AI tools. Without these components, AI developments are impossible, and their manufacturers have a veritable weapon of economic warfare at their disposal. Access to and production capacity for these components is a matter of economic warfare.

To achieve such objectives, in such a short space of time, with stretched financial resources, it is necessary to collect data in almost infinite quantities and, above all, to obtain results. It is legitimate to wonder about the origin of the data used as training data in AI tool development programmes. Of course, it is not a question of levelling simplistic accusations at one or other of the protagonists, but it is clear that there is a fine line between legality and illegality, as the example of Facebook cited above shows. It would also be unfair to point the finger solely at GAFAM, BATX and NATU or even the major powers such as China and the United States. Indeed, every state power has AI ambitions, every sector of economic activity needs AI tools, and every malicious actor (organised crime, ideological terrorism, etc.) is looking to improve its modus operandi.

We are therefore faced with a world of high-intensity economic warfare, in which the use of mercenaries is no less a reality than in a traditional military conflict, and in which data is at the heart of the conflict.

Source:
1. https://www.lebigdata.fr/tiktok-donnees-proteger
2. Si veda il nostro articolo sull'argomento https://www.blockapt.com/health-data-from-raiding-to-reselling/
3. https://www.theregister.com/2023/09/14/caesars_mgm_hacks/
4. I trasformatori, o modelli sequenza-sequenza (Seq2seq), sono modelli di Deep Learning che appartengono a una classe speciale di architetture di reti neurali ricorrenti. Sono reti che trasformano una data sequenza di elementi, come la sequenza di parole in una frase, in un'altra sequenza. Vedere https://blent.ai/blog/a/transformers-deep-learning
5. L'elaborazione del linguaggio naturale (NLP) è una branca dell'intelligenza artifi ciale. Si tratta di addestrare i computer a comprendere, elaborare e generare il linguaggio umano. L'NLP si basa su una combinazione di apprendimento automatico e linguistica computazionale. I sistemi vengono addestrati sui testi per imparare a riconoscere le parole e il modo in cui sono messe insieme. Per alimentare i sistemi di ML si utilizzano frasi, estratti di testo o addirittura interi libri. Questi dati di addestramento vengono elaborati e il sistema impara a prevedere il resto del testo identifi cando i modelli. Vedere https://datascientest.com/introduction-au-nlp-natural-language-processing
6. Il riscaldamento dell'indirizzo IP consiste nell'invio progressivo di e-mail, anziché in un unico blocco, ottenendo comunque un alto tasso di coinvolgimento. Questo processo consente di costruire una reputazione positiva del mittente e quindi di aggirare i fi ltri antispam.
7. Una sandbox è una macchina virtuale isolata in cui il codice software potenzialmente pericoloso può essere eseguito senza infl uire sulle risorse di rete o sulle applicazioni locali.
8. https://incyber.org/ia-une-aubaine-pour-ingenierie-sociale/
9. https://mpost.io/fr/data-heists-evolve-how-cybercriminals-are-using-artifi cial-intelligence-to-steal-your-data/
10. https://www.cnet.com/news/privacy/facebook-chief-security-officer-alex-stamos-web-summit-lisbon-hackers/
11. https://nakedsecurity.sophos.com/2016/11/11/facebook-is-buying-up-stolen-passwords-on-the-black-market/
12. Stamboliyska, Rayna (2017), La face cachée d'internet, Larousse.
13. Thibout, C. (2018), " L'intelligence artifi cielle, une géopolitique des fantasmes", Etudes digitales, n°5 - 1.
14. Roberts, H.; Cowls, J.; Morley, J. et al. (2021), "The Chinese approach to artifi cial intelligence: an analysis of policy, ethics, and regulation", AI & Society, n. 36.
15. Wu, F. ; Lu, C. ; Zhu, M. et al. (2020), "Towards a new generation of artifi cial intelligence in China", Nature Machine Intelligence, n°2.
16. Frankopan, P. (2018), Les nouvelles routes de la soie. L'émergence d'un nouveau monde, Flammarion, Champs Histoire.

Post-Quantum Cryptography: Stay Calm. Keep Encrypting. In NIST we Trust.

Marco Essomba

Marco Essomba is the Founder & CTO of BlockAPT – a UK based innovative cybersecurity company. An influential thought leader in cybersecurity with almost 2 decades of working with some of the largest and well known institutions. Marco's passion, expertise and knowledge has culminated in the design of the unique central management, command and control BlockAPT platform which allows businesses to stay ahead of cyber threats 24/7. Marco is often called upon as a panellist at cybersecurity conferences and has been a host ambassador at CyberTalks, one of London's largest cybersecurity events. With 16,000+ followers on LinkedIn, 35,000+ on X(Twitter), Marco has been recognised as Engati's 101 global Twitter influencers to follow. He is sought after for his quick problem-solving approach and helping businesses futureproof their security infrastructure.

Introduction

The potential power of quantum computers to break current encryption algorithms is well documented. The power of quantum computers could bring huge benefits to the way our digital communications are secured today and in the future. At the same time, there is also a huge risk because of the way quantum computers could be used by cybercriminals and various threats actors to break today's classical encryption algorithms and protocols.

Access to practical quantum computers will pose a significant threat to the way we protect data at rest and data in motion. This is because the existing protocols and algorithms that we rely on to protect our digital communications will be at risk against the sheer brute force of quantum computers. This risk is not just limited to our existing digital communications on the Internet but would seriously undermine the confidentiality and integrity of any system relying on existing classical cryptographic algorithms.

But is it time to panic?

Let's start with the basics: what is quantum security?

At the fundamental level, quantum computers rely on quantum mechanics principles to create a computation system that can perform calculations using qubits or quantum bits. Unlike bits used in classical computers which can have a state of one or zero, qubits can exist in multiple states simultaneously, allowing it to perform certain tasks faster than classical computers.

The order of magnitude is significant. For certain types of operations, for example cryptography operations that would take a classical computer years to complete, can be completed in seconds in a quantum computer. It is this tremendous power of quantum computers that poses a significant threat to the way we protect digital communications today, not just on the Internet but to any secure digital communications system.

Let's start with the basics: why do quantum computers pose a threat to our current entire digital security infrastructure?

Today's digital communications rely on encryption to protect data at rest and data in motion against unauthorised access by threat actors.

Encryption relies on complex mathematics to protect sensitive electronic information, including our day to day use on the Internet to access our online banking securely for example. The key assumption is made that current encryption algorithms rely on maths problems that cannot be solved by even the fastest classical computers, ensuring that our digital communications are inaccessible to unwanted third parties or threats actors.

Encryption algorithms provide a mechanism to transform “clear text” into “code” often referred to as cipher. The cipher can only be unlocked, deciphered or decrypted, by a person or a system that has the relevant key.

The key can be a selected number of combined characters that are usually a long complex combination of letters, numbers, and symbols that can be used to encrypt or decrypt a message. Hence, the process of finding a key can be time consuming and complex requiring significant computational operations.

Classical computers are ill suited for these types of computational operations. However, quantum computers have the significant advantage to tackle types of operations because of their ability to perform calculations using qubits or quantum bits. It is this power that renders any classical encryption algorithms at risk against quantum computers.

Stay calm. NIST is on it.

The National Institute of Standards and Technology (NIST) is a global body that is focusing on developing and guiding the brightest minds in cybersecurity around the world to focus on this challenge head on by improving existing standards and by also developing a new set of protocols that will be quantum resistant whilst remaining applicable to protect against classical computers attacks.

Using its global network of cyber security experts, NIST initiated a worldwide competition to research and develop quantum-resistant cryptographic algorithms.

NIST is looking to develop quantum-resistant cryptography systems that will be interoperable to secure both quantum and classical computers without changing the underlying protocols and standards of our existing digital communications infrastructure.

It’s a matter of when. Not if.

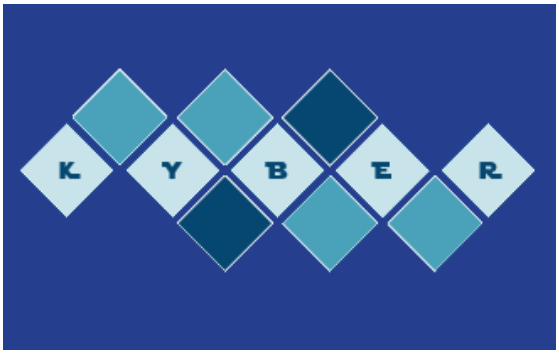
When will a large-scale quantum computer be built and deployed at scale? This is subject to many debates. The recent advancement and breakthroughs in quantum physics have significantly increased the confidence of a physical large scale quantum computer. Some estimate that within ten to twenty years quantum computers will be significantly advanced and accessible to break all public key schemes and algorithms that we currently use to secure our daily digital communications.

If we take into account the transition phase required to upgrade our existing digital communications infrastructure which may take a decade or more to be upgraded, it is clear that we must begin to prepare today.

Stay calm. Keep encrypting.

NIST’s recommendation is clear. Keep encrypting as before following recommended guidelines. Whilst algorithms are being developed and standardisation is currently in progress for one or more quantum-resistant public-key cryptographic and signatures algorithms, the short term solution for organisations is to continue to follow best practices in classical encryption’s methods.

There are several post-quantum software and hardware solutions available today in the market, however, rigorous testing is required before these solutions can be implemented at scale. It will take time before these solutions become the norm.



NIST - Proposed Algorithms

NIST has proposed two main algorithms that can be used for general encryption and digital signatures. The focus of general encryption algorithms is to protect any data in motion travelling through a public network. Digital signatures focus on the identification and authentication of digital transactions.

CRYSTALS-Kyber algorithm was selected because it offers small encryption keys that can be exchanged easily with little overhead whilst providing high speed transactions.

CRYSTALS-Dilithium, FALCON and SPHINCS+ were selected for digital signatures. For high efficiency transactions, CRYSTALS-Dilithium is recommended as the primary algorithm, however, for applications that require much more smallest signatures, FALCON is recommended. As a backup, SPHINCS+ is recommended because it is much larger and slower.

Conclusion:

NIST has made significant progress in the development of one or more algorithms and standards designed to withstand cyber attacks that can be unleashed by quantum computers. This process is ongoing and requires a number of iterations, feedback, and testing before the final algorithms are selected. NIST has proposed four algorithms that can withstand the power of quantum computers. However, as these algorithms are put through their paces in real world digital communications systems, only time will tell how well they can withstand attacks against quantum computers.

Further reading:

Post-Quantum Cryptography: A Q&A With NIST’s Matt Scholl
PAO, ITL Receive 2022 Communicators Award of Distinction for Video Animation
Cryptography
NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers
NIST’s main cryptography page: https://www.nist.gov/cryptography.
Migrating to Post-Quantum Cryptographic Algorithms, https://www.nccoe.nist.gov/projects/building-blocks/post-quantum-cryptography.
Kyber
Falcon
SPHINCS+

BlockAPT™

MicroToken Exchange (MTE®) Technology

The next level quantum-safe or quantum-resistant data protection and secure communication capabilities.

