Cybersecurity Trends

UK edition n.1 / 2022

HFS Research : 2022 Cybersecurity Predictions

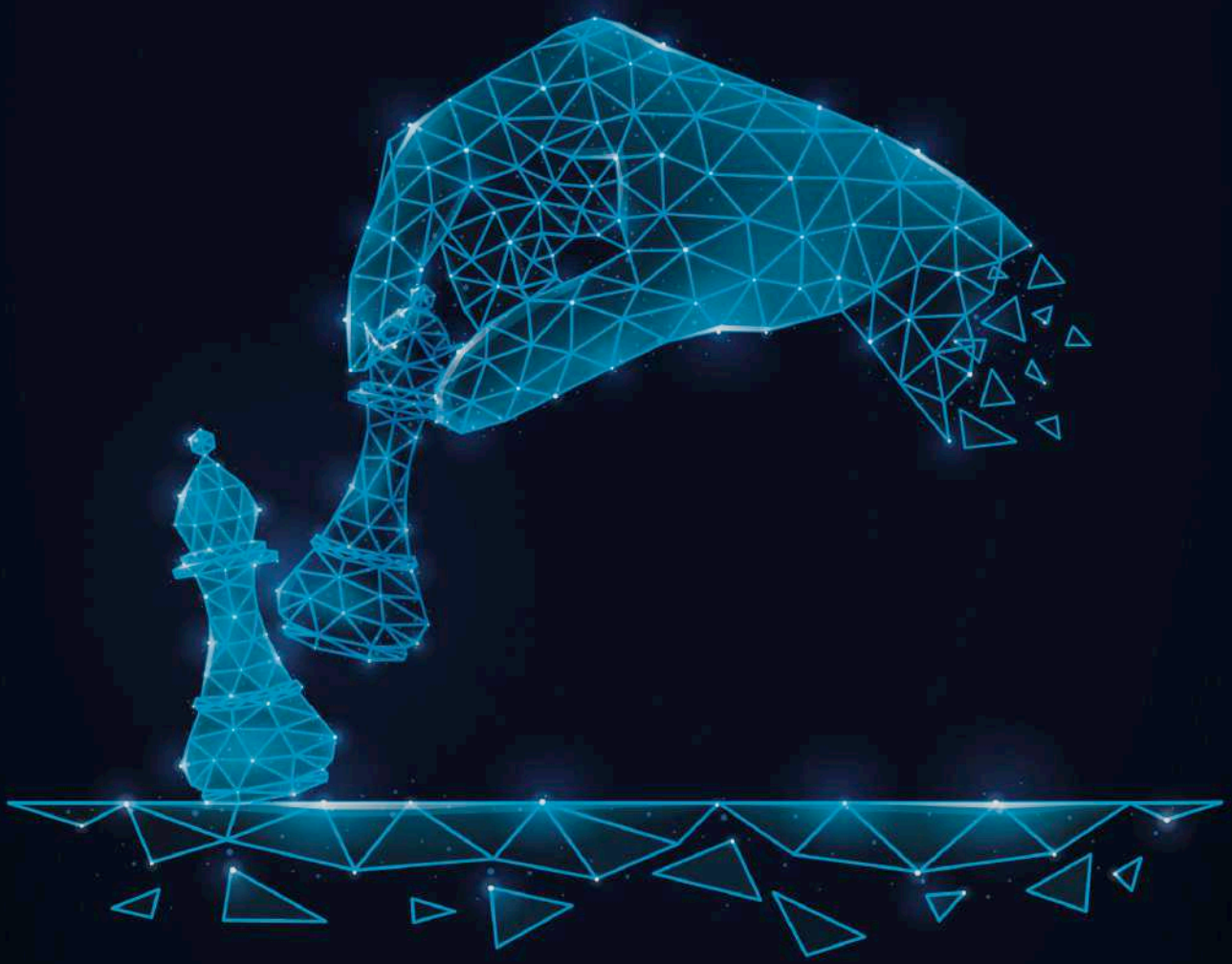
BLOCKAPT™

Next level encryption & quantum computing, building cyber resilience... and more.

BLOCKAPT™

A centrally managed **COMMAND** & **CONTROL**
single platform experience.

Eliminate the weakest link.



info@blockapt.com

blockapt.com

Contents

Cyber Resilience is not an optional extra.



Authors: Raj Meghani, Marco Essomba, Laurent Chrzanovski

It is showtime.

A very Happy New Year to all our publication subscribers and readers!

While everyone has been settling into 2022, we have been busy working with our industry peers and associates to bring you the latest from the world of cybersecurity. Frankly, there is no shortage of bizarre and bewildering stories from around the world when it comes to this sort of thing.

To kick off our first edition of 2022, we wanted to bring in the latest viewpoints without getting lost in the jargon or jumping on the next 'industry buzzword'.

Our aim is to strive deeper into emerging concepts that will shape the future of cybersecurity for Enterprise and Small and Medium Businesses. It is important to remember that some of the concepts at this point in time need further preparation, ground-work and planning to adopt over time. Methodologies like Zero-Trust for example, which we discussed in our past issues require not only the strategy and technology side of things for implementation but also a mindset change.

Stay Resilient : Cyber Resilience is the word of the year.

Mindset, an often missed out entity is an important variable when it comes to affecting security resilience strategy. Mindset acts as a basis for a lot of the articles that you will be reading about in this and future issues that works towards promoting a resilient mindset.

In the UK, new laws have been proposed by the Government to strengthen the UK business' resilience from cyber attacks in the wake of recent high profile attacks. This sees a £2.6 billion injection into a new 'National Cyber Strategy'.

"Every UK organisation must take their cyber resilience seriously as we strive to grow, innovate and protect people online. It is not an optional extra."
- Julia Lopez, Minister of State for Media, Data & Digital Infrastructure

It is obvious that more firms are providing essential services digitally and hence the move towards stricter security duties with target fines (much as £17 million) for non-compliance, more stringent incident reporting and the driving up of standards in the security profession. To this effect, the Network and Information Systems (NIS) Regulations which look at critical services (water, energy, transport, healthcare, etc) are also being updated based on improving their security measures.

An important update to NIS now includes scoping in Managed Service Providers (MSPs) and IT outsourcing organisations as these firms handle privileged access to their client's networks and systems.

We will also see more active roles from Ofcom, Ofgem and the ICO with regards to incident reporting and subsequent handling of reports.

So, this is why it is a crucial time to raise your cyber resilience game. But resilience is just a word summing up the multi-faceted elements within security. This could be from strategy, technology and all the way to addressing cybersecurity skills/training shortages.

Our publication brings together peers and thought leaders to help bring various aspects of resilience by shining light on important topics - themes well captured within HFS Research' top 20 cybersecurity predictions for 2022.

We hope these articles inspire you to build your resilient and future-ready security strategy.

Happy reading! ■

HFS Research 2022 Cybersecurity Predictions.

Author: Ralph Aboujaoude Diaz

HfS Research
The Services Research Company™

2022 will be the year where enterprises realise that the only way to effectively respond to emerging cyber threats is to take care of their talents, automate processes, boost intelligence, increase visibility and improve collaboration. Here are our twenty down to earth cybersecurity predictions/trends for 2022, mapped to HFS OneEcosystem™.

Wealth of acquisitions by large service providers of supply chain cyber risk management pure players	Security orchestration and automation platforms will gain significant traction	Way more focus on preventive measures to fight ransomware attacks	Increased international collaboration to disrupt and dismantle Safe Havens fuelling ransomware attacks
The "great" cyber resignation is real and will cause deployment paralysis	Focus will be on building an integrated passwordless strategy	More automation related services to help enterprises alleviate the unsustainable compliance burden on security functions	Significant investments in optimising cyber hygiene activities
Rise in privileged accounts hijacking	Enterprises will get serious about building a cybersecurity conscious culture	More enterprises will delegate their responsibility for managing security risks and controls to CSPs and/or MSSPs	Defining and embedding holistic cloud monitoring frameworks will be high in CISO's agenda
Increased partnership between Intelligent Automation vendors and cybersecurity vendors	Emergence (and acquisition) of few innovative vendors providing virtualised cryptography solutions	Cybersecurity readiness platforms for SecOps teams will gain significant traction	Significant increase in enterprise-wide adoption of DevSecOps practices
Rise in adoption of AI-powered offensive techniques to increase the effectiveness of threat hunting processes	Managed security service providers will bring to market holistic and tailored 5G security offerings	Readiness initiatives will be on the rise to help enterprises prepare for quantum-safe cryptography	Application containerisation will become the new norm for securing BOYD environments

DETAILED OVERVIEW

#	Prediction/ trend	HFS OneEcosystem touchpoint
1	**Wealth of acquisitions by large service providers of supply chain cyber risk management pure players** Supply chains continue in chaos going into 2022, alongside the increasing complexity that predated COVID-19. To cope, improving the transparency and integrity of those supply chains will be a must for organisations across all industries. 2022 will see organisations thinking beyond just securing their own perimeter to better secure their vendor ecosystems. As a consequence, 2022 will see a wealth of acquisitions and partnerships by established large service providers focused on supply chains. Specialised supply chain risk management companies offering advanced capabilities, such as AI and Machine Learning, to monitor and anticipate cyber threats across global business relationships will be their main target.	Partner Experience (PX)
2	**Security orchestration and automation platforms will gain significant traction** Our recent HFS Cybersecurity Pulse study showed that 74% of cybersecurity teams are unable to keep up with the increasing volume of security events and nearly 65% struggle to manage the complexity of too many disconnected security and compliance tools. 2022 will be the year when enterprises realise that the alert management "fatigue" can only be contained through the deployment of "above the landscape" and vendor-agnostic platforms capable of orchestrating and automating a wide range of disparate, routine, and high-volume security activities (from threat detection to incident response).	Employee Experience (EX)
3	**Way more focus on preventive measures to fight ransomware attacks** "Run somewhere" and wait for the disaster to happen is not an option anymore to combat ransomware. In 2022, CISOs, IT and Business leaders will seriously focus on strengthening defensive and resilience measures to avoid or minimise impact of ransomware attacks. And this will be done by balancing technology alongside people and processes. Enterprises will double down on preventive measures by putting threat intelligence and incident containment measures at the forefront of their ransomware defence strategy.	Employee Experience (EX) and Partner Experience (PX)
4	**Increased collaborations and partnerships to dismantle Safe Havens fuelling ransomware attacks** The vicious circle of democratisation (making ransomware available to anyone), cryptocurrency (anonymising payments), and safe haven (legitimising practices) has drastically driven the intensification of ransomware attacks in 2021. Many countries are providing safe havens to attackers, allowing them to run and expand their criminal organisations legitimately. We will see in 2022 increased international collaborations and partnerships between enterprises, law enforcement authorities and intelligence agencies to disrupt and dismantle the criminal ecosystem in these safe havens, leading to many high-profile arrests.	Partner Experience (PX)

#	Prediction/ trend	HFS OneEcosystem touchpoint
5	**The "great" cyber resignation is real and will cause deployment paralysis** 2022 will be known as the "great" cyber resignation and increasing cybersecurity budgets will not save the day. The negative impact of the global cybersecurity talent shortage in 2021 will be exacerbated in 2022 due to the fact that an excessive workload has been forcefully pushed to existing cybersecurity teams, contributing to an operational "fatigue" and increased burnout rate in 2022. Our research revealed that 81% of organisations are actually planning to increase the use of managed security service providers in 2022 to tackle the talent shortage but this will unfortunately not be enough. Outsourcing security activities to MSSPs will certainly not solve the skills shortage as MSSPs will be having the exact same problem finding talented professionals that organisations desperately need. MSSPs have significantly increased their investments in 2021 to train the cybersecurity "workforce of the future" but the return on investment will not materialise before 2024 due to the technical expertise required for cybersecurity jobs.	Employee Experience (EX)
6	**Focus will be on building an integrated passwordless strategy** Organisations realised in 2021 that going passwordless can significantly help them enforce enhanced security standards and improve user experience. Passwordless authentication is trending up, especially for SaaS, and is soon becoming the industry standard. But our latest HFS Cybersecurity Pulse study showed that 83% of organisations are still facing challenges in establishing passwordless authentication mechanisms since most organisations have tackled passwordless as an overnight destination rather than a well thought out journey. We will see in 2022 more and more organisations spending time and effort to build an integrated passwordless strategy across the enterprise.	Customer Experience (CX), Employee Experience (EX) and Partner Experience (PX)
7	**More automation related services to help enterprises alleviate the unsustainable compliance burden on security functions** The implementation of Governance, Risk, and Compliance technologies was the number one area where organisations received the most value out of their cybersecurity investments in 2021 (nearly 30% of organisations highlighted this in our HFS Cybersecurity Pulse study). But the volume and frequency of risk and compliance activities kept increasing in 2021 and GRC technology alone is not enough to alleviate the compliance burden on information security functions. 2022 will be the year where security service providers will actively reposition/rebrand their existing intelligent automation products and services to meet the increasing demand from enterprise clients to automate a wide range of compliance activities. We will see many organisations deploying a digital workforce (intelligent virtual assistants, RPA bots, etc.) to guide cybersecurity professionals and end-users through the execution of risk, security, and compliance activities.	Employee Experience (EX)

#	Prediction/ trend	HFS OneEcosystem touchpoint
8	**Significant investments in optimising cyber hygiene activities** Good IT security housekeeping (patching, upgrades, corrective notes, etc.) is an invisible, time-consuming and in many cases complex service. But good housekeeping practices require good process discipline, collaboration and execution speed. It is not a surprise that lapses in security hygiene have presented significant opportunities for attackers in 2021. As highlighted by our recent HFS Cybersecurity Pulse study, cyber hygiene will be a top priority for 84% of organisations in 2022. We will see significant investments from organisations to implement best practices for managing the security around IT assets and increase the remediation speed of vulnerabilities detected during ongoing cyber hygiene scanning.	Employee Experience (EX) and Partner Experience (PX)
9	**Rise in privileged accounts hijacking** Privileged accounts are usually the primary targets of attackers, allowing them to gain elevated administrative access and quickly move laterally through the network searching for sensitive data and other high-value assets. Our latest HFS Cybersecurity Pulse study has revealed that one of every two enterprises still rely on too many manual processes for managing privileged access, leading to low operational efficiency and significant risk exposure. Well-designed privileged access processes are unfortunately not enough to keep pace with the constant and soaring number of privileged accounts, and our view is that only high levels of automation can guarantee the completeness, accuracy, and timeliness of day-to-day operational activities. In 2022, we will see a significant increase in security breaches, especially in the Operation Technology domain, caused by privileged accounts hijacking (human and non-human identities), especially cloud account hijacking.	Employee Experience (EX) and Partner Experience (PX)
10	**Enterprises will get serious about building a cybersecurity conscious culture** Our latest HFS Cybersecurity Pulse study highlighted two main factors which have contributed to sixty percent (60%) of security events in the past two years: human errors caused by a lack of adequate training or process discipline and new IT initiatives implemented without proper security oversight and controls. In 2022, enterprises will prioritise initiatives that address the human factors that weaken the cybersecurity chain. We will see more and more organisations establishing enterprise-wide programmes to develop and measure cybersecurity literacy. Organisations will implement mandatory cybersecurity learning paths more adapted to the context of each user community, but more importantly, will start measuring individual goals as part of the periodic performance review process. Last but not least, when leaders just talk the talk, it's unrealistic to expect employees to walk the walk in organisations. We will be expecting much more from senior executives in 2022 and the effectiveness of their cyber-aware attitude will be measured. Cybersecurity-related metrics will be embedded into their key performance indicators to make them more accountable.	Employee Experience (EX)

#	Prediction/ trend	HFS OneEcosystem touchpoint
11	**More enterprises will delegate their responsibility for managing security risks and controls to CSPs and/or MSSPs** The increasing adoption of Security as a Service (SECaaS) models have already moved the responsibility for managing security operations from organisations to Cloud Service Providers (CSPs) and/or Managed Security Service Providers (MSSPs). Our latest Cybersecurity Pulse study showed that almost two thirds (61%) of organisations expect their first line of defence information security functions to move to a second line of defence role in the future. We will see in 2022 more and more organisations delegating the responsibility for managing security risks and controls to CSPs and/or MSSPs. This push will be accompanied by the deployment of a wide range of internal monitoring processes from the enterprise side, and automation will play a critical part in bringing greater efficiency and assurance.	Employee Experience (EX) and Partner Experience (PX)
12	**Defining and embedding holistic cloud monitoring frameworks will be high in CISO's agenda** Our latest HFS Cybersecurity Pulse study showed that monitoring and measuring the effectiveness of security policies across cloud environments were the biggest challenges faced by organisations on their journey to secure the cloud environment (44% of organisations). Organisations will spend much more time and effort in 2022 defining cloud monitoring frameworks to effectively monitor applications, infrastructures, user interactions and process adherence. KPIs to measure cloud security visibility will be developed and advanced reporting capabilities will be deployed.	Employee Experience (EX)
13	**Increased partnership between Intelligent Automation vendors and cybersecurity vendors** The hard truth is that most organisations have deployed intelligent automation in a rush in the past few years, treating security as an afterthought. Intelligent automation providers, especially Robotic Process Automation vendors, will make significant investment in cybersecurity in 2022. We will see a wide range of partnerships being formed with cybersecurity vendors to improve the effectiveness of controls governing identity and access management, privileged access management, authentication and credential management, and endpoint detection and response.	Partner Experience (PX)
14	**Emergence (and acquisition) of few innovative vendors providing virtualised cryptography solutions** Enabling a truly multi-cloud and customer-owned key management environment to strengthen data privacy controls has been a real challenge for most organisations in 2021, struggling to consolidate multiple management systems from different hardware security module (HSM) vendors, different cloud key management systems (KMS) and cloud HSMs, as well as keys used in home-grown solutions. As a result, organisations have	Employee Experience (EX)