- **FIPS 140-3** conformance tested standard technology
- Security - Deep integration of quantum secure protocols across the full tech stack
- Speed - Ultra fast performance with quantum speed and low latency
- Sustainability - Decrease energy consumption whilst maintaining a sustainable strengthened cybersecurity posture
- Secures data inside the platform with a layered defence
- Fully secured 2-way channel for communications

blockapt.com

In alliance with QDex labs™

In the Spotlight:
Professor Lisa Wilson

Accolades

DUniv., FBCS., FRSA., Grad. Cert Sc., Bch T&D, Dip. T&A Sys., Adv. Dip. OHS, BA (Economics, Geog., Fin. Mgt.) Dip. Ed.
Professor Extraordinaire: Innovation, Digital Technology & EntrepreneurshipManaging Director, XTCC Investments, Tallinn,
Advisor, BondStream - Estonia, UK, Singapore, Dubai
Advisor, Bedford Row Capital - UK, Estonia, Singapore, Dubai
Academic Advisory Board: International Association of Trusted Blockchain Applications [INATBA]
Legal Advisory Council - UK ICC Centre for Digital Trade & Innovation [C4DTI]
Chief Research Officer, Global Foundation for Cyber Studies & Research [Washington DC]
Fellow Royal Society of Arts, Manufacturers and Commerce [FRSA], London UK
Fellow British Computer Society [FBCS], London UK
Adjunct Faculty La Trobe University
Adjunct Faculty SARChI Innovation Research Group [Tshwane University of Technology [South Africa]]
Adjunct Faculty African Post Graduate Academy [APGA]
UK IT Guru Nomination: Most Inspiring Woman in Cyber 2022
UK Security Serious Awards Unsung Hero 2022 Nomination: Education
Top 100 B2B Women Thought Leaders & Influencers in the World to follow in 2020, 2021 & 2022
Top 100 B2B Thought Leaders in the World to follow in 2020, 2021 & 2022
Top 20 Global Thought Leaders & Influencers on Cryptocurrency 2020, 2021 & 2022 - No 8
Top 20 Global Thought Leaders & Influencers on Blockchain 2020, 2021 & 2022 - No 16
Top 50 Global Thought Leaders & Influencers on EdTech 2021
Top 100 Women in Crypto in the World in 2020, 2021 & 2022

Professor Lisa Wilson [Short] is internationally renowned and respected for her track record to design, develop and deploy 'end-to-end' digital technology led ecosystems that are commercially astute, resilient, impact driven, secure, trusted and crucial for global economic development. Her passion to drive digital trust, de-risked innovation, market acceleration and entrepreneurship, that combines the need for education to advance deployment of emergent technologies of blockchain, AI, Metaverse, IoT and others, has positioned Professional Wilson as a preeminent innovator with vast global experience, including inventing several Patents. She has founded and managed multiple cross - jurisdictional companies with significant cutting-edge digital technology for trust, value, and supply chain improvement projects, across different segments, and global markets including UK, APAC, Africa, Singapore, Europe, and UAE.

Currently Professor Wilson is the Managing Director for XTCC Investments who are the pioneer in exchange traded carbon credits, recently unveiling the world's first multi-currency structured investment product for high-quality Voluntary Carbon Credits (VCCs). offering exceptional liquidity across both digital and conventional capital markets.

A passionate advocate for advancing women in tech, entrepreneurship, security for SMEs and mentoring women in the economy, Professor Wilson disrupts the norm and stays at the forefront of pioneering effective positive change, digital trust, and transformation.

Professor Wilson's career is augmented by a lifelong commitment to mentoring others, holding multiple Board appointments, appointments by the EU Commission, INATBA, UN Commission on the Status of Women, pro bono work globally for the industry and the community. A highly respected international, multi-disciplinary academic approach relied upon for risk and research contribution, she has a wealth of accolades, as listed earlier, which are testament to her achievements.

Professor Wilson's latest book authorships, include contributions to Blockchain Impact, Blockchain: A to Z Explained and to many mainstream journals and media publications which highlights her passion for advancing digital technology and ensuring people and business are kept secure, educated, and informed.

Bio

With a distinguished career in education management, training, development, and infrastructure, her achievements have been merited with the development and delivery of the first Accredited VET Qualification and Training Package in Australia, the embedding of WHS skillsets in all Training Packages, and the first Registered Training Organisation to attain 7 Years initial Registration under ASQA with 100% compliance. She is a proud author of the Blockchain: Social Impact Building Block Programme and Resilient Leadership in a 21st Century Digital Economy Programme, a Masters unit in Blockchain Technologies and is also currently contributing to a new Master's in Information Technology for Navitas (42 Campuses), a Master's in Engineering Management: Technology for innovative venture creation at Tshwane University of Technology and many industry leading programmes to advance digital transformation for CFTE.

Professor Wilson's vision has taken her many times to the United Nations and to engage with the Permanent Secretariat of Nobel Peace Laureates. She has twice been honoured with Honorary Doctorates, and with Fellowships from the Royal Society of the Arts, Manufacture and Commerce (FRSA) and British Computer Society (FBCS), in special recognition and privilege for her lifelong dedication, commitment, and sincere efforts to grow business and develop digital technology on the international map, and for her contribution to social, economic, and corporate fields.

The Interview

Raj Meghani (RM) and Prof.Lisa Wilson (PLW)

RM: Hello Professor Lisa. Let's start with what inspired your blockchain career and how your passion for this field has evolved over time?

PLW: My interest in blockchain technologies was inspired by work commenced in the early part of 2012 – I just didn't know it was called blockchain at the time. I was delivering a solution to support a request by the Australian Productivity Commission to find a way to reduce the high turnover rate of staff in the care worker industries that constitute some 12% of the global workforce. At the time, the quality of training being provided to them was low, and their employers and the Registered Training Organisations had little motivation to change.

I architected an autonomous technology ecosystem that was designed to ensure quality in education was high, and where key stakeholders were encouraged by an inbuilt quality mechanism to do the right thing and reward both staff and the clients they were entrusted to serve.

I required my ground-breaking new IT to be 'non-compliance prohibitive'. Put simply, technology that seamlessly and silently stopped business and workforce, including educational organisations, doing the wrong thing, but which guided and aligned them to the correct way. At that time, like many others, I knew nothing about blockchain. By 2016, I knew and had developed this to be a blockchain solution, with many smart contracts and perhaps one of the earliest and still to this day, one of the most amazing use cases for a utility token – purely for quality.

From these early days, I've grown and evolved to know that this technology in the hands of wise people has the incredible capacity to change thinking, the way we conduct business and to improve democratised outcomes for people and business. It's this that drives me.

RM: Blockchain is often described as a disruptive technology. In your view, what are the most disruptive applications of blockchain in the cybersecurity domain?

PLW: Blockchain is the disruptor of the 21st Century. In the broadest terms, it gives us the inherent capacity to be digital and safe in a 'trustless' environment. Not because we can't always trust those we engage with – but because we don't need to! As I have written recently in my Chapter in the book Blockchain Impact "It has for Society 5.0 become the core building block of trust, that has enabled belief in the technology as a 'confidence engine' for inclusion." That means we can have data transparency secure in the knowledge it is immutable and with decentralised gate-keepers dependent on majority agreement. If you think about it, it's like securing every lifetime memory in a glass bottle for prosperity that people can always see and read – if they could hold the bottle and open the lid.

There are many blockchain based solutions and applications available 'as a service' from simply using it as a secure ledger, for back-up and recovery, and distributed filing to the more complex abilities for access key encryption. For me though, the greatest disruption will be re-thinking cybersecurity altogether – from a protective reactive state of 'security' to one that invests in a proactively designed system of 'trust'. The digital world we live in is a pervasive ecosystem and we must think how information flows through that ecosystem. IoT, AI and edge computing are all fruit ripe for the picking by malicious actors trying to access systems with tighter security controls. A blockchain-based Domain Name System (DNS) — the protocol for directing internet traffic — can remove the single point that allows attacks on these ecosystems to succeed.

Applications that provide provenance and protection of user generated data and media whether it be in social media or for legal evidentiary trails, such as MEA Connexus by Issured are changing the way we conduct our lives in this digital world.

RM: With wider blockchain adoption, how can we balance transparency with privacy, especially for sensitive information?

PLW: These two concepts are always seen as being diametrically opposed particularly as transparency is fundamental in blockchain technology's fundamental design. They shouldn't be. There is a difference between confidentiality, privacy and transparency and with Zero Knowledge Proof, discreet transactions, use of private permissioned and consortium blockchains these should no longer be a forefront concern.

They are often still held up as a reason not to use blockchain technologies by those who don't understand what is possible. I like to think of it like driving a car without a seatbelt – we used to do it before we knew any better. Now there's no excuse. There is no logical sense for not using blockchain technologies to ensure information is secure. The issue is always education.

RM: You have been immersed in blockchain for decades now. What excites you most about its future potential?

PLW: Without any doubt in the areas of net zero, user generated content and digital ID.

My work currently at XTCC Investments is only possible through the underpinning benefits of blockchain technologies that provides provenance and confidence to investors that high-quality voluntary carbon credits are exactly that! Attaining a point where carbon emissions are minimised and offset to reverse the current climate crisis will require a vast evidentiary secure supply chain of carbon offsets available from renewable energy sources – blockchain technologies do this. It creates that 'trustless environment' which allows investors to overcome concerns of analogue, fragmented processes and markets fraught with fraud, greenwashing and double counting. What really excites me most though, is that these things are happening now and will continue to evolve at a very rapid

rate and it is again the thinking and people that will ignite these changes. With XTCC – we could never have launched a suite of exchange traded carbon credit investment products without aligning years of knowledge, expertise, the synergy of fintech, regtech and legal tech – and the benefits of a blockchain infrastructure.

Trusted user generated content and a digital ID and the ability for these to transform lives and build new economies of scale - safely will be the big space to watch. Many talk of Web3 as being the exciting part – but I see that as the outcome of digital ID and the ability for users to generate and engage with trusted content and information enabled by the blockchain technologies that are the foundation of Web3. I see blockchain as the horses and Web3 as the cart.

RM: As an educator, how do you envision blockchain transforming approaches to learning and academic management?

PLW: In 2019, I was asked to deliver a presentation to the UK Government about blockchain strategy in education to the All-Party Parliamentary Group on Blockchain. Then I spoke about the fact that as a 21st Century and 4th Industrial Revolution foundational piece of technology, blockchain education was critical. In particular about blockchain technologies, about the use of blockchain solutions within the business of education and about how blockchain technology could transform learning itself and really empower education and academic management. In 2023, I'm sadly still saying the same thing. Education must lead by example – not follow. Every educational institution should be issuing their credentials on a blockchain eliminating huge operational costs, but also providing security and provenance assurance to the economy. They aren't!

Intellectual property from its source can be valorised and monetised using blockchain technologies that are as simple as an application on any smart device by the very institutions who create vast quantities of our knowledge base. They aren't! If they were, learning could drive a new economy where students could value education and lifelong learning and in many places where education is unaffordable – actually earn an income from learning.

Universities also benefit from vast amounts of revenue from research. Through synergy of blockchain and AI the value and delivery timelines of this could be escalated from years to months. What must change is thinking of the thinkers. I write about this extensively in Blockchain Impact and the Chapter Blockchain's missing block in the chain of success. It continues to be a frustration that education and academic management is too slow in the adoption curve for technology that is fundamental to 4.0 and Society 5.0.

RM: If you had a magic wand and could instantly manifest one blockchain cybersecurity solution, what would it be?

PLW: That's easy. Two things – a blockchain enabled DNS security system and the adoption of widespread practice to use blockchain based digital ID as an entry key to access and create digital and social media profiles. The latter is important, because it is now getting harder with more sophisticated deepfake technology, to discern between what's real and what's not. But also, it provides a layer of transparency that people should expect from these large digital platforms to safeguard everyone.

RM: For aspiring cybersecurity students interested in blockchain, what foundational skills and knowledge do you recommend they build first?

PLW: I think students need to understand the actual technology, and why this knowledge drives business decisions and adoption – and of course the potential risks that might exist. This includes understanding the blockchain stack and new blockchain innovation layers and how they connect to adoption choices that might include relative trade-offs between privacy, compliance, speed, scalability and sustainability by choosing a public versus a consortium blockchain model.

Also understanding the differences in languages used to code blockchain might alert future cyber professionals to areas of potential malicious opportunities. It's really about opening their minds to learn as much about blockchain as they do the internet because they are both foundational technologies.

Lastly I would say build knowledge from the perspective of how this technology can support cybersecurity and redesign a more trusted world – rather than from the misinformation that prevails. Go out and seek the information and get answers from those like myself in the industry who focus on the technology, digital assets and other technologies with ethics and integrity designed and embedded as the way forward.

RM: Outside of work, what hobbies or activities refresh your mind so you can come back to blockchain research with new inspiration?

PLW: I turn away from technology altogether and go into my garden or kitchen – often using produce I've taken great delight in growing. I always like to surprise people that despite my 'tech' and 'leader' background, I also have a life outside tech that is important to maintain humanity. I used to have champion gardens in Australia many years ago and whilst that isn't always possible travelling as I do, you can always grow a pot of fresh herbs on your windowsill and feel grounded. My husband says I look at home with a water hose in my hand and dirt under my nails admiring my garden….

Travel, good food, wine and time with my husband and friends and family also refreshes my soul and inspires my mind. Often it is these conversations and serviette documents that become the next brilliant idea.

RM: You must have faced scepticism early on about blockchain. How did you maintain conviction?

PLW: Scepticism and the downright naysayers for many years and still do. I remember a conference only this year when a panellist in London regurgitated a tirade of utter nonsense regarding digital assets and the alleged lack of collaborative regulatory efforts being undertaken globally. The joy I had was following that and having the confidence to remove the 'emotional' nonsense and talk facts. It was a particular revelation because I was actually speaking about my work with the European Commission and EMIR Refit Programme regarding the identification of digital assets from their data meta tags – so that organisations could report to regulatory authorities.

A colleague and friend of mine once said I always engage Lisa on risk management because she'll never say anything she doesn't back up with research. My conviction is easy to hold and strengthen as the technology evolves because I am seeing first-hand the incredible benefits delivered to people, business and nations. On many scales – from the first home my friend could buy as a result of financial freedom to transparency in business and speed in international transfers that have opened the doors to business that could never happen before.

I've also learned from personal experience what this technology could have prevented and that becomes an unyielding determination to continue learning and understanding what this technology can deliver. If I share my experiences and help others – I can overcome the scepticism.

RM: Can you recall an early "aha moment" or breakthrough that got you hooked on blockchain's possibilities? Feel free to geek out on the technical details!

PLW: I've had many "aha moments" but one was during my work with LawTech UK regarding increasing access to dispute resolution for SMEs through smarter legal contracts.

Blockchain is perfectly set up to use consensus mechanisms – the agreement on how data is added to a blockchain – for decentralised dispute resolution for all manner of basic transactions in life. This includes disputes in insurance, payment services and judicial reviews. In these cases, a decentralised mechanism of independent expert nodes can determine outcomes with transparent pragmatism and no bias.

My real 'aha' was that this could be used to determine applications for Visas that are one of the most fragmented, archaic and biased processes that still exist in the world today. Instead of 1 decision maker – you would have an entire decentralised, pseudonymous network basing a decision on information with full transparency. To that I say – bring it on! Can you imagine how much money could be saved if the inefficiency and bias of dispute resolution for the vast majority of simple matters were completed this way - only leaving the complex matters to be decided by the courts and tribunals? It would also shift the power of justice back to the people and enable small businesses to level the playing fields against the more powerful corporations who can afford to fight the system. Currently justice is for the wealthy – not for what is right and wrong. That must and can change with blockchain – and of course relates to one of my own Patents.

RM: With the increasing metaverse advances, I'd love to hear your perspectives on the intersection of blockchain and metaverse development. What role does blockchain play in securing these new immersive virtual reality worlds?

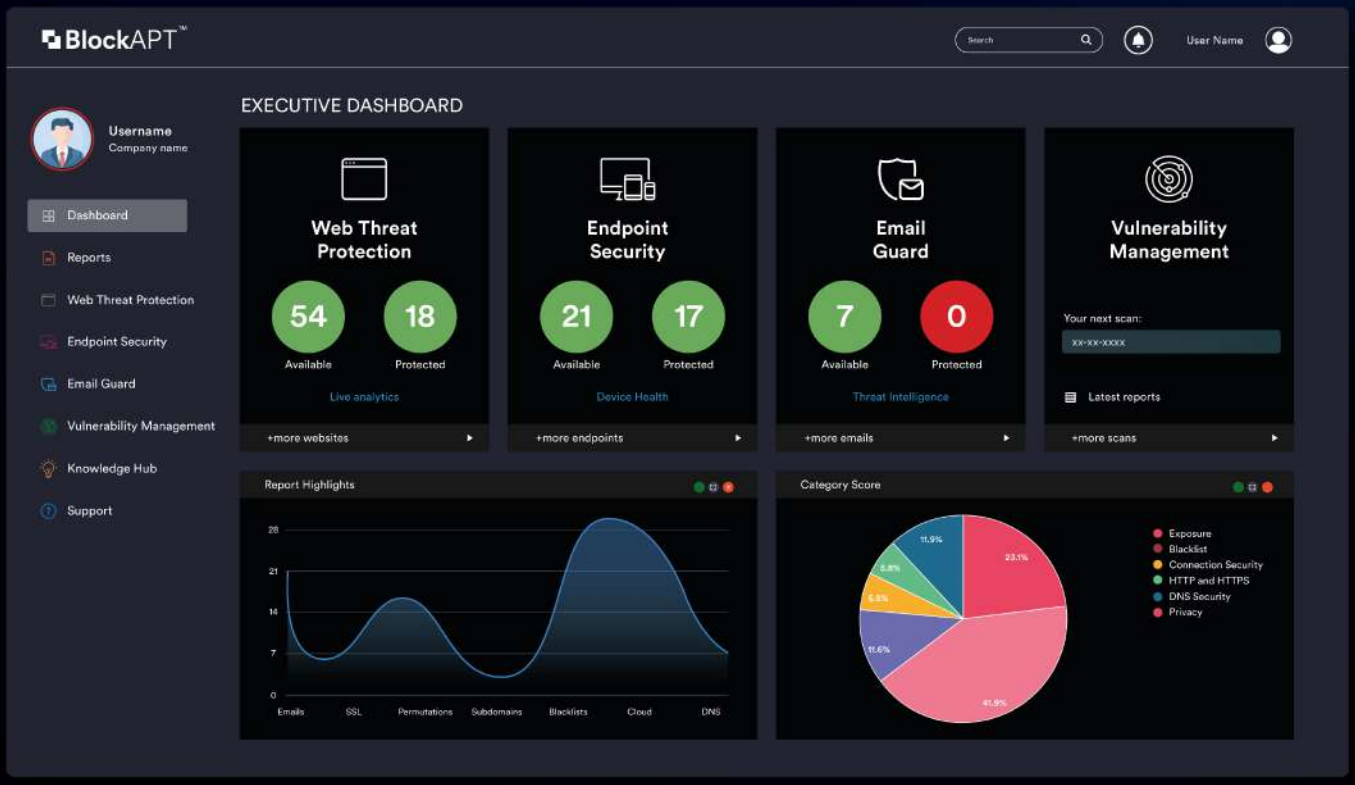
PLW: This is probably the least understood topic about blockchain. Metaverse is a part of Web3 which is built on top of a foundation of blockchain, smart contracts and crypto assets with the principles of decentralisation applying to all user generated data.

People can interact on the web with anyone, anywhere in a ubiquitous, connected, decentralised and immersive 3D digital network. Web2 was an human and social upgrade of Web1 where rather than just seeing and moving information people could engage and contribute user generated content. The Metaverse is another realm of engagement and user generated content where blockchain allows new virtual economies. It's a difficult concept to visualise as it's like a 4D world built on a totally decentralised neural network. So really the role that blockchain plays is similar to the tangible world we live in – our ethics and cybersecurity requirements don't change. However, it does make the need for digital trust and verification even more critical.

BlockAPT™

Executive Dashboard

Customisable executive dashboard for your entire infrastructure with analytics and reporting.



- Strengthening IT and Security Teams
- Supporting Compliance Teams
- Empowering Business Leaders
- Boosting Operational Teams

blockapt.com

The Pertinence of Cybersecurity in Japan's Digital Ecosystem

Tsutomu Yoneyama

Tsutomu Yoneyama (Yonny) has 25+ years of Enterprise and Service Provider Infrastructure Design & Implementation experience and is presently Representative Director at Novias K.K., a strategic company of BOW holdings group providing cybersecurity professional consultancy & managed services with no bias.Yonny's major focus is on facilitating digital transformation (DX) through cybersecurity governance, risk management, business continuity and resiliency consultancy as well as project management and telecommunications & network expertise.

In an age increasingly marked by interconnectedness and reliance on digital platforms, the subject of cybersecurity has never been more salient. The issue takes on a particular gravity in Japan, a nation known for its advanced technology infrastructure. However, this technological prowess also renders the country a high-profile target for cyber adversaries.

Overview of Emerging Cyber Threats and Trends in Japan

Recent findings from Acronis Mid-Year Cyberthreats Report 2023 unveil a disquieting trend—Japan, along with Singapore and Brazil, leads in the number of malware attacks for Q1 2023. Furthermore, a surge in ransomware incidents, recorded by Japan's National Police Agency, witnessed a 58% Year on Year escalation in 2022. Particularly concerning is the paradigm of 'double extortion,' which constitutes 65% of ransomware onslaughts. Even more unsettling is the tendency for these malevolent activities to focus on Small and Medium Enterprises (SMEs) across various sectors. This glaring vulnerability reveals a landscape in which entities, irrespective of their scale or domain, are potential targets.

In Japan, the legality surrounding ransom payments is unequivocal: it equates to financially supporting a criminal syndicate, thereby incurring sanctions. Apart from this, there exists a reputational risk should the transaction become public knowledge. In some instances, payment fails to guarantee data recovery, adding another layer of complication.

In a particularly disconcerting event, the Nagoya Port Unified Terminal System (NUTS) fell prey to a LockBit ransomware attack in July 2023. This was not an isolated incident affecting one organisation but had a domino effect on Japan's broader transport and logistical supply chain, halting container operations for an unsettling 60 hours.

Moreover, Business Email Compromise (BEC) is morphing into a technologically sophisticated criminal enterprise. While linguistic differences once offered a modicum of defense, the dawn of generative Artificial Intelligence and deep-fake technologies now facilitates increasingly credible voice and email spoofing campaigns.

Moreover, advanced persistent threats are evolving with the assimilation of AI and machine learning. Attackers have innovated recruitment methods, enticing internal collaborators with promises of privacy and financial rewards. The IBM Cost of Data Breach Report 2023 reinforces the gravity of data breaches, ranking Japan fifth globally with an average breach cost of $4.52 million.

Challenges and imperatives in Cybersecurity Fortification: A Regulatory and Operational Perspective

The evolving threat landscape requires an equally dynamic defense strategy. However, several impediments exist. The proliferation of cloud computing technologies, while offering numerous benefits, also scatters data across multiple providers. This distribution complicates the exercise of centralised control and oversight, thereby inhibiting swift and coordinated response measures.

Furthermore, the Japanese government has ratcheted up its regulatory framework surrounding data protection and cybersecurity. Enhanced laws mandate immediate reporting of data breaches and impose severe penalties for non-compliance. The scope of these regulations extends to businesses operating outside of Japan but handling Japanese data, thereby adding another layer of complexity to cybersecurity compliance.

Yet, most cyber insurance policies in Japan currently cover only incident response costs, lost profits, and third-party liabilities, while explicitly excluding paid ransoms and funds transferred during BEC scams. As demand for such insurance products rises, so do the qualification criteria, requiring businesses to adopt more sophisticated cyber defense mechanisms and processes.

Human resources remain another bottleneck in cybersecurity defense. The (ISC)2 Cyber Security Workforce Study of 2022 illuminates a stark reality: Japan's pool of cybersecurity professionals is growing, but not at a pace that aligns with the escalating threats. This shortage has tangible operational repercussions. A staggering 53% of organisations confessed that they lack sufficient time for risk assessment and management, leading to vulnerabilities. Additionally, 31% and 20% of organisations reported being unable to adhere to established processes and system setups, respectively.

Counteractive Strategies and Future Outlook: Navigating an Uncertain Digital Terrain

In an environment where no defense mechanism can claim absolute efficacy, a nuanced approach termed "defense in depth" becomes crucial. This layered strategy, which combines multiple defensive mechanisms, is akin to the collective safety features in modern automobiles, such as seat belts, airbags, and anti-lock braking systems. However, the indiscriminate implementation of multiple security tools can also generate "alert fatigue," thereby diminishing the ability to discern legitimate threats from false positives.

Contemporary perimeter-based security designs are inadequate for modern distributed network environments, exacerbating the operational load and amplifying talent scarcity. Given the non-controllability of the attacker's behaviour and the unpredictability of future threats, the focus should be on rapid detection, assessment, and initial responses.

In such a context, where should an organisation direct its resources? One viable strategy lies in the Cybersecurity Mesh Architecture (CSMA), an emerging paradigm that offers streamlined and centralised security management for decentralised digital assets. By reducing manual intervention and employing automated incident response mechanisms, CSMA ensures both effective and efficient threat mitigation. Importantly, it is critical to store response plans and playbooks in a separate environment from the main network to safeguard against their compromise during an attack.

Conclusion: Crafting a Resilient Cybersecurity Posture for Japan

Japan's cybersecurity landscape is a complex tapestry, woven with advanced technologies, sophisticated threats, and evolving regulations. It is no longer sufficient to adopt a static, one-dimensional defence strategy. Rather, the need of the hour is an agile, multi-faceted approach, calibrated continuously in the face of new and emerging threats.