#	Prediction/ trend	HFS OneEcosystem touchpoint
14	realised the hard way that orchestrating such operations can quickly become a very costly and daunting task. We will see in 2022 the emergence (and acquisition by large technology vendors) of few innovative vendors aiming to tackle such problems by providing virtualised cryptography solutions to facilitate the management and orchestration of encryption keys.	
15	**Cybersecurity readiness platforms for SecOps teams will gain significant traction** Cybersecurity readiness will be high on the CISO agenda in 2022. Modelling, quantifying, and ultimately enhancing cybersecurity posture will become a key priority. We will see the emergence of third-generation cyber range platforms that will allow organisations to run a wide range of training exercises (powered by automated and AI-enabled attack simulations) with the ultimate goal of continuously strengthening their cybersecurity stack and assessing the readiness and skillsets of their cybersecurity personnel.	Employee Experience (EX)
16	**Significant increase in enterprise-wide adoption of DevSecOps practices** Our latest HFS Cybersecurity Pulse study revealed that only 31% of organisations have deployed DevSecOps practices widely across the enterprise. CISO mandates exist but IT functions are still not able to effectively translate global security requirements into local standard operating procedures supported by dedicated technology enablers. 2022 will be the year where the level of adoption of DevSecOps practices will significantly increase throughout the organisation. A special focus will be on securing APIs, and we will see the emergence of many tools aimed at helping developers better orchestrate authorisation and policy management for their applications and services.	Employee Experience (EX)
17	**Rise in adoption of AI-powered offensive techniques to increase the effectiveness of threat hunting processes** Attackers have started to leverage an arsenal of AI-powered offensive techniques in 2021 to be much more effective in their campaigns, making cyber-attacks more effective, finely targeted, and difficult to attribute. 84% of organisations have highlighted this threat as the most damaging threat vector they will face in the next 2 years. Most organisations have realised in 2021 that they cannot cope with such sophisticated attacks, and 2022 will be the year where many of them will start to actively adopt AI-powered offensive techniques too in order to increase the effectiveness of their threat hunting processes.	Employee Experience (EX)
18	**Managed security service providers will bring to market holistic and tailored 5G security offerings** In our latest HFS Cybersecurity Pulse study, 82% of organisations have raised a serious concern regarding the exponential rise of new IoT devices introduced into 5G networks, injecting novel threats (due to an increased	Employee Experience (EX) and Partner Experience (PX)

#	Prediction/ trend	HFS OneEcosystem touchpoint
18	attack surface), and drastically strengthening existing ones. Organisations need help and they clearly understood in 2021 that security cannot be an afterthought. We will see the emergence in 2022 of Security Operation Centres tailored for 5G security. Service providers will come up in 2022 with compelling service offerings aimed at tackling the 5G security threat landscape in a holistic manner (from terminals to internal/external services and applications).	
19	**Readiness initiatives will be on the rise to help enterprises prepare for quantum-safe cryptography** Significant technical advancements in quantum computing have been made in 2021. We are yet to see commercially viable applications, but the few industry-specific use cases have shown promising results. Organisations realised in 2021 that it is not so much a question of if but when. And they also recognised that the systemic risks that quantum computing will pose must be addressed sooner rather than later. In our latest HFS Cybersecurity Pulse study, 81% of organisations have raised a serious concern regarding the impact of quantum computing on current cryptographic security protocols. To better equip their IT and Security teams, organisations will initiate in 2022 enterprise-wide quantum safe readiness programmes to assess the impact of quantum computing on existing cryptographic systems. These programmes will also help organisations understand the various adoption challenges and better plan their migration journey to post-quantum cryptography.	Employee Experience (EX) and Partner Experience (PX)
20	**Application containerisation will become the new norm for securing BOYD environments** Our latest HFS Cybersecurity Pulse study revealed that close to 40% of organisations strongly agree that the rapid convergence of Cloud, IoT (Internet of Things) and BYOD (Bring Your Own Device) has raised new significant security concerns on data protection. As a result, mobile security is becoming a critical issue in BYOD as more and more employees in 2022 will be using their own mobile devices to access their organisation's data and systems. One particular BOYD security model will see a significant increase in adoption throughout 2022: the application containerisation used in conjunction with mobile application management (MAM), allowing organisations to remotely prescribe and monitor security controls to specific applications and data.	Employee Experience (EX)

BIO

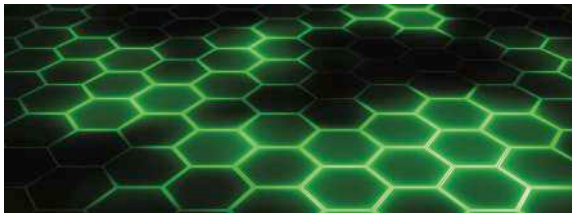
Ralph Aboujaoude Diaz is a Practice Leader at HFS, based in London, UK. With over 16 years of professional experience, Ralph has helped a wide range of organisations improve and transform their IT security, risk and compliance environments. Ralph has strong risk management knowledge (gained through 11+ years of audit and advisory experience in the Big 4). He was also Senior Director in the Core Tech Strategy & Transformation Leadership Team (Life Services industry), where he led the design, delivery and operation of a global Security and Governance transformation programme. With over 32K+ followers, Ralph is an active contributor on LinkedIn and was a key contributor to the first book on Intelligent Automation (IA).

Exploring 'Cybersecurity Mesh'.

Just another tag or a paradigm shift?

Author: Raj Meghani

It is the new year and the security landscape is already brimming with new acronyms, tags and terminologies. Cybersecurity Mesh (CM) has hit the centre stage and is a term that you will soon hear much about with regards to strategy and architecture.



As defined by Gartner, the Cybersecurity Mesh is a distributed architectural approach to scalable, flexible, and reliable cyber control. The mesh changes the focus from protecting a traditional IT perimeter (a 'walled city' approach) to a more modular approach that centralises policy orchestration but distributes enforcement of cybersecurity policy.

The definition is a mouthful and certainly a theme that needs to be read and visited a few times to be fully absorbed and digested.

To explore the concept of CM, we should essentially revisit the topics I wrote about in the previous editions, namely the Zero Trust and Defence-in-depth topics. CM is essentially an extension of these themes.

Some may question the need for another label if it is just an extension of Zero Trust. I am neutral to that debate, but I do acknowledge that Zero Trust is a very broad topic with its application across strategy and implementation.

The industry is still new to Zero Trust and bringing in CM to the mix can be overwhelming. But I do believe the fundamentals of CM are essential when it comes to security transformation.

Zero Trust - A Total Recall

According to the National Institute of Standards and Technology (NIST), Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to focus on

BIO

Raj Meghani is the Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.
Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank.
Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 20 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.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

users, assets, and resources. A Zero Trust Architecture (ZTA) uses Zero Trust principles to plan industrial and enterprise infrastructure and workflows. Zero Trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership.

Understanding Cybersecurity Mesh

There is no doubt that the pandemic's shift on IT systems and workforces have driven the need for evolution to the existing structure of traditional security perimeter.

This is because more and more assets now fall beyond the traditional security boundary, and thus security needs to be redefined around the identity of humans or machines. As perimeter security becomes less suited to the current climate, the security approach of a walled city must evolve to the current shift of enterprises.

Cybersecurity Mesh enables scalable, flexible and reliable cybersecurity control via a dispersed architecture approach.

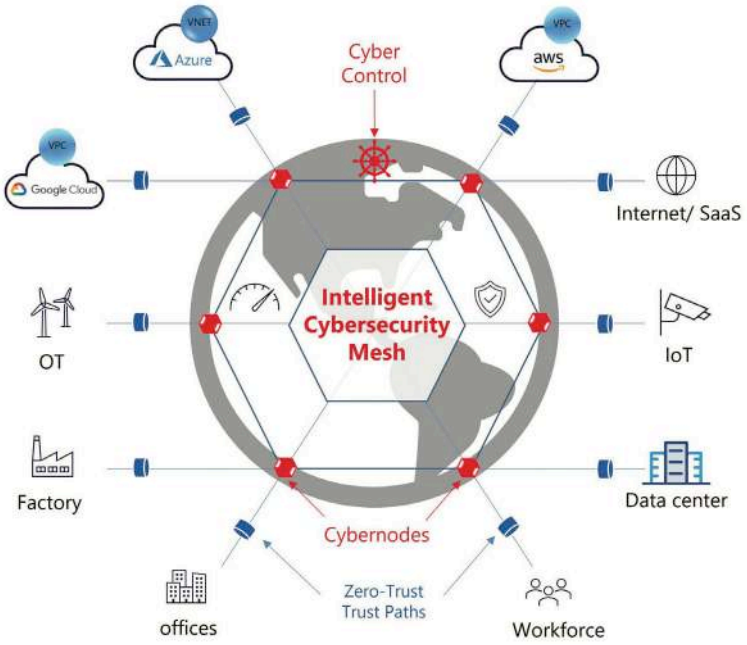
CM's method of network security leads to a more standardised and responsive approach that is aimed at preventing cybercriminals from infiltrating a part of the network and spreading their access to the wider network as with the case of Advanced Persistent Threats (APTs).