Only through such a comprehensive and forward-looking strategy can Japan hope to secure its digital frontiers and protect its organisational ecosystems from the rising tide of cyber risks. This strategy must synergise technological innovation, regulatory compliance, and human capital to create a resilient defence architecture capable of withstanding the evolving cybersecurity challenges of the 21st century.

Cybersecurity Challenges & Insights in India

Aniket Chavan

Aniket is currently working as a Cyber Incident Handler at Atos Paladion. He also specialises as a Threat Hunter and is a Certified Ethical Hacker. In Aniket's spare time, he is active in Bug Bounty Hunting. Aniket is also the Founder and Organiser of Flutter Mumbai and Flutter India.

The world is increasingly interconnected, and this has led to a rise in global cybersecurity threats. Cybercriminals are constantly developing new and sophisticated methods of attack, and organisations of all sizes are at risk.

India is one of the most digitally connected nations in the world, with over 1.2 billion mobile subscribers. This has made the country a prime target for cybercriminals. In recent years, India has witnessed a significant increase in the number and severity of cyberattacks.

In the first half of 2023, India has witnessed several key cybersecurity incidents, from financial frauds to data breaches. These episodes put the spotlight on the importance of cyberdefense strategies.

Topical Cybersecurity Issues in India

Data breaches: Data breaches have become increasingly common in India, with several high-profile incidents reported in recent years. In one incident, a major data breach hit the Ministry of Health and Family Welfare. A notorious hacking group called Phoenix allegedly breached the Health Management Information System, jeopardising sensitive data across the nation's hospitals.

Ransomware attacks: Ransomware attacks have also emerged as a major threat to Indian organisations. In 2021, the country witnessed a 120% increase in ransomware attacks, with the average ransom demand reaching $1.5 million.

Phishing attacks: Phishing attacks remain one of the most prevalent cyber threats in India. In 2022, over 80% of Indian organisations were targeted by phishing attacks.

Malware attacks: Malware attacks are also on the rise in India, with malware variants such as trojans, viruses, and spyware becoming increasingly sophisticated. In a recent scam, Indian investors were targeted, exploiting the rising popularity of cryptocurrencies. Phony platforms lured unsuspecting investors into parting with over ₹1,000 crore (£10bn), underscoring the need for heightened investor awareness within the crypto space.

Supply chain attacks: Supply chain attacks are another emerging threat to Indian organisations. In 2021, the country witnessed a 150% increase in supply chain attacks.

Cybersecurity Challenges in India

Lack of awareness: Lack of awareness about cybersecurity remains a major challenge in India. Many businesses and individuals are unaware of the latest cyber threats and how to protect themselves from them.

Skilled workforce shortage: India faces a shortage of skilled cybersecurity professionals. This is due to a number of factors, including the low number of cybersecurity graduates and the high demand for cybersecurity skills in the global market.

Outdated infrastructure: Much of India's IT infrastructure is outdated and vulnerable to cyberattacks. This is especially true in government agencies and public sector organisations.

Regulatory framework: India's cybersecurity regulatory framework is still evolving. This makes it difficult for businesses and organisations to comply with all the relevant cybersecurity regulations.

Thematic Insights

The rise of new technologies: The rise of new technologies such as Artificial Intelligence (AI), Machine Learning (ML), and the Internet of Things (IoT) is creating new opportunities for cybercriminals as they use content to craft sophisticated phishing attacks. Cybercriminals use AI-generated content to create persuasive phishing emails and messages, leading to unwary individuals or organisations sharing sensitive information or installing malware. IoT has also proven a fruitful ground for cyberthreats. With India's move towards smart cities, IoT vulnerabilities pose serious security challenges.

The increasing sophistication of cyberattacks: Cyberattacks are becoming increasingly sophisticated, making it difficult for organisations to defend themselves. For instance, ransomware attacks are now targeting critical infrastructure, such as power grids and hospitals. Recent reports show an alarming trend of fake loan apps gaining momentum. These apps exploit gullible users seeking small loans. They access personal data such as contacts and photo galleries, and use the threat of leaking this information as a method to intimidate and exploit users.

The growing threat of state-sponsored cyberattacks: State-sponsored cyberattacks are becoming more common and sophisticated. These attacks are often highly targeted and difficult to detect.

Cybersecurity Trends in India

The increasing adoption of cybersecurity solutions: Indian organisations are increasingly adopting cybersecurity solutions to protect themselves from cyberattacks. This is evident in the growing demand for cybersecurity products and services in the country.

The rise of Managed Security Services: Managed Security Services (MSS) are becoming increasingly popular in India. MSS providers offer a range of cybersecurity services, such as security monitoring, incident response, and threat intelligence. This helps organisations to reduce their cybersecurity costs and improve their security posture.

The growing importance of cybersecurity awareness: Cybersecurity awareness is becoming increasingly important in India. Organisations are investing in cybersecurity awareness programs to educate their employees about the latest cyber threats and how to protect themselves from them.

Cybersecurity challenges and trends vary from country to country, depending on a number of factors, such as the level of digitalisation, the regulatory environment, and the threat landscape.

As the costs associated with cybercrime rise exponentially in India, we will see a shift in the regulatory landscape.

Developed Countries

Developed countries tend to have more mature cybersecurity programs and regulations in place. However, they are also more likely to be targeted by state-sponsored cyberattacks.

Developing Countries

Developing countries are often more vulnerable to cyberattacks due to a lack of awareness, resources, and skilled cybersecurity professionals. However, they are also increasingly adopting cybersecurity solutions and investing in cybersecurity awareness programs.

India in Focus

India is a unique case in terms of cybersecurity.

On the one hand, it is one of the most digitally connected countries in the world, with a rapidly growing internet user base and a thriving startup ecosystem. It is leading global initiatives to encourage international cybersecurity cooperation.

On the other hand, India faces a number of cybersecurity challenges, including a shortage of skilled cybersecurity professionals, outdated infrastructure, and a still-evolving regulatory framework.

The National Cybersecurity Strategy: Shaping the Future of Cyberspace

Kurt Sanger

Kurt Sanger served in the U.S. Marine Corps for over 23 years as a cyber operations attorney, criminal defense counsel and prosecutor, advisor to the Afghan National Army, international law instructor at Marine Corps University and National Defense University, and as a planning officer with U.S. Central Command. He earned a degree in National Security Law from Georgetown University in 2015. From 2014 to 2017, Kurt was General Counsel for U.S. Marine Corps Forces Cyber Command. He served with U.S. Cyber Command from 2017 to 2022, first as the lead attorney for plans, policy, domestic and international partnerships, and legislative affairs, later as lead attorney for operations and intelligence, and finally as the Command's Deputy General Counsel. He retired from the Marine Corps in November 2022. Kurt is Founder and Director of Integrated Cybersecurity Partners, LLC, an information technology and national security consultancy. He is also a cybersecurity board member and advisor for Cowbell Cyber Insurance and Batten Safe Corporation, and a non-resident Senior Associate for the Strategic Technologies Program with the Center for Strategic and International Studies, a Washington, D.C. think tank.

In March this year, the White House released its National Cybersecurity Strategy, updating U.S. policy for the first time since 2018. The strategy's principal function is to guide members of U.S. federal departments and agencies in the implementation of the Biden administration's cybersecurity objectives. These organisations range from the Environmental Protection Agency and Transportation Security Administration, which have responsibility for setting cybersecurity requirements for industries in their sectors, to the Departments of Homeland Security, Defense, and Justice, which are additionally assigned many of the United States' overarching cybersecurity responsibilities.

The strategy's aspiration is to create "… a defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive or private information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences."

Though the strategy's direct influence falls on the U.S. executive branch, it will shape the future of cyberspace and the use of information technology for many other entities. Framed across broad, interdependent interest areas, strategic objectives are categorised under five pillars:

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals.

The strategy is worthy of attention by many more than its intended primary audience, especially the private sector. Below are three critical takeaways found throughout the strategy that highlight the most important developments that will likely affect private sector organisations.

1. Public-Private Partnership on Operational Matters:

The strategy is a distinct step forward from its predecessors. It is not the first U.S. cyber strategy to acknowledge the private sector's importance to cybersecurity, but it is the first that recognises the importance of the private sector as a partner to the U.S. Government rather than a mere contributor. This is perhaps a recognition of private control over most portions of the domain's infrastructure, the software that runs it, and the individuals who use it.

Cyberspace's terrain is redesigned, technically and cognitively, by hundreds of millions of users daily, most of whom are not under the control of or employed by any government. The time for governments to recognise that the domain is governed by forces they need to partner with is past due, but it appears that time has arrived.

The strategy states that facing adversaries, "… will require greater collaboration by public and private sector partners to improve intelligence sharing, execute disruption campaigns at scale, deny adversaries use of U.S-based infrastructure, and thwart global ransomware campaigns."

Many of the discussed practices are already in place, and most are administrative in nature, but the phrase 'execute disruption campaigns' is particularly remarkable. It contemplates asking the private sector to participate in operational activities. While cyberspace operations rarely lead to traditional military operations' most serious consequences, they do require similar levels of focus and dedication to process.

Despite inherent challenges, integration is essential to disrupting criminal and nation-state threat actors because, "The private sector has growing visibility into adversary activity. This body of insight is often broader and more detailed than that of the Federal Government, due in part to the sheer scale of the private sector and its threat hunting operations….". Private sector organisations will need to interface with the U.S. federal government to share information and take actions that support cyberspace operations at the scale and pace required for effective operations.

2. Regulatory Development:

While free market advocates may not admit it, the strategy aptly states that, "market forces alone have not been enough to drive broad adoption of best practices." The absence of regulatory requirements and consequences for failing to meet them has led to software vulnerabilities, under protected information technology systems and the physical components they're attached to – to include critical infrastructure. Regulatory regimes must be leveraged to improve behaviours and practices.

While greater responsibilities and associated costs may be imposed on the private sector, there is nevertheless hope for free marketers. The industry has been invited by the regulators to help develop the relevant rules: "A collaborative process between industry and regulators will produce regulatory requirements that are operationally and commercially viable and will ensure the safe and resilient operation of critical infrastructure."

The strategy acknowledges that not all are well-resourced to implement cybersecurity measures: "Different critical infrastructure sectors have varying capacities to absorb the costs of cybersecurity." The same could be said of all sectors. Hopefully this acknowledgement will lead to appropriate levels of government support as well as proportional accountability measures.

3. Liability for Software Vulnerabilities:

Specific to software development, there is a particular motivation for reform: "To build the secure and resilient future we want, we must shape market forces to place responsibility on those within our digital ecosystem that are best positioned to reduce risk."

In most cases to date, software developers have prioritised functionality over security, asking licensees to hold them harmless in exchange for the use of their products. The strategy states, "We will shift the consequences of poor cybersecurity away from the most vulnerable, making our digital ecosystem more worthy of trust. In this effort, we will not replace or diminish the role of the market, but channel market forces productively toward keeping our country resilient and secure."

The strategy elaborates, "Companies that make software must have the freedom to innovate, but they must also be held liable when they fail to live up to the duty of care they owe consumers, businesses, or critical infrastructure providers. Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software…."

The strategy's consistent references to market forces and regulation reflects the delicate balance between innovation and security that is necessary to create an effective information technology environment.

The private sector, to include international organisations, should look for opportunities to participate in executing the U.S. National Cybersecurity Strategy, as the Biden administration encourages. This is an unprecedented opportunity, and hopefully one that will be emulated by other democracies.

Teamwork between the private and public sectors is essential to securing cyberspace. Now, as enshrined in the strategy, that concept is not only wise, but also policy.

Collaboration is Paramount: Unveiling Geo-specific Threats and Mitigation Strategies.

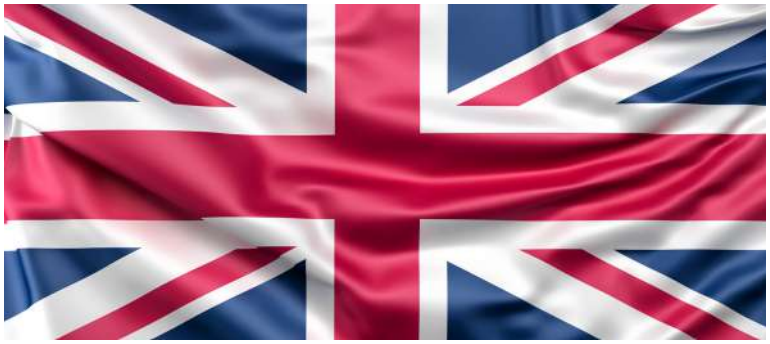
Susan Brown

With over 35 years of distinguished experience and visionary leadership in the financial accounting sector focused on data privacy and cybersecurity, Susan Brown has been instrumental in influencing and driving the 21st Century fight against Digital Humanity theft. As Chairwoman of Zortrex, Susan has passionately steered the company towards excellence, instilling the ethos of "Security First" in all aspects of their operations. Her deep understanding of the complexities of data privacy and security has led Zortrex to adopt data analysis in cybersecurity.Susan's thought leadership and dedication has renowned her as the "First Lady in Data Privacy Security" a testament to her tireless advocacy for privacy rights and robust data protection measures.

In the rapidly evolving realm of cybersecurity, understanding the intricacies of cyber threats is paramount to effective defence strategies. One approach that has proven valuable in this pursuit is geo perspective. By analysing cyber data geographically, security professionals gain critical insights into regional cyber threats, vulnerabilities, and attack patterns.

Embracing geo perspective empowers cybersecurity analysts to discern cyber threats specific to geographic locations or regions. Each area faces distinct challenges influenced by geopolitics, economic factors, and technological infrastructures. By understanding regional cyber threats, organisations can tailor their defence strategies to address localised risks proactively. Moreover, this approach helps international cooperation, encouraging the exchange of threat intelligence and best practices to bolster the collective resilience against cyber adversaries.

Some typical examples to illustrate this point are below:



UK:

Disinformation and privacy continue to cause major concerns. The 2021 Online Safety Bill aims to address harmful content and cyberbullying. Over 1,700 data breaches were reported in the first half of 2022, according to the ICO.

The ICO's 'Data Security Incidents Dashboard' revealed that cyber incidents accounted for 25% of all data breaches in 2022. The report goes on to reveal that there was a 133% increase in large scale attacks compared to the previous year, 2021.

According to Sonic Walls Cyber 2023 report, the United Kingdom occupies the second position (behind the US) for the highest volume of malware attacks, reporting 432.9 million attacks in 2022.

US:

Cybercrime and election interference are amongst the top priorities. The 2020 US Presidential election faced renewed cyber risks according to the CNAS think tank. The FBI reported 2,084 ransomware attacks in 2021, costing over $16 billion. But in 2022, the FBI reported Phishing attacks as the number one cybercrime with total losses due to phishing attacks exceeding $10.3 billion.

However, according to the July 2023 Black Fog Ransomware report, exfiltration continues to be the primary weapon of choice for attacks. Leveraging data for extortion contributes to that quarter's all-time record, with an average pay out of $740,144. China continues to be the main destination for data loss at 41% with Russia at 9%.

India:

Securing digital payments and avoiding identity theft are urgent issues. Per the Data Security Council of India, 44% of Indian organisations faced a data breach or cyberattack in 2021. The Personal Data Protection Bill seeks to safeguard individual privacy.

Fast forward to 2023, and India comes third on the list (behind US and UK) for the highest volume of malware attacks, totalling 335.4 million, showcasing a noteworthy increase of +31% Year On Year.

Australia:

Combating ransomware and data breaches appears to be key focus areas. The 2022 ACSC Annual Cyber Threat Report highlighted ransomware as the most disruptive threat. Optus and Medibank breaches impacted millions of Australians in 2022.

Sharing different geo cyber threats, trends, insights remain paramount to joining together in a public-private collaboration to tackle the global fight against the hackers.

Sadly, this is not as easy as it seems with different geo political agendas for cyberwarfare data. There have been almost 500 documented geopolitical cyber-attacks worldwide since 2009 making cyberwarfare a major technological threat to nations and their citizens. Between 2009 and 2018, there was a 440% increase in global cyberwarfare attacks - 30% originated in China or Russia.

In contrast, countries like Singapore focus on protecting critical infrastructure from cyber threats (GovTech, 2022). South Korea is battling digital sex crimes and personal data leaks (Do, 2022).

Hotspot detection:

Analysing cyber incidents from a geographical standpoint uncovers hotspots of cyber activity, where certain regions experience higher cybercrime rates or targeted attacks. Finding these hotspots is instrumental in deploying targeted security measures to fortify vulnerable sectors. Organisations can prioritise resources to safeguard critical infrastructures, sensitive data repositories, and vital digital assets in regions more susceptible to cyber threats.

Attribution and investigation:

Geo perspective plays a vital and pivotal role in attributing cyberattacks to specific threat actors or nation-states. By examining cyber incidents through a geopolitical lens, analysts can gain valuable insights into the motivations and intentions behind the attacks. Such information is essential for effective incident response and investigation, enables prompt mitigation by organisations and appropriate diplomatic strategies by governments.

Geopolitical influence:

The impact of cyberattacks often extends beyond technical consequences and delves into the realm of geopolitics. State-sponsored actors are increasingly involved in cyber espionage, cyber warfare, and cyber influence operations. Adopting geo perspective helps cybersecurity professionals understand the broader geopolitical context, enabling organisations and governments to formulate the right diplomatic responses and strategies to limit further escalations.

Collaborative defence measures:

Incorporating geo perspective in cybersecurity strategies fosters a culture of international collaboration and information sharing. Recognising that cyber threats are borderless, the global community can work together to protect the digital ecosystem for the mutual benefit of all. It encourages the establishment of international norms and standards for responsible behaviour in cyberspace, promoting cybersecurity as a shared commitment among nations.

The role of emerging technologies:

As cybersecurity continues to evolve, the adoption of emerging technologies plays a vital role in bolstering defences and enhancing the efficiency of geo perspective. Artificial intelligence and machine learning algorithms can process vast amounts of cyber data, allowing for real-time threat analysis and initiative-taking defence measures. Additionally, blockchain technology can offer secure data storage and decentralised threat intelligence sharing, further enhancing collaboration among cybersecurity stakeholders.

Educating the next generation:

To ensure a sustainable and resilient cybersecurity ecosystem, there must be a strong emphasis on educating the next generation of cybersecurity professionals.

Promoting cybersecurity awareness, ethical hacking practices, and responsible data handling from an early age can cultivate a skilled workforce capable of addressing region-specific cyber threats effectively.

Adopting a geo perspective provides a holistic view of threats while uncovering region-specific risks. Examining cybersecurity geographically allows tailored defences and enables hotspot detection, attribution, and understanding geopolitical implications. This fosters international cooperation for mutual benefit against borderless threats.

As Kofi Annan once wisely stated, "*We must unite against common threats and harness common opportunities.*" In the borderless realm of cyberspace, we must come together through a shared understanding that geographical differences influence region-specific dangers. Only then can we build collaborative defences, attribute threats more effectively, and grasp the geopolitical context.

Geo perspective and emerging technologies, along with education, are critical to safeguarding our digital future. United by geography and driven by technology, we can build a safer cyber ecosystem. For in the words of Helen Keller, "Alone we can do so little; together we can do so much." Our cooperation determines our resilience.

Let us embrace geo perspective, forge international collaboration, develop innovative solutions and empower future generations. This multi-faceted approach represents our best chance to meet the challenges of tomorrow and secure the promise of a safe cyberspace.

The task ahead is not easy, but united with shared understanding and common purpose, we can and will safeguard our interconnected world.

Aesop puts it best - *"United we stand, divided we fall."*

Building a Cybersecurity Culture: 7 Key Strategies for your Organisation

Raj Meghani

Internationally recognised thought leader and cybersecurity influencer, Raj Meghani is the Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25+ years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. She's esteemed as a successful brand builder and a business growth hacker. Her unique expertise in scaling start-ups and disrupting markets with new tech has earned her recognition as a "One in a Million" female founder by The Entrepreneur's Network and placed her in the Top 44 "Cyber Power Women" by Top Cyber News Magazine. Raj is also Non-Executive Director on the Board of Money Matters Community Bank.

Cyber threats are growing every day, with damaging data breaches making headlines repeatedly. No organisation or individual is immune.

It's a subject close to my heart - I'm a strong believer that to embed a cybersecurity culture and cement cyber reilience, technical controls alone won't do the trick. It starts with the right mindset and that means embedding cybersecurity into the DNA or fabric of every business. It's not just the responsibility of the IT department but everyone in the business has a role to play with clear responsibilities. That's why building a robust cybersecurity culture is critical for every business.

So, I ask myself, what exactly does a strong cybersecurity culture look like? It starts from the top, with engaged leadership setting the tone and prioritising security. Employees at all levels are trained on cyber hygiene, risks and their responsibilities. Security awareness becomes ingrained into everyday operations as BAU not a one off, induction tick box training exercise.

Crafting this culture (and it's not as easy as it seems) requires strategic focus in several key areas:

1. Establish clear security policies and procedures.

- Document required security practices, including policies and procedures, on everything from strong passwords, device usage and management and phishing responses to more.
- Review policies regularly or annually at a minimum and update them to reflect new threats and practices as needed.

2. Train employees continuously.

- Conduct cybersecurity training upon hiring with quarterly updates – share latest breaches via internal newsletters, intranets, etc to raise awareness.
- Ensure training is tailored to different roles in your organisation (e.g., Executives, Managers, End Users, etc) and focuses on cybersecurity 'champions' to get employee engagement rates up.
- Use real-life examples and simulated phishing tests to illustrate threats.

3. Incentivise vigilance.

- Recognise and 'reward' employees who spot suspicious activity or potentially risky behaviours. It doesn't have to be costly – public recognition via 'shout outs' and gift cards can go a long way – it's the thought that counts.
- Publicise internally "caught in the act" stories of those individuals who have prevented attacks to motivate participation – introduce "Security employee of the month/quarter" announcements.

4. Embed security into operations.

- Include security reviews in product development, vendor evaluations, acquisitions, etc.
- Make security a standing agenda item in meetings and strategy sessions – in other words it's not bundled into "AOB"….!
- Routine security discussions keep it top of mind.

5. Promote open communication.

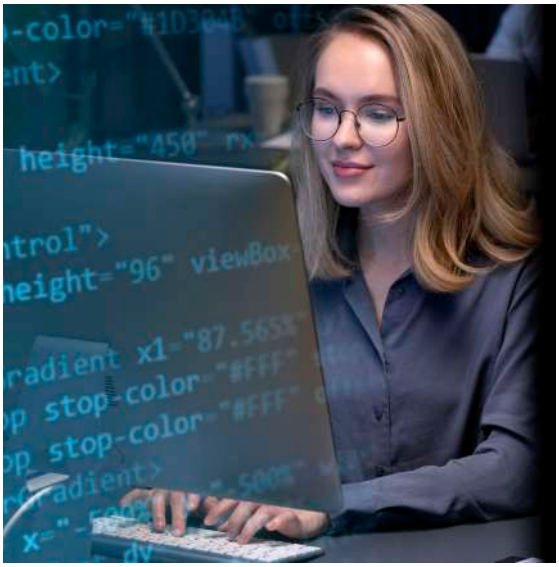
- Maintain an open-door policy for reporting concerns – no matter how trivial they may seem. Discourage a blame culture where individuals are made to feel as 'troublemakers'.
- Encourage discussions about close calls to foster learning from near misses or possible missteps so everyone can learn from them.