'Meshison' Impossible or Sensible?

As cyber defence strategies go, CM makes complete sense as this course secures every device with its own border security (for example firewalls, network security tools, etc).

Today many security practices still use traditional perimeter-centric tools to secure whole IT environments and this has resulted in some of the big-name breaches we have seen across 2020 and 2021. CM's holistic approach

is closely linked to the 'defence-in-depth' principles (albeit, with a distributed technique) that I widely preach and endorse.



Security infrastructure needs to be agile enough to cover the remote workforce working on the intellectual property of organisations. This kind of flexibility in security infrastructure can only be achieved by decoupling policy decisions and enforcement.

The new course of security will essentially then be mapped around identity than the traditional perimeter or physical boundaries. This will ensure that the right personnel have access to the right data across the network regardless of location or where data is stored.

Sure, the task is easier said than done. But it makes sense that decentralised IT and workforces environments are equally secured by a decentralised security concept, i.e. Cybersecurity Mesh.

Mesh essentials

As CM is a step up over the more recent tried and tested cybersecurity practices, it is essential that enterprises make sure their current strategy and technology are in line with foundations such as centralised policy management and orchestration, threat intelligence and triggers and a distributed identity access management.

This allows for a natural transition to a meshed transformation with minimal disruption to business operations.

Closing remarks

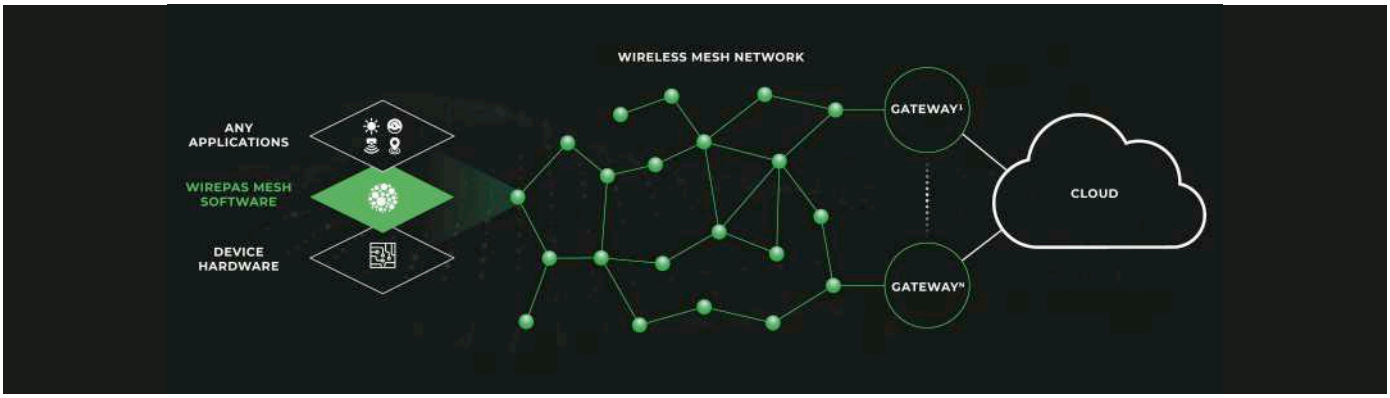
Mesh will remain a talking point for the next few years. It is predicted (Gartner) that by 2024 mesh technology will be the cornerstone of tackling breaches and the financial impact for organisations.

Currently, mesh as a concept is heavily a strategy but eventually mesh technology will heavily rely on analytics and intelligence to likely move beyond SIEM and SOAR's reliance on integration.

Mesh adoption will also become a building block for achieving Zero Trust, which ensures data, applications and devices are securely accessed by authorised and trusted personnel in a location-agnostic manner.

Existing Identity and Access Management (IAM) suffers from security, scalability, reliability and privacy, so this needs to be addressed by security technology and configured to adapt the mesh approach. Achieving holistic security requires more investment in upskilling, risk assessments and learning particularly from the Blockchain services industry.

Paradigm shift it is then. ■



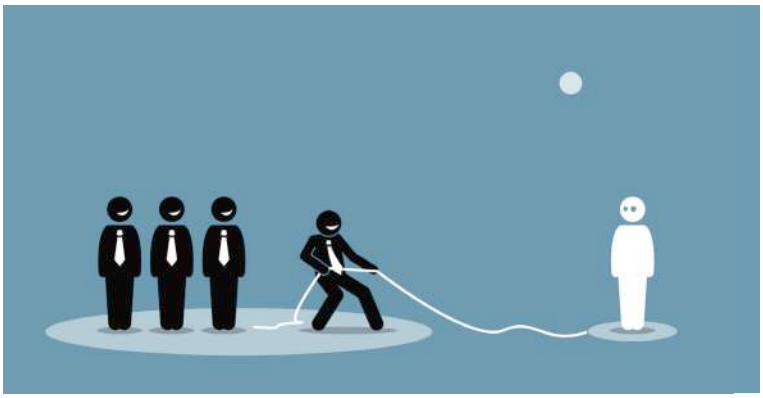
IT starts with MISSION.

Private organisations can attract talent by putting cybersecurity work in a larger context.

Author: Kurt Sanger

I recently ran into a friend and former U.S. Service Member now working as an Executive with a cybersecurity company. In my position with the U.S. Department of Defense I did not have much insight into the business from a non-government perspective. With retirement from the military rapidly approaching, I asked him what he focused on in his work. *"I spend 90% of my time filling boat spaces",* he answered … Marine Corps lingo for finding people to fill jobs.

The answer surprised me. I knew government organisations had trouble finding and retaining qualified personnel, but I thought it was because organisations like my friend's were offering better salaries and perks. *"It's across the board",* he said, *"there is nowhere near enough talent to go around ... for anyone".*



As I learn more about the private sector I am discovering the pervasiveness of the issue. The competition for talent appears to be cutthroat. It is particularly difficult for the U.S. Government to succeed in such a competitive marketplace because of its standard pay schedules and benefit programs, from which there are rarely deviations.

What the U.S. Department of Defense can offer, that few others can, is access to sophisticated tools, information and platforms that are known only to select audiences because of their classification, and because they can be used only by those working under authorities that solely belong to the government. Certainly, the Department does rely on this privileged access when recruiting cyber talent. However, it more heavily relies on the same thing that militaries have relied on in recruiting since the first soldiers were ever organised: a sense of **MISSION**.

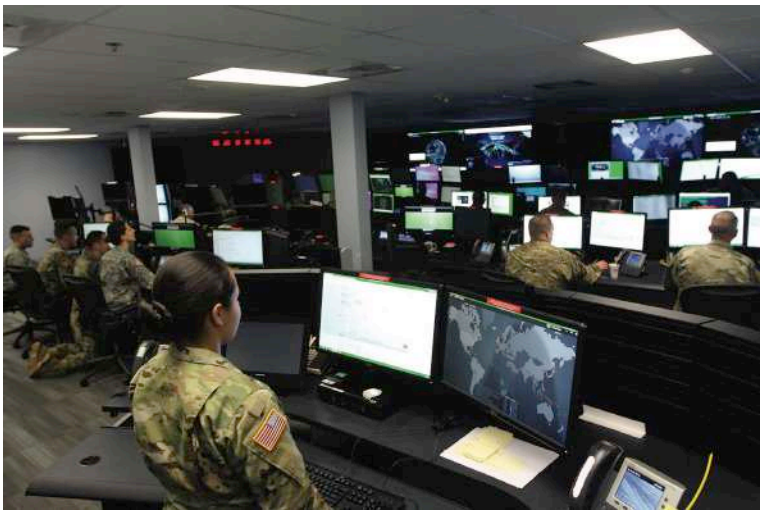
The term 'mission' is used in different ways in the military context. It can be used to describe a single operation, or a set of operations. It is easy to identify these types of military missions. They are often spelled out explicitly in orders from commanders.

BIO

Kurt Sanger is a Lieutenant Colonel and Judge Advocate with the US Marine Corps. He is a 2015 graduate of the Georgetown University Law Center's National Security Law program. Since 2014, Kurt has advised senior military and policy leaders on cyberspace operations and national security issues. As a well-respected military industry veteran, Kurt is sought after for his thought leadership and contributes writing, producing and hosting conferences, speaking at webinars and events with a global presence. Kurt is a panelist at the June 2022 RSA Conference in San Francisco and can be followed via his LinkedIn profile. These opinions are Kurt's own and do not necessarily reflect official positions of the Department of Defense.

'Mission' is also used in a more meaningful sense. It is not a discrete activity to be accomplished, but a reason for existing, not only as an organisation but as an individual... something that is larger than oneself but that defines oneself. This type of mission also is associated with religious orders and the efforts they pursue in service to the higher powers they believe in.

Militaries and religious groups are not the only organisations that have missions, however, and certainly are not the only organisations whose missions are vital to individual professions, communities and nations, as well as international security and stability. Considering the dependence of most commerce and daily life on a functioning and secure internet, cybersecurity professionals are as important to economic and physical security as any professional armed force, if not more so in our technologically advanced and technology dependent world.



It is vital for cybersecurity professionals to recognise their value to society and humanity, and it is in any organisation's interest to develop a sense of mission among their cybersecurity professionals. Through demonstrating to employees that their value cannot be measured in the bottom line alone, but also through their contribution to a greater good, an organisation can distinguish itself among competitors for talent.

How can a private cybersecurity organisation build this recognition among its workforce? In the same way the military builds its sense of mission and esprit de corps among its troops... by connecting the efforts of the organisation to the bigger picture. An employee can find value not only in salary and benefits but in the understanding that their work has meaning and positive effects that radiate far beyond one's immediate view.

Anyone employing a cybersecurity professional should prioritise helping their employees recognise the greater value in what they do. Employers should highlight the direct line between cybersecurity work and the functions cyberspace facilitates, not only for the employees that immediately benefit from their work, but the customers, vendors, and everyone in the production and output chains who depend on the systems they support. Cybersecurity professionals should be ever conscious of the fact that the networks they protect exist within a larger system, and that billions of people depend on that system to enable most aspects of their professional and personal lives. With the mission to protect the wellbeing of any part of that system, even the most mundane aspects of work can become meaningful.

Militaries and religions have used the gratifying sense of mission to attract potential members from their beginnings. So too can private organisations rely on mission to differentiate themselves when competing for talent that is in high demand. An organisation that merely pays its employees will always be outcompeted by an organisation that pays and inspires them. ■

Is Encryption dead?

Author: Marco Essomba

Not quite, but I had to use a clickbaity title to get the message across.

But we have to acknowledge that traditional data encryption is faced with a myriad of problems on top of being prone to vulnerabilities as well as not being able to keep up the pace of the technology industry. I deliberately chose not to list some of the big-name data breaches associated with this as, firstly, we all know of them, and secondly, not to stray far from the topic.

All things considered, we are not far off from seeing the end of traditional encryption techniques.

I strongly believe that Micro-Tokens will succeed with the current outdated encryption methods. But before we go on to this, it is good to have quick definitions of both.

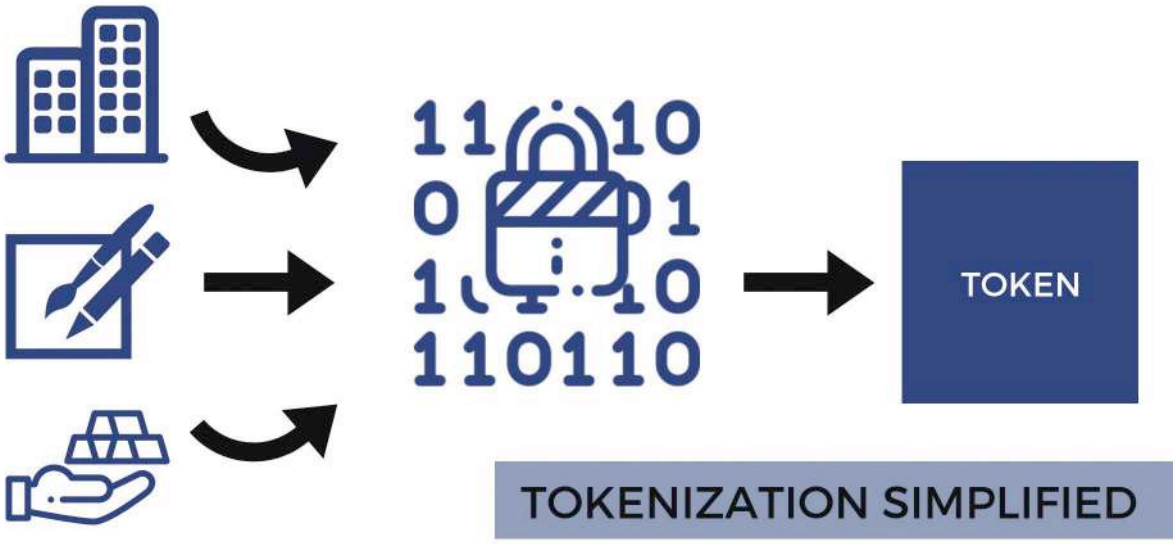
What is?

Encryption is the process of using an algorithm to transform plain text information into a non-readable form called ciphertext. An algorithm and an encryption key are required to decrypt the information and return it to its original plain text format. SSL/TLS encryption are examples of commonly used encryption methods to protect information as it's transmitted on the web.

Tokenization is the process of turning a meaningful piece of data, such as an account number, into a random string of characters called a token that has no meaningful value if breached. Tokens serve as a reference to the original data, but cannot be used to guess those values.

BIO

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 and 35,000+ on Twitter, he is sought after for his quick problem-solving approach and helping businesses futureproof their security infrastructure.
To find out more about BlockAPT, please visit https://www.blockapt.com
To find out more about Marco Essomba, please visit https://www.linkedin.com/in/marcoessomba/ or https://twitter.com/marcoessomba



Why is this a problem?

Quite simply, the problem with encryption arises from the reliance on 'keys' or 'passwords' to lock and unlock data.

Information, data or transactions communicated internally or to 3rd parties using traditional solutions such as SSL/TLS are open to vulnerabilities. The use of encryption keys makes it easy for Man-in-the-Middle (MiM) attacks or rogue DNS points to intercept the key and decrypt valuable/sensitive information.

The below quote put this into a perspective.

"If you put a key under the mat for the cops, a burglar can find it, too. Criminals are using every technology tool at their disposal to hack into people's accounts. If they know there's a key hidden somewhere, they won't stop until they find it."

– Tim Cook, Apple's CEO

Technical and IT-led limitations related to latency and degradation issues around encryption aside, an MiM attack is the biggest threat that organisations are facing currently when using traditional encryption methods.

Enter Micro-encryption

The concept behind the micro-encryption or micro-token lead data exchange is acknowledging the fact that real data can be intercepted, stolen or extracted by a bad actor in the middle and hence let us not use real data at all. So how does this work?

Instead of encrypting data at its origin point as a data package, Micro-Token exchange replaces the data at the origin with Micro-Tokens.

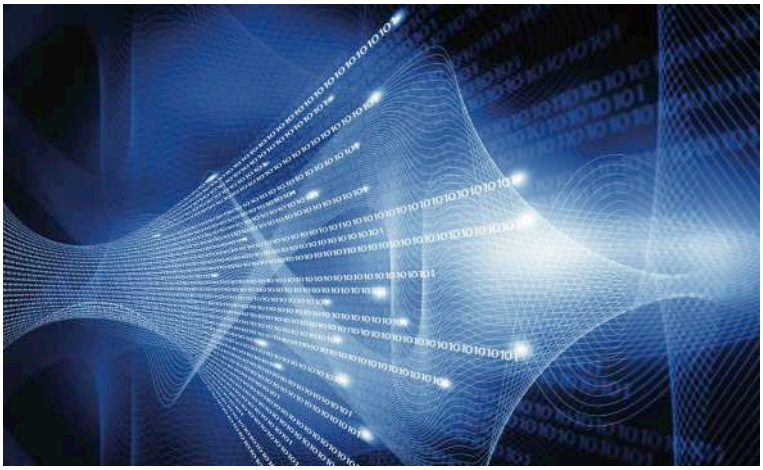
Cybercriminals are used to breaking through the firewalls and encryption to intercept data. In this case, all they get are micro-tokens, which are meaningless in value or worth.

Unlike encryption, tokenization does not use a mathematical process to transform the sensitive information into the token. There is no key or algorithm that can be used to derive the original data for a token.

They are rendered so meaningless that hackers can unleash all the quantum computing power they have and they still won't be able to reverse engineer the tokenized data simply because they are not based on the usual encryption techniques.

This is a big breakthrough in tackling data breaches on a massive scale. For cybercriminals, the cost and complexity involved in trying to break into micro-tokens based systems makes it uneconomical and ultimately will make them consider other easier targets.

There are also other benefits of this technology. Firstly, original data not leaving the location which appeases some of the stringent compliance requirements. Secondly, micro-tokens exchange is quicker and more efficient when it comes to point to point secure transactions.



Final thoughts

Visualise this. Is it safer to have a box with a padlock protecting a valuable piece of information or a box that contains the same piece of information but this time individually (letters) shredded into micro-pieces, dropped back into the box and shuffled around?

You can agree that the padlock can be broken and content assessed but putting the shredded information back together is almost impossible and not worth the energy or time.

This will be revolutionary as the application easily extends beyond data exchange all the way to other connected and smart devices including IoT, Smart Electric Vehicles and so on. In fact, any device or infrastructure that is constantly emitting and receiving data and information and are prone to be taken over by hackers can be protected with this methodology.

Any downsides? As with everything, there are some kinks to be ironed out such as how to scale securely while maintaining performance as the size of databases increases. But the merits far outweigh any disadvantages.

This application is very applicable right now to the payment card industry standard (PCI), where transactional information needs to be securely stored and protecting digital information documents such as identity cards/ passports, credit card and other PII data.

That is why this is such a game-changer. No more lottery wins for the bad guys.

So back to my original question, is encryption dead?