6. Lead by example.

- Executives and Managers must model security behaviour and best practices first and foremost. It sets the standard for the entire organisation – lead by example.
- Convey leadership as brand ambassadors in ongoing awareness campaigns

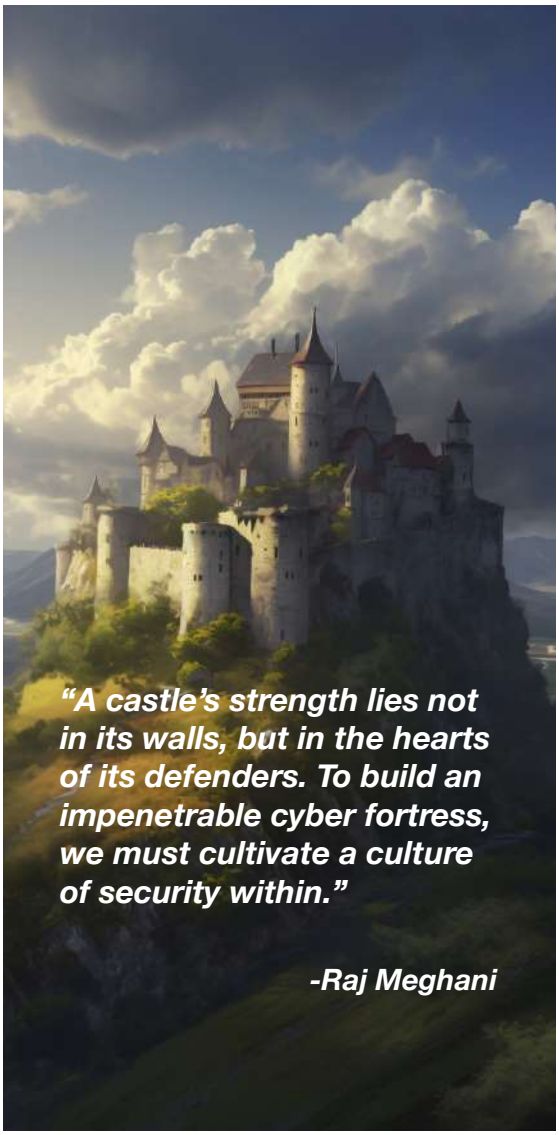
7. Learn from incidents.

- Analyse any breaches or near misses to identify defences and process improvements.
- Deploy cybersecurity solutions and a cybersecurity mesh architecture which gives you a unified, customisable view and control across your entire digital ecosystem with Executive level dashboards for regular reporting.
- Conduct periodic after-action reviews of security incidents are key as is ensuring the ongoing enhancement of your organisation's cyber defence strategy.



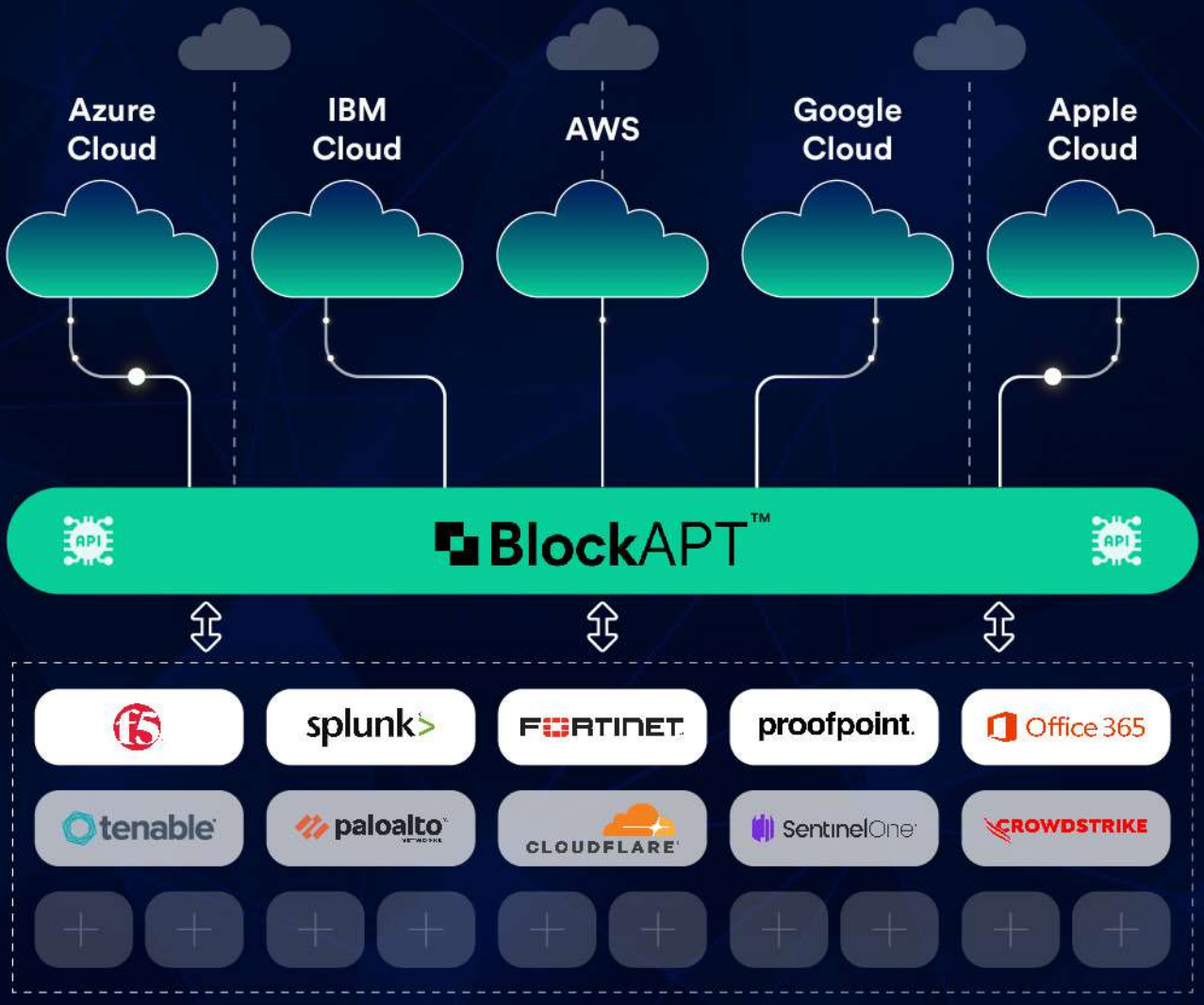
With constant focus and engagement at all levels, security culture can take root. It becomes just *"the way we do business here"* and you can transform your security efforts into an ingrained culture.

Cybersecurity becomes intrinsic to daily operations – the way business is done…..not waiting for the 'if we get attacked' but preparing proactively for 'when you do get attacked'. That's your organisation's best cyber defence.



BlockAPT™

Centralised Cloud Management & Native Control



- Seamless Orchestration
- Optimise your Cost & Efficiency
- Automated Config Management

blockapt.com

Securing the Supply Chain of Trust: Mitigating Third-Party Risks

Chani Simms

Chani is an multi award-winning cybersecurity leader and a passionate entrepreneur serving her clients as C-level advisor, vCISO, ISO27001 and IASME auditor, Cyber Essentials assessor and specialist in helping organisations to implement and manage information security and data protection programs. Has been an information technology professional for over 19 years. Chani co-founding Meta Defence Labs in 2015, an award-winning boutique information security service provider and an UK NCSC Assured Solutions Provider / Authorised Certification Body for the Cyber Essentials Scheme in the UK She also founded SHe CISO Exec. give back platform in cybersecurity, leadership and empowerment. Consists of free five-day Boot Camp, meetups and monthly mentoring platform (www.shecisoexec.org). Chani's own experience in the industry and her passion for the InfoSec industry led her to create the SHe CISO Exec. platform that is on a mission to bridging the gaps in cybersecurity industry by empowering a diverse talent pool of emotionally intelligent cybersecurity leaders.

If you are an IT security professional like me, then typically the first thing that will come to mind when you hear Chain of Trust, will be digital certificates and their hierarchy of trust established by Certificate Authorities (CAs).

We use digital certificates every day in our daily online activities. This chain of trust ensures that users can trust the authenticity of websites and digital identities online. The chain of trust for digital certificates involves a sequence of certificates that ultimately leads back to a trusted root certificate. Web browsers and operating systems have a pre-installed set of root certificates from globally recognised CAs. When a website presents its digital certificate to a user's browser, the browser checks whether the certificate was issued by a trusted CA. If the certificate was issued by a trusted CA, the browser trusts it and establishes a secure connection.

But it does not stop there… The "Chain of Trust" is a concept used in various contexts, in each context, it refers to a different but related concept. Chain of trust in supply chain management is one area that I want to dive into.

In supply chain management, the Chain of Trust refers to the establishment of trust and accountability among various entities within a supply chain network. It involves creating a transparent and secure network where all participants can trust one another's actions and data.

This concept is especially important in global supply chains, where goods and services pass-through multiple organisations, including suppliers, manufacturers, distributors, and retailers.

A Chain of Trust in supply chain management includes practices such as due diligence in selecting reliable suppliers, implementing robust contracts, monitoring supplier performance, and creating contingency plans to mitigate risks.

A well-established Chain of Trust in supply chain management helps organisations minimise disruptions, ensure product quality, and maintain the security of their supply networks.

What kind of risks can compromise the assurance that a link or entity in the supply chain can no longer be trusted to perform its role without compromising the security, integrity, or quality of the products or services being delivered?

- **Data Breaches** in the supply chain can expose sensitive information, risking data breaches and loss of confidential data. This is something that we hear about more often these days.
- **Counterfeit Products** can harm consumers, damage brand reputation, and trigger product recalls if any supply chain link is compromised.
- **Supplier Reliability** is crucial; disruptions like bankruptcy or quality issues can disrupt the entire supply chain.
- **Regulatory Compliance** failures in the supply chain can lead to legal penalties, fines, and reputational damage.
- **Environmental and Ethical Concerns** can lead to reputational damage and legal consequences if ethical and sustainability standards are not met.
- **Geopolitical Risks** affect supply chains spanning multiple countries due to tensions, trade disputes, tariffs, and international issues.
- **Natural Disasters and Disruptions** can disrupt the supply chain by affecting production, transportation, and distribution.
- **Quality Control** challenges can lead to product quality variations if not enforced at every supply chain stage.
- **Single Points of Failure** arise from an over-reliance on a single or limited number of suppliers for critical components or materials.
- **Cyberattacks** on any supply chain link can spread threats like phishing, malware, or ransomware throughout the network.

The Chain of Trust is a fundamental concept for ensuring security, reliability, and transparency in complex systems and networks. In today's interconnected and globalised business landscape, organisations rely extensively on third-party suppliers and a complex web of supply chain partners to deliver products and services efficiently. While this interconnectedness brings numerous benefits, it also exposes businesses to a heightened level of risk, making it crucial to establish a robust "Chain of Trust."

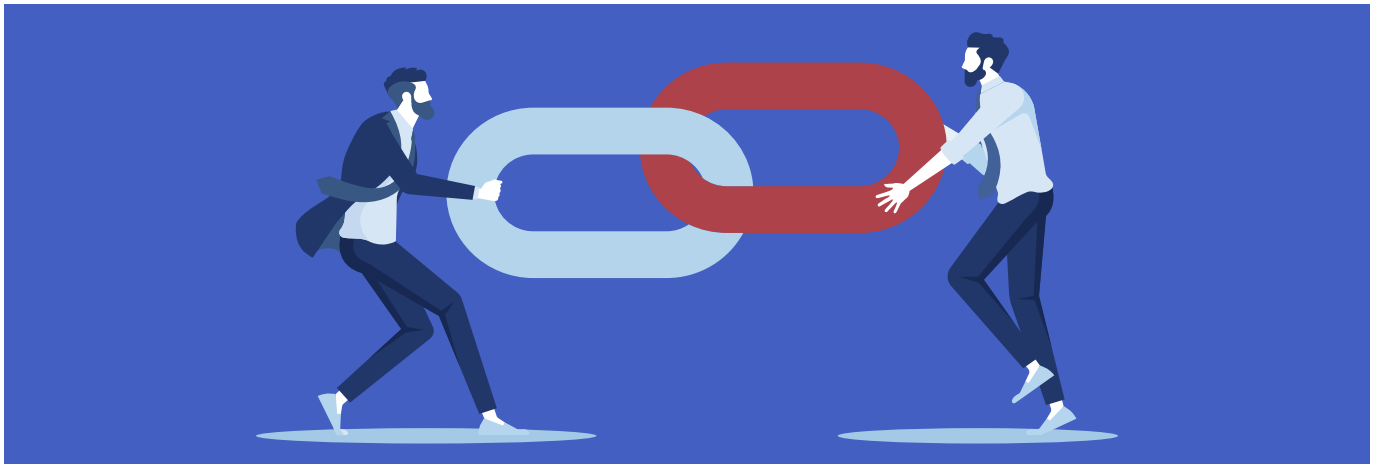
What kind of strategies can we use to mitigate supply chain and third-party supplier risks effectively?