Not quite, but we have to kill it at some point so that it paves the way and bring awareness towards Micro-Tokenization. ■

Quantum Computing requires advanced safeguards.

Author: Aron Seader

Society has already benefited from quantum computing, and we continue to witness how quickly this powerful technology can simulate and test theories. But not everyone uses this technology for good - with more powerful technology comes more advanced bad actors who will use it maliciously. We cannot continue to wait for these hackers to use quantum computing against us, so preparation now is critical. To combat these threats, it will take proactive, thoughtful approaches to cybersecurity and a new understanding of best practices that may seem foreign but will be instrumental in protecting our data and companies moving forward.

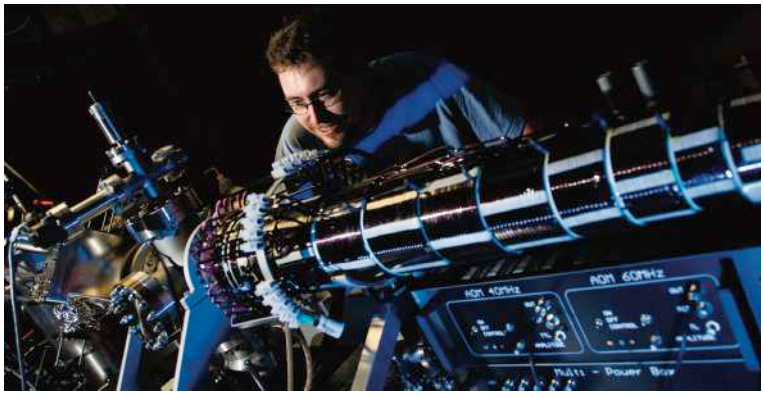
BIO

Aron Seader brings nearly 15 years of technical and leadership experience to Eclypses as the Senior Director of Core Engineering. His industry sector experience spans solar energy, fibre optics, and mechanical engineering. At Eclypses, Aron leads the Core Engineering team, overseeing implementation and software development projects, and conducting product management of Eclypses' MTE technology. Aaron and his team were instrumental in securing the FIPS 140-3 validation. He works closely across business units to ensure Eclypses' core technology and messaging are aligned and up to date.

How does quantum computing work, and what makes it vulnerable to cyberattacks?

Quantum computing works on the same principles as modern computing, representing the world through complex mathematical equations. The difference is that instead of being restricted to a binary (yes/no, on/off, 0/1) answer, quantum computing can use qubits and superposition to represent more complex answers.

Because they are quantum particles, Qubits can exist in 2 states at once, and it is the superposition, the amount it is in one state versus the other, that can be utilised to answer more complex questions. Classical computers can only compute one answer at a time, systematically computing through lots of individual equations to reach an overall conclusion.



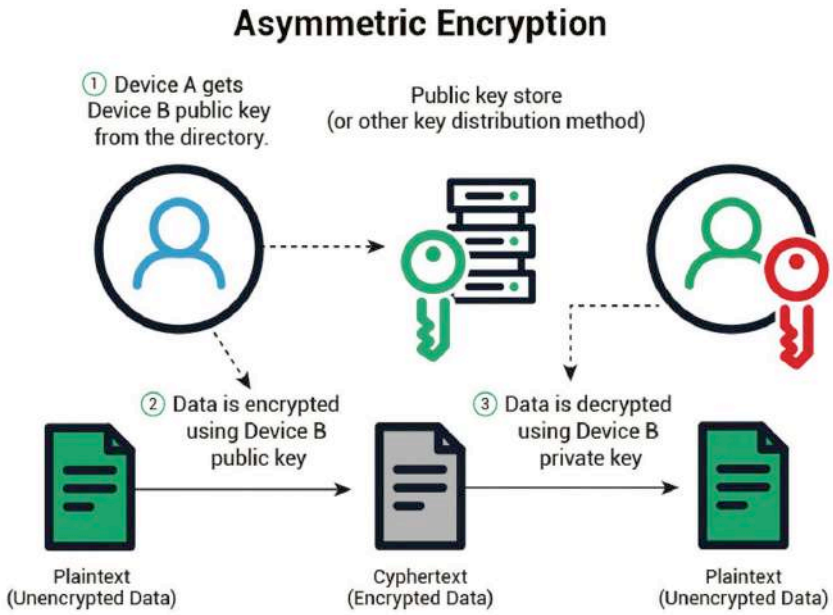
Quantum computers, on the other hand, can do many related calculations simultaneously to arrive at an overall conclusion in one operation. This ability becomes very concerning in cybersecurity and encryption because it exponentially speeds up public key and brute force attacks.

Data encryption & its vulnerabilities

These quantum algorithms, specifically Shor's and Grover's, will supply a way to break both asymmetric and symmetric style encryptions. Asymmetric encryption, in this case, refers to the key agreement used to set up the encryption, not the encryption algorithm itself. These key agreements allow endpoints to share a public key insecurely and generate private keys to encrypt and decrypt data. This method is widely depended upon because

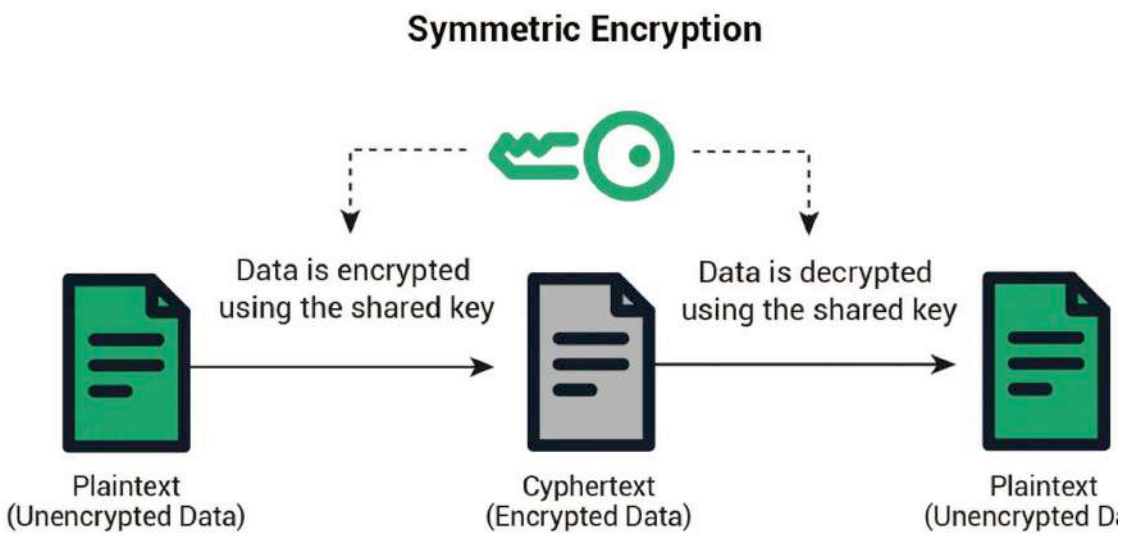
it enables endpoints to have no previous knowledge of each other, making it very flexible and easy to set up. It is also important to note that these agreements are used in various instances (i.e., digital signatures), and the following points apply to all.

On the other hand, symmetric style encryptions are widely accepted as more resistant to quantum computing attacks because there is no public key to manipulate into a private key. Only a private key exists that must be securely stored on the encrypting and decrypting devices or securely provided to the encryption algorithm when needed.



Today, these asymmetric algorithms are safe because the calculations needed to break them take so long to execute that it is not a practical attack vector for cybercriminals. Quantum computers, on the other hand, can perform the factorisation and logarithmic algorithms needed to break asymmetric algorithms at an alarmingly fast rate, making them an efficient attack vector. Cybercriminals using quantum computing will target asymmetric algorithms first, not only because it is so widely used but also because they can manipulate a public key to get a private key.

This style of encryption, in turn, is typically compromised by brute force methods. Even when using key chaining, once one key is exposed, one can apply the same chaining to that key to gain other keys. These brute force methods are currently linear operations where conventional computers guess keys one at a time until they recognise the data as decrypted (for reference, this style of brute force would take the Fugaku supercomputer an average of 23 trillion years to perform on an AES-128 encrypted payload). Contrastingly, quantum computers can try every encryption key in parallel and reveal the data in hours instead of years.



Advanced computing requires advanced safeguards

These problems of tomorrow call for a unique solution unlike what is in use today. There are two strong possibilities for this solution; it could not use encryption at all or could manage encryption keys in a way that removes quantum vulnerabilities.

The first possibility may seem farfetched as anything outside encryption seems otherworldly, but it would be relatively simple in theory to produce an alternative quantum-resistant technology. Drawing upon successful schemes of the past, which have proven to be some of the most secure data protection methods, the one-time pad would be a great model to work off.

Developed in WWI, the one-time pad takes data protection to the byte level, shifting each byte of data by a different random amount instead of altering an entire piece of data with a single key as encryption does. It does this by using a sample of random data that is the same length as the data being secured and XORing each byte of both data sets to get a secure third string of bytes. This byte-level replacement of actual data for random data is robust and eliminates quantum computers' advantage of guessing a key to decrypt an entire payload. Guessing of keys only works because there are recognisable clues in a payload that verifies if the guessed key is correct or not. Brute forcing at the byte level becomes astronomically harder than verifying an entire payload because of the lack of contextual clues.

The trouble with the one-time pad is that the random data must match the data length and somehow get to both sides for the securing and un-securing actions. These are complex challenges to overcome, primarily when the basis of most modern systems are zero-knowledge and session handshaking. However, the new push for zero-trust full-knowledge environments and the use of secure deterministic random bit generators (DRBGs) make these challenges manageable. They enable secure endpoint relationships to persist between sessions and simultaneous generation of random data at any length, respectively.

The second possibility of managing keys might seem like a solution already offered, but the popular answers are anything but quantum resistant. This solution takes the process of key generation down below the level of encryption and removes all third parties and humans from the mix. It would eliminate the need to share public/private keys by systematically generating random single-use encryption keys when needed, only keeping them around while in use and never reusing them.

This method allows keys to change with every transmission instead of the session-based approach of TLS and other securities. Also, making the keys random means there is no basis on the data or any other key, eliminating the links that quantum computing manipulates. Creating such a method seems like a tall order, but again it only takes a shifting perspective for the proposition to seem obtainable. The generation of the keys via DRBGs would allow two paired endpoints to generate encryption keys simultaneously without ever sending any key information.

Removing the need to send a public key eliminates the most significant attack surface quantum computing has on encryption. The problematic piece to figure out is how do these two endpoints synchronise. Drawing again on the fact that environments are driving towards zero-trust with full knowledge, the seeding of the DRBGs could draw from knowledge both endpoints already know, thus eliminating credential sharing and handshaking. Also, if the secure relationship persists between sessions, the registration of endpoints could be more secure and stringent than today's since it would only need to happen once during the first use of an endpoint.

These two solutions can even be combined using byte-level substitution for highly sensitive pieces of data and random key generation for larger, less sensitive data. This combined approach would be a highly secure yet efficient solution with endless flexibility to accommodate any environment.

Readily available quantum computing is on its way, and the time is now to start future-proofing systems for its arrival. Waiting until we have the first quantum computing breach is too late. Gone are the days of monitoring being enough; quantum computing has the power to obliterate an environment within seconds of discovering a vulnerability.

There will not be enough time to quarantine and take the reactive steps relied upon currently. Data needs to be the focus of security, and that security needs to anticipate the power of quantum computing. ■

BLOCKAPT™

BlockAPT are proud to announce our visit to the **Republic of Congo** to speak at the Digital Forum.

Tune in to hear about technological innovation, data and cybersecurity at the heart of digital transformation.

Marco Essomba
(Founder & CTO)

Raj Meghani
(Chief Marketing Officer)

16 - 18 FEBRUARY 2022
Hotel Atlantic Palace
1212 Avenue Charles de Gaulle, Pointe-Noire

LIVRET DE PRESENTATION

FORUM NUMERIQUE CONGO
3ème EDITION

info@blockapt.com

www.blockapt.com

Governance: A destination?

Author: Sarb Sembhi

Introduction

As security professionals, no matter which event or type of event we go to, no matter how long it is, whether it's a webinar, panel discussion, or a three-five-day expo and conference, the one topic which either crops up time and time again directly or indirectly, will be governance. And if it doesn't, there's something amiss there.

In its early immature days' cybersecurity was seen as a low-level technical activity, but as standards, regulations and security risk management have matured, so has the importance of governance in cybersecurity. This has been good for cybersecurity professionals, as it has been a contributor to taking security from the basement to the board room.

BIO

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 and is currently the CISO at AirEye.

Cybersecurity governance means many things to many people, one only has to do an internet search for the topic and compare the top 10 items to realise that either the search engine is useless, or the content, or both! We

have certifications, standards, frameworks, books, etc. all to help us figure out what we should be doing. However, what is most important is what cybersecurity governance should mean in your organisation, since most of the literature tells you to make it work for you and your organisation.

I'm currently working on some content on governance good practices, but I wanted to take this opportunity to cover things from a completely different perspective. In this short article, I want to cover two separate issues:

- The first is around the perception of governance and good practice which speakers at events give about governance and successes of good practice.
- The second is the one single challenge I've worked with clients on from my consultant days which helped get governance starting to work well in their organisations.

The biggest CISO challenge

Over the years as a consultant, I've spoken to many CISOs who work hard, doing long hours to do everything they believe they are supposed to do to meet the role. The difficulty of every role (not just that of a CISO) is that no matter how bad things are, it is not possible to admit to sharing the reality. Those who were able to do so, were only able to do so because the support they had was good enough for them to communicate what wasn't working for them.

Today's CISOs have so much expected from them in business environments which are more demanding than ever before. It would be very unprofessional of any CISO to publicly talk about how bad things are

where they work, but unfortunately, I sometimes think that we have completely taken a wrong turn.

What I mean by that is, CISOs talk about topics like controls, risk, threats, governance, etc. as if they have those things completely solved. We talk about things at events on how things should be in terms of good practices, rather than how they actually are in reality.

This is not to say that we shouldn't be talking about good practice, or that all CISOs are doing a bad job, but that when we only talk about how things should be we continue to create the myth that everyone is doing a great job at creating and following good practices.

A friend of mine used who used to be a CISO and then became a consultant (for one of the big four) was amazed that those same CISOs who spoke about all the good work they were doing in their organisations wanted to call this consultant (ex-peer) in to implement that very same good practice which was supposedly already in place. This isn't the picture everywhere, but it does illustrate that CISOs do talk things up. There is a time and place for that. There is nothing wrong with bringing consultants in to implement good governance practices, but as attendees, we mustn't believe that perhaps we are the only ones who don't have a handle on governance.

As speakers and participants, we should spend a little more time talking about what can and does go wrong and how we deal with those situations. Spending more time on how to deal with what goes wrong is probably more beneficial than "We're all doing great if we do this". We would do our industry and colleagues a greater service by bringing back some of the realities we encountered, are still encountering and contend with on a day-to-day basis and the strategies and approaches we deployed to overcome them.

We need more war stories on all aspects of cybersecurity, but especially around governance, as it is such a hard practice to achieve. As an industry we need to look at how we can talk about breaches and what we can learn from the very largest ones, rather than just be glad that it wasn't us, without knowing why it wasn't us, and what we can do to be enable our organisation to get its governance right to be able to respond in the best way we can.

The single biggest governance challenge

The many standards, frameworks, books and articles on the internet pointing to so many really useful things that to pick one or two as the ones which represents what good is, would not be right and perhaps not fit into what the reader needs for their organisation. However, what I believe is useful to consider, regardless of which standard of framework your organisation uses, are some of the challenges to getting cyber security governance right.

Again, there are many articles on the challenges, but the two key ones which appear not just in many lists, but also as topics in their own right within the standards and frameworks are Transparency and Accountability. They are both related and connected, but out of the two the one that is hard to get right as it is such a big topic is Accountability.

One of the best examples of what to do to get accountability right (in principle) is on the UK regulator Information Commissioner's Office website. Not only does it provide information on security outcomes in relation to data

protection, but it has information around accountability and governance. The examples and example documents and references to why you need to do what you need to do are all useful.

Done well, accountability provides assurance for governance and eases transparency, as it makes it clearer in terms of what can be shared, who with and what they can do with it. Many of the outputs which need to be completed to achieve accountability contribute to the outcomes of achieving governance on data protection.

The reasons I chose data protection accountability as the model to discuss governance include:

- It is a topic that is still hot for many organisations.
- Many security people are now in data protection roles.
- The data protection community has produced some good outputs on examples of accountability.

I'm sure that many would agree that accountability is very important when it comes to cybersecurity governance, but they may disagree that it is the single biggest challenge. However, although I identified accountability as one of the two key challenges in current literature, I believe that there is an even bigger challenge to cybersecurity governance. But that challenge is not discussed much in articles, standards or frameworks.

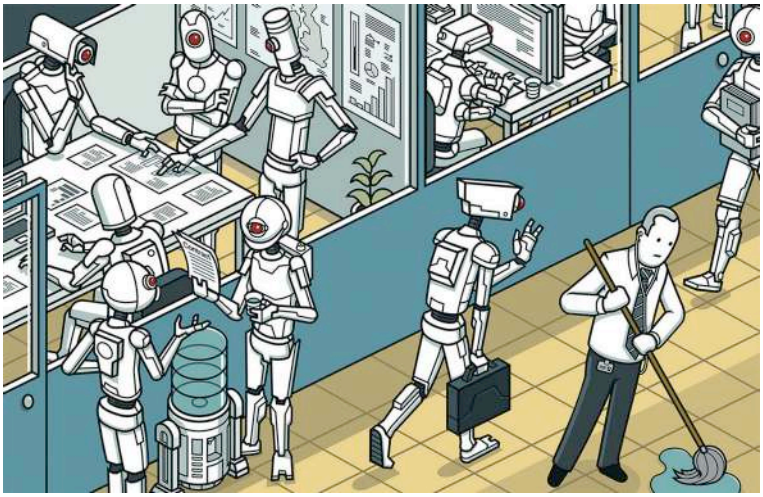
The greatest challenge to not achieving governance (let alone good governance) is often not doing anything, due to not being able to get it right the first time since there seems to be so much to do and everyone else seems to be doing such a good job at it. We need to get beyond what others are doing or not doing, but to look at what we need to do, and just do it, get started and start to get it right along the way.