As business owners, the first step is to comprehend the risks. Without a clear understanding of the risks our business faces, we will not be able to effectively protect against them. Organisations need to establish a secure and reliable network of suppliers and partners, minimising risks while ensuring business continuity. It involves creating a culture of transparency, accountability, and collaboration among all supply chain participants.

Some of the key elements of a Chain of Trust include:

- **Due Diligence:** Thoroughly vetting and assessing potential suppliers and partners before engagement.
- **Contractual Agreements:** Implementing robust contracts with clear Service Level Agreements (SLAs) and compliance standards.
- **Continuous Monitoring:** Regularly evaluating supplier performance and adherence to security and compliance standards throughout the partnership.
- **Contingency Planning:** Developing strategies to mitigate disruptions and vulnerabilities within the supply chain.

Here are the measures and practices I encourage my clients to put in place to safeguard the digital components and information within the supply chain. It involves ensuring the confidentiality, integrity, and availability of data, systems, and communication channels at every stage of the supply chain, from suppliers to manufacturers to distributors and beyond.



Here is an explanation of key aspects of cybersecurity in the Chain of Trust supply chain management:

1. Regularly assess the supply chain for vulnerabilities and create risk mitigation plans.

- Conduct regular supplier audits to ensure adherence to security and quality standards. Establish a culture of continuous improvement.

2. Enforce stringent cybersecurity measures, including data encryption and access controls, to protect sensitive information. If you are a business in the UK, make sure your suppliers have Cyber Essentials PLUS as a minimum cybersecurity qualification to demonstrate basic IT hygiene;

- Ensuring the security of all endpoints (devices connected to the network) is crucial.

- Implementing firewalls, intrusion detection systems, and regular network monitoring helps safeguard communication channels against cyber threats like malware, phishing attacks, and unauthorised access.

- Employing robust authentication and authorisation mechanisms ensures that only authorised personnel can access critical systems and data, reducing the risk of unauthorised activities.

- Ensuring that all software used within the supply chain is secure and up-to-date helps protect against known vulnerabilities. Regularly applying patches and updates is crucial.

3. Employees should be educated about cybersecurity best practices, constantly trained, and tested to recognise and respond to potential threats, such as phishing attempts. This should not be old school annual training anymore. I test my teams on a daily basis.

4. Protecting sensitive data, such as customer information, proprietary designs, and financial records, is paramount. Encryption, access controls, and data loss prevention tools are used to prevent unauthorised access, leakage, or theft of data.

5. Having a well-defined incident response plan in place helps in the rapid detection and mitigation of cyber threats. It includes procedures for reporting incidents, containing the damage, and recovering affected systems.

6. Continuous monitoring of the supply chain's cybersecurity posture helps identify emerging threats and vulnerabilities, allowing for timely mitigation.

7. Diversified Sourcing by avoiding over-reliance on a single supplier.

8. Foster transparent open communication and collaboration with suppliers to identify potential risks and implement proactive solutions.

A robust Chain of Trust is paramount in today's supply chain landscape. By establishing a culture of trust, accountability, and collaboration among supply chain participants, organisations can effectively mitigate risks, enhance business resilience, and maintain a competitive edge.

In an era of increasing supply chain complexity, embracing the concept of a Chain of Trust is not just an option; it is a necessity for sustained success in the global marketplace.

Increasing Visibility is Key for Fighting the Emerging Threats

Nicola Sotira

Head of CERT at Poste Italiane Group, Nicola has been working in the field of IT and network security for over twenty years, with experience gained in international environments. The contexts he has dealt with cover cryptography, infrastructure security, but also mobile networks and 3G. He has collaborated with several IT magazines as a journalist, contributing to the dissemination of knowledge related to security and its technical and legal aspects. Member of the Association for Computing Machinery (ACM) since 2004, Nicola has collaborated with several start-ups in Italy and abroad. In this field, he has participated with several companies in the design and development of mobile services; he is co-editor of the Italian version of Cybersecurity Trends (www.cybertrends.it) and has been on the board of the Global Cyber Security Foundation (GCSEC).

We are witnessing an ever-evolving scenario in digital, but one that has at its base a world that is becoming increasingly interconnected, thus changing the risk posture of even items that previously did not foresee a networked scenario. In this context, cybersecurity has become a significant concern for individuals, businesses, and governments. Cyber threats, unfortunately, have evolved and intensified over the past few years, making it essential to take effective and innovative measures to protect our data, identities, and the systems that host them.

The advent of the COVID-19 pandemic has set the stage for significant changes in many areas, including cybersecurity. With the accelerated adoption of cloud computing, COVID-19 has redefined cyber scenarios and posed new challenges for protecting data and information systems. With the increased remote work and forced digitisation of daily activities, organisations have faced new vulnerabilities and threats. In addition, cloud computing has emerged as an essential response to the need for connectivity, flexibility, and scalability during the pandemic. The cloud has provided new opportunities for work and collaboration, enabling organisations to operate effectively even in times of crisis. However, migrating to the cloud requires the right security measures to protect sensitive data.

The cybersecurity landscape is constantly evolving, and the combination of the scenarios created post-COVID-19 and cloud computing combined with the ongoing digital transformation process requires the development of new strategies to protect our networks, data, and identities in an increasingly interconnected and digital world.

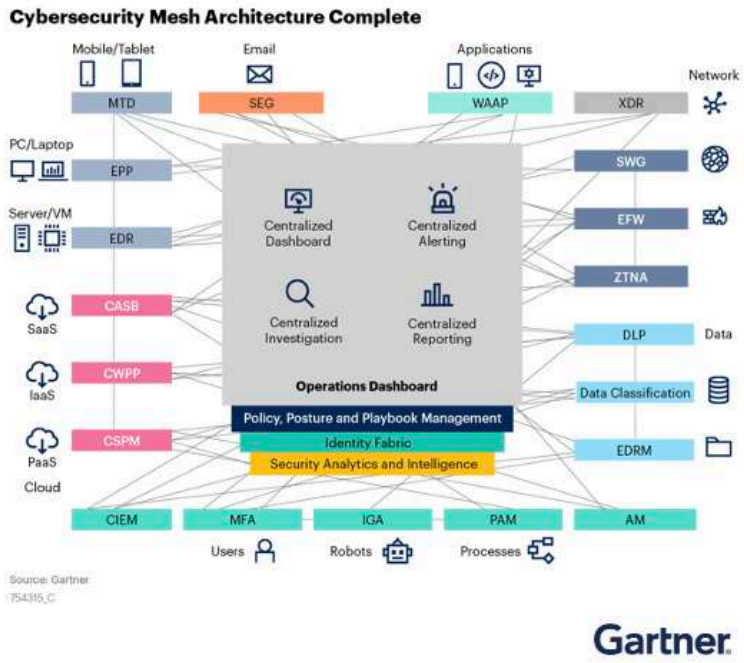
All these situations teach us how important it is to be agile and flexible. The complexity of threats has intensified, and the areas of vulnerability have expanded. These challenges have emerged because of the accelerating cloud transformation and the dissolution of traditional boundaries of enterprise networks and distributed workforce. As a result, there is growing interest in security strategies emphasising security controls covering a wide range of resources, including multicloud ecosystems.

The adoption of multicloud and remote working has dramatically increased the complexity of cybersecurity. Most organisations today turn to different cloud providers offering service models such as IaaS, SaaS, and PaaS. In addition, individual applications often span multiple cloud service models provided by various providers. The fragmentation of technology ecosystems has further worsened with the growth of cloud computing and the decentralisation of the workforce. Currently, employees are distributed everywhere, leading to increased demand for distributed technologies and the adoption of SaaS services.

The security needs emerging in this new situation are not answered by traditional architectures and strategies; a new approach is needed. This is where Cybersecurity Mesh Architecture (CSMA) comes in to minimise the need for a specific IT environment.

CSMA the Gartner definition.

The term "cybersecurity mesh" was coined by analyst firm Gartner, which called CSMA one of the key strategic technology trends in 2022. Gartner defines cybersecurity mesh architecture as a "common, broad, and unified approach that extends security beyond the enterprise perimeters." According to Gartner, CSMA focuses on composability, scalability, and interoperability to create a collaborative ecosystem of security tools.



What is the Cybersecurity Mesh Architecture (CSMA)?

As mentioned, the Cybersecurity Mesh Architecture (CSMA) is a security architecture idea proposed by Gartner. CSMA's distributed architectural approach aims to provide scalable, flexible, and reliable cybersecurity control. This architecture provides a fundamental base layer that facilitates a dynamic security environment, enabling different security services to operate synergistically. CSMA's core approach focuses on security modularity, where each tool is carefully integrated into a larger framework. The CSMA presents a collaborative approach for distributed security services, thus providing increased power to achieve greater security cohesion with fewer resources. To achieve this goal, CSMA takes a unique path by configuring and managing four core layers for distinct security services.

Security analytics and intelligence:

The first level focuses primarily on the collection and analysis of security data provided by various security tools within a company's security ecosystem.

Distributed identity fabric:

This layer prepares and provides the security framework with decentralised directory services that are fundamental to a zero-trust model. These include adaptive access, identity proofing, decentralised and user rights management.

Consolidated policy and posture management:

This layer aids in the configuration of individual security tools by translating a central policy into native configuration constructs.

Consolidated dashboards:

Integrating disconnected security tools often requires switching between multiple dashboards, hindering operations. This layer provides an effective single-panel dashboard to view and manage an organisation's entire security ecosystem.

How to implement a Cybersecurity Mesh architecture?

Although Cybersecurity Mesh is a Gartner concept, specific steps can protect an organisation's critical access points and help create a more connected, tight-knit security infrastructure network. These steps include:

Interoperability should be a top priority when choosing security solutions for your cybersecurity infrastructure. Invest in creating an integrated framework of compatible security tools to achieve a more synergistic effect.

Choose tools that work as part of a larger framework rather than as independent silos. Priority should be given to vendors with an open policy framework that allows policy decisions to be made outside of the tool.

Provide resource access authorisation only to authorised users, overseeing each request to detect malicious activity.

Select vendors with a proven track record of adapting to the latest security standards latest and able to adapt readily to any new changes.

The transition from traditional VPN services to reliable and secure network access based on zero-trust technology, integrated with an access management tool.

Define KPIs and monitor them.

This is the only way to ensure the CSMA works well together and produces the expected results. The organisation must identify the essential metrics to track and report, considering that there may be multiple KPIs to address. For example, a CISO may want to register specific KPIs at the board level to demonstrate that the CSMA strategy impacts business outcomes. At the same time, individual teams will need to measure separate KPIs to assess overall security posture and cyber resilience.

Final thoughts.

Cybersecurity Mesh is a new cyber defense strategy. As explained earlier, the Cybersecurity Mesh Architecture (CSMA) includes four layers to configure and manage distinct security services: security analytics and intelligence, Distributed identity fabric, Consolidated policy and posture management, and Consolidated dashboards. Gartner predicts that by 2024, organisations adopting a cybersecurity mesh architecture will reduce the financial impact of individual security incidents by an average of 90 percent.

Busting the Biggest Myths of Supply Chain Cyber Risk

Raj Meghani

Internationally recognised thought leader and cybersecurity influencer, Raj Meghani is the Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25+ years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. She's esteemed as a successful brand builder and a business growth hacker. Her unique expertise in scaling start-ups and disrupting markets with new tech has earned her recognition as a "One in a Million" female founder by The Entrepreneur's Network and placed her in the Top 44 "Cyber Power Women" by Top Cyber News Magazine. Raj is also Non-Executive Director on the Board of Money Matters Community Bank.

Modern enterprises operate complex, interconnected supply chains and third-party networks full of security blind spots. High profile breaches like SolarWinds and Kaseya underscore the major risks that exist outside the firewall.

Yet myths and misconceptions regarding supply chain cybersecurity are still floating around. So I'm delving into examining the top 10 common ones – not an exhaustive list or in any priority order.

Myth 1: We can fully protect our ecosystem with vendor due diligence.

Reality: Vendor security reviews provide a false sense of safety. Questionnaires offer just a snapshot of controls and compliance. Hackers exploit the smallest vulnerabilities and constantly change attack vectors. No due diligence process provides full visibility across extended networks - unless it's real-time and truly unified across the entire digital ecosystem with built in capability to seamlessly and quickly see the external digital footprint of the supplier and its existing vulnerabilities.

"Check-the-box security assessments give incomplete risk insights," notes Gartner analyst Roberta Witty. "Partner ecosystems are too large and fast-moving to capture with traditional reviews."

Myth 2: Securing our own environment is sufficient.

Reality: Hackers actively target supply chains to breach downstream customers. For example, the infamous NotPetya attack that crippled Maersk started with compromised accounting software. A vulnerability anywhere in an ecosystem can lead to catastrophic effects for all parties.

"With interconnectivity soaring, organisations cannot focus purely inside their four walls," says Pete Cooper, Principal Analyst at Omdia. "Supply chain cyber risk management requires looking beyond just your owned assets."

Myth 3: Third parties won't share enough info for proper diligence.

Reality: Transparency limitations do exist, but maturing regulations and standards are making third parties more forthcoming. For example, CMMC drives accountability down the US defence supply chain. In the UK, guidance like the HMG Supplier Standard helps align expectations.

"The paradigm is shifting. As cyber supply chain management matures, third parties understand the need for appropriate transparency to build trust," says Kishore Rao, Head of Cyber Practice at Tata Consultancy Services. "Proactively communicate your security posture and requirements."

Myth 4: Our industry has less supply chain cyber risk.

Reality: Every industry is vulnerable, with attackers seeking targets in finance, healthcare, retail, government, and more. Data breaches are on the increase - in a number of different forms. No sector is immune.

"Supply chain cyber risk is ubiquitous across industries. Defence in depth is mandatory regardless of your sector." - Amit Yoran, CEO at Tenable

Myth 5: We can fully assess risks through contractual terms.

Reality: While legal contracts are useful, they have limited utility in stopping attacks. Hackers don't check contracts before breaching suppliers with weak defences. Enforceable contracts lag the pace of emerging threats.

"Contracts provide guidelines but zero guarantees of supplier security. Vigilance must go beyond the written page."- Chris Wysopal, CTO at Veracode

Myth 6: Our customers don't really care about our supply chain security.

Reality: Customers, regulators, and partners increasingly scrutinise the cyber risk management of suppliers. New laws also mandate diligence of vendors before sharing data. Don't be fooled - robust supply chain security is now a competitive differentiator.

"Build trust with customers by transparently showing your supply chain security measures, don't just claim it." - Laura Koetzle, VP at Forrester

Myth 7: This is solely an IT problem to address.

Reality: Managing supply chain cyber risk requires coordination across security, procurement, legal, IT, and executive leadership. Holistic governance and cross-functional collaboration is key - there is no room for a blame culture.

"Making supply chains cyber resilient requires breaking down silos and bridging cross functional teams." - Edwin van Schalkwyk, Partner at EY.

Myth 8: We can just avoid high-risk suppliers.

Reality: In today's interconnected business ecosystem, no company can fully avoid dependencies on third-parties, even higher-risk small businesses. The focus should be risk management not risk avoidance.

"With today's complex supplier networks, you can't eliminate third-party cyber risks - you must manage them." - Sandy Carielli, Director at RSA Security

Myth 9: Our people won't click malicious links from suppliers.

Reality: Employees let their guard down with partners. Social engineering like vendor impersonation persuades staff to click risky links. Robust security awareness is essential across supplier interactions. Keep your people trained on what to look out for and carry out regular security training sessions to educate, educate, educate.

"Continuous security awareness is crucial – employees let down their guard with partners." – Troy Hunt, Microsoft

Myth 10: Insurance fully covers supply chain breach damages.

Reality: While cyber insurance helps, it does not cover all liability, legal, recovery and reputation costs from incidents originating in the supply chain. Prevention and resilience are still critical.

"While insurance helps, robust supply chain cybersecurity is still imperative for managing business risk." - Reshmi Khurana, MD at KPMG

Establishing Facts on Supply Chain Cyber Risk

So how can security leaders debunk these myths and strategically manage supply chain cyber risk? Ask these key questions:

- Where are our critical third-party connections and data flows? Map your ecosystem.

- How can we maintain real-time visibility across the attack surface? Monitor beyond periodic reviews.

- Are partners meeting our security expectations in reality? Validate don't just trust.

- How quickly can risks or incidents be discovered and communicated? Improve threat sharing.

- Are we prepared to operationally respond if a third-party is compromised? Test incident response processes.

With ecosystems so fluid, organisations need continuous visibility and dynamic control across the extended attack surface, rather than trusting to point-in-time vendor reviews. New solutions allow just-in-time evaluation of supplier security. Emerging standards will also mandate greater transparency from third parties.

"Assume compromise will occur somewhere in your ecosystem," advises Microsoft CVP Tom Burt. "Have the capacity to isolate and minimise the impact."

The days of simply passing cyber risk down the supply chain are over. Every organisation is only as secure as its partners. As threat vectors rapidly multiply, security leaders must confront supply chain cybersecurity myths with facts. Managing risk holistically across the ecosystem is critical as enterprises digitally transform and interconnect.

With modern supply chain connectivity and risks, organisations need to move beyond outdated point-in-time vendor assessments. Continuous visibility andc control across the entire third-party environment is required to truly manage risk and increase resiliency..

"The expanding cyber attack surface requires a fundamentally new approach to third-party risk - shifting from imperfect periodic reviews to continuous contextual visibility across the entire ecosystem." - Raj Meghani

Cybersecurity Resilience: Fundamental Changes are required

Sarb Sembhi

Sarb Sembhi is CISM, CTO & CISO, Virtually Informed. As a well-respected industry veteran, Sarb speaks, writes and contributes to global security events and publications. He was the Workstream Lead for Thought Leadership of the UK Cyber Security Council Formation Project, is the Co-Vice Chair of the Smart Buildings Working Group and Executive Steering Board member of the IoT Security Foundation. He advises and sits on several start-up boards and is a Mentor on the Cylon accelerator programme. Sarb was shortlisted 5th in the IFSEC Global 2020 "20 Most Influential People in Cyber Security" and included in "2018 Tyto Tech 500 Power List" of influencers in the UK's technology sector.

The resilience governments and enterprises desire will be unachievable without fundamental changes in the industry and enterprise boardrooms.

Words and language mean a lot and make a greater difference than we often realise, we only have to look at how we used to talk about IT Security, then Information Security, then Cybersecurity and now Cybersecurity Resilience. These were not just changes of words to mean the same thing, but more a reflection on the ever-changing world within which we are operating. Many of those who have lived and worked through these changes, if they are still in the profession may actively be looking to move out of it? Let's have a look at why this may be the case and its impact on cybersecurity resilience

The last twenty plus years have seen some of the greatest technological advancements in computing and how business is conducted. Every single one of these changes has both a direct and indirect impact on cybersecurity and how we as professionals respond and manage it. Here's a short list of some of these changes.

1. Increase in cybersecurity standards and frameworks, and the range of changes in them to accommodate the changing threat landscape. Whereas once there were only a few, now it's a case of "pick a standard, any standards". Yet there are many more on the way, that security professionals will need to keep abreast of.

2. Increase in regulatory or legislative compliance, these have been growing more so in the last few years. However, the internationally picture for the future is that there is a greater range of regulations to come. Further, that to accommodate the fast moving technologies, the regulators are being given powers to extend compliance without requiring additional legislation; the UK and European legislation on consumer product security is an example of things to come. All of these and how they impact the enterprise need to be understood.

3. In reality, the standards and regulations have followed the challenges created by the technology available, in use and the growing adoption. Just like the mobile phones each of us use today are better than any spy could have wished for 20 years ago. Devices we have today and what they are capable of have grown very fast, and what was only within the reaches of large enterprises have become within the reach of not only small business, but also many consumers. This has been one of the contributors of not just the Internet of Things, but more the Internet of Everything. Where these devices are far more pervasive than the shadow IT of yesteryear security professionals contend with.

4. The shadow IT isn't just the devices available to users within an enterprise, but the Apps on these devices or available through a browser, facilitated by Cloud Services. Collectively and individually, devices and Cloud Services have enabled and facilitated business models that were previously never possible, but equally they have made it harder for enterprises to control the use, sharing and movement of data between applications, devices and geographical locations.

5. The growth in devices, apps and many multiple user accounts have all been written in code, where the use of secure coding practices and secure by design and default have not been the norm by any stretch of imagination. This has meant that devices and apps may come with gaping vulnerabilities, sometimes it is within the code produced by the manufacturer, sometimes it's within the Application Programming Interface (API) libraries – which means all the apps using the API will be affected in one go.

6. The other impact of multiple devices, apps and accounts is that the number now required to manage one's life has meant that an average mobile device user may have anywhere from 50 to 200 apps and accounts which may hold their user credentials and payment details. Thus making personal devices and authentication details a valuable commodity for attackers. Recent research by Microsoft found that BYOD devices were a major weak point and a successful target for attackers.

7. A further impact of the growth of devices, apps and accounts is that the overall attack surface of an individual and hence the enterprise in which they work has grown exponentially. Whereas, several years ago security managers may only have been concerned about the IT in an enterprise now, there is IoT, OT and other technologies that employees may use or connect with. Making it harder for security teams to close the attack gaps.

8. Not surprisingly, with a fast growing attack surface, attacks have increased, and along the way cyber crime has attracted traditional criminal organisations. Amongst the many advantages for criminals, is that cyber crime knows no boundaries, so opportunities for them are not just the local market, it is wherever their operating skill level takes them.

9. Over the same period, professional bodies and certifications have responded and created certifications for the many technologies and roles that have been created in response. However, virtually all of these certifications focus almost entirely on technology and technology skills.

10. The liability of security managers / CISOs of advice or actions taken or not taken. The findings of the Uber case in the US a few years ago resulting in the CISO going to prison was a wake up call. Although the circumstances in which it happened are outside the discussion here, the fact that it happened, created a precedent that had not previously existed. This has impacted security managers, and has been the topic of many discussions at security events.

There are likely many more changes that readers can add to the list, although it is long enough to serve its purpose to demonstrate that the environment and landscape in which we operate and try to manage cybersecurity has vastly changed. Not only do security professionals need to know so much more, but they are having to be responsible for, overseeing and advising on so much more in order to ensure that their organisation is resilient to attacks. Likewise, enterprise response teams may not have grown at the same pace as incoming attacks have.

In October 2022, I chaired a two day event for security managers where one of the discussion topics was how do we manage change and the impact of the change. Most of this discussion was on our stress, burnout and mental health, and that of our colleagues in the industry. At the end of the discussion it seemed that this was probably enough interest to follow-up on, so I asked if anyone would be willing to volunteer to write-up about this topic. Luckily, there were two amazing colleagues, resulting in the production of a paper which we released in May 2023 during Mental Health Awareness Month -https://www.virtuallyinformed.com/resources/security-papers

In the process of writing the paper, we found that the Cyber Resilience of almost every national government strategy, relied on the Cyber Resilience of its enterprises, and that the Cyber Resilience of an enterprise relied on the resilience of its cybersecurity teams. However, nowhere is there a commitment by any national government nor enterprise to take care of their cybersecurity teams to ensure the Cyber Resilience they desire.

Furthermore, there was overwhelming evidence that despite a skills shortage the impact of burnout, stress and the mental well-being of the most skilled professionals, was making them question their commitment to stay in the industry.

The stark situation that the industry finds itself in is that if burnout, stress and mental well-being are forcing out the most skilled professionals while there is already a skills shortage, what should the government and enterprises be doing about it? Because if they don't do anything about it, then the Cyber Resilient Strategies of governments and enterprises won't be worth the paper they are written on.

The paper led to a presentation and panel discussion at InfoSecurity Europe in June 2023, and a decision by us as authors to set up the Mental Health in Cybersecurity Foundation to take the work proposed in the paper forward. One of the proposals was to develop a Charter for organisations to sign up to at the board level. We will be going public with this in the very near future.

In closing, we cannot over emphasise that the Cyber Resilience of your organisation is directly dependent on the resilience of your cybersecurity teams, so, what are you doing to help them?

A Publication

web for business
swiss webacademy

Edited by:

BlockAPT™

Redaction:
Laurent Chrzanovski and
Romulus Maier †
(all editions)

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

Addresses:

Swiss Webacademy - Str. Scoala de Înot
nr.18, 550005 Sibiu, Romania

BlockAPT Limited
Alpha House, 100 Borough High St, London SE1 1LB

www.swissacademy.eu
www.cybersecurity-dialogues.org
www.blockapt.com