Most organisations have some governance in place, but not all of them have it aligned for cybersecurity, and the push to improve it or get it right may have to come from the CISO. So, the greatest challenge to cybersecurity governance in several organisations I've worked with, was thinking of it as a destination rather than a journey. For example, I once worked for an organisation where they hadn't registered with the ICO as a data processor, because they wanted to get things right first, then they would register. What they didn't realise was that by not registering they were breaking the law.

Yes, governance is big and can involve a lot of people, processes, and time, but whatever we do, we should get started on that journey by doing something. Or, to use another analogy, we need to eat the elephant by taking that first bite. Take whatever works for you, but don't let what you hear about how well others (on stage, or in webinars, or articles) are doing stop you from getting started and doing something. ■

Plugging the cyber skills Gap.

Author: **Dr. Andrea Cullen**



It is projected that half of our jobs will be replaced by AI, robots, and technology by 2025, according to the World Economic Forum. On top of this, approximately 1 million people were made redundant during the first year of the COVID-19 pandemic, and current unemployment levels are still higher than at the start of 2020. Finally, it is estimated that the cyber industry will need an additional 3.5 million qualified professionals by 2023, so it's clear to see we're approaching a potential employment crisis. The pandemic has changed the world of work with far-reaching and potentially permanent effects, crippling certain industries which may never fully recover. We have a growing number of adults in the UK who need to reskill, and an industry crying out for new, diverse talent.

Drawing from my professional background in cybersecurity consultation, education and recruitment, I have seen the opportunity to help adults in need of a career change transition into the world of cybersecurity.

There is a market to re-skill adults into cybersecurity professionals entirely online, within 6 months, and with no up-front costs. Believe it or not, there are cyber bootcamps, like CAPSLOCK, which delivers cyber education via a rigorous curriculum in collaboration with some of the UK's largest cyber employers. This ensures that learners are graduating with the skills and experience that UK cyber employers need, rather than just theoretical knowledge from a textbook.

There is a need to plug the gap of cyber fundamentals, including business understanding, cyber ethics and culture, governance, risk and compliance, offensive and defensive security, and cloud security. There is

a need for our CISOs of tomorrow to work towards solving real-world cyber security problems working as part of a team. There is a need to encourage, engage, explore, innovate - all with confidence.

As with many industries, cyber suffers from a stark lack of diversity in many forms, including gender, ethnicity, and neurodiversity. Starting to remedy this problem would help to close the cyber skills gap, which is why increasing the diversity of the cyber workforce should be high on a company's list of priorities.

The way I see it, the more our cyber workforce reflects the diversity of our society, the better our cyber solutions will be. It is imperative to remove the traditional barriers which have prevented people of all genders, ethnic backgrounds and walks of life from entering the cyber industry. There are huge amounts of untapped talent in these demographics, and the goal should be to help people access the education and support that will unlock their potential.

One initiative to make cyber education more accessible is by removing the financial barriers to retraining. Rather than charging learners a tuition fee upfront, they are required to pay back a percentage of their income after completing the course, but only if they land a job with a good salary.

This financial model is known as an Income Share Agreement and it opens the door to people who need to re-skill but can't afford huge up-front fees or traditional loan debt.

BIO

Andrea has worked within the cyber sector for almost 20 years. She is a co-founder at CAPSLOCK where she is a lead tutor and Chief Innovation and Research Officer (CIRO). Andrea is an experienced senior information security professional, who has worked extensively in industry and as a senior academic. She is also currently a visiting fellow at the University of Bradford supervising PhD studies and inputting into research projects.

The underlying point here is that we're simply not going to plug the cyber skills gap by letting history repeat itself. We have to bring more diverse voices into the industry and shake up traditional models of education.

There are more accessible ways to enter the cybersecurity industry, allowing UK adults to re-skill in an efficient, thorough, and affordable manner. ■

What's best for you: In-house cybersecurity or the MSSP route?

Author: Raj Meghani

The dilemma to manage your security posture via a cybersecurity in-house team or outsourcing to an MSSP is a decision that often has cost at the very heart of it.

Both options provide benefits and have their downsides, but readers beware – sometimes it just makes logical sense to opt for one over the other depending on how mature and big your business is. As the saying goes – one size does not fit all.

Building an in-house cybersecurity team can be seen as an extension to the traditional IT department set up. The responsibilities and skill sets are there to manage the typical infrastructure needs of the business from server and database management, routine maintenance, email security through to web threat prevention. The business retains control. The business reputation is intact and protected by the data it holds securely having the flexibility to manage its resources as, when, and how it needs without having to go via third parties.

But we all know keeping on top of security comes with hiring subject matter experts (CISOs) who are more than ever in demand (thanks to the cybersecurity skills shortage) and they come at a cost.

On the flip side, say hello to your new/extended Managed Security Service Provider. Included are 24/7 security monitoring, extensive knowledge of the latest hacks, a defence in depth approach, potential cost savings and the ability to scale with your business with minimal disruption to your business. Faster response times means a faster call to action to block threats and mitigate against reputational damage, fines, legal challenges, etc. It also enables your teams to focus on developing the business and it's core competencies.

BIO

Raj Meghani is the Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.
Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank.
Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 20 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.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

Do you take control and build a team to manage it all in-house or do you leave it to the security experts who offer a fully managed MSSP service? Whichever option is taken, cybersecurity today with the increasing number, frequency, sophistication of cyber breaches and lack of governance makes it onto the boardroom agenda.

So let's get down to the nuts and bolts – what's the case for in-house cybersecurity team vs outsourcing?

The case for in-house cybersecurity – but beware:

One word which is seen as a key advantage point – is having total **CONTROL** of your network systems, resources, software, business priorities, data and so on. The agility with which management can make decisions to flex their resources across broader IT areas helps retain the knowledge in house and provides for a conducive, collaborative culture.

KNOWLEDGE TRANSFER is retained in the business as you invest in training, job shadowing and upskilling individuals. They are familiar with your disparate technologies, legacy system issues, operational processes and configuration protocols including change control. They are also more likely to share experiences whilst problem solving, allowing management to have total visibility on ROI metrics on productivity and resource utilisation efficiency.

With the in-house team comes immediate **ACCESS** to other teams across the business. Time is of the essence when it comes to cybersecurity threats and breaches so being on-site often expedites communication channels and minimises downtime without having to rely on a third-party involvement.

However, having an in-house cybersecurity team does not come without its own set of challenges.

The big one which springs to mind is that it can be **EXPENSIVE** – you need to have skilled cybersecurity expertise and rely on them to monitor, manage and orchestrate the whole of your security ecosystem.

Whilst the in-house teams are usually small in number, there is an additional challenge in **RETAINING** them as loyalty for some individuals is only as good as the highest salary they can secure.

Add to that the potential lack of **SECURITY TOOLS** or the lack of budget to develop bespoke software enabling them to manage their security ecosystem from a single interface without having to toggle or keep on top of multiple different systems or applications. With this lack of automation comes manual processes, manual checks - ergo room for human error which can result in costly mistakes notwithstanding the reputational damage it can cause.

Cybersecurity hackers don't work on a typical 5-day week from 09:00 – 17:00 – it doesn't matter if it's night or day. If your business is operating in the UK or globally, then you will need to ensure your staff can cover 24/7 monitoring and support. Good luck managing that one.

Let's not kid ourselves. Establishing an in-house cybersecurity team outside of the expense takes **EFFORT** and **TIME**. Research indicates that getting the necessary physical infrastructure, hardware, security toolkits, resources, training, policies and procedures, etc to the point of having an in-house team up and running could take the best part of 6 to 12 months. Rapid deployment is not an option here, unlike the MSSP model, so the business will need to consider what steps it has in place to protect itself from cyber threats during this time.

"Caveat Emptor – one size does not fit all.
It may be prudent to see if there is a balance between both worlds"

– Raj Meghani.

The case for outsourcing to an MSSP – but beware:

Key to partnering with an MSSP is the **COST SAVINGS** that can be achieved – albeit with the upfront, initial payment it may not necessarily feel or look that way! With a specialised and experienced security team/analysts on hand around the clock, investment in up-to-date security toolkits, etc, it provides a more economical way of securing your business given no overhead expenses.

Time is of the essence as we continue to see an increasing number of cyberattacks such as Ransomware – with the MSSP, your business benefits from **RAPID DEPLOYMENT** offering 24/7 monitoring, threat detection and response, web & email security, endpoint protection, vulnerability scanning, incident response management alongside detailed reporting to support governance and compliance requirements. An MSSP's infrastructure and

full tech stack is already set up to onboard and manage new clients with minimal disruption to the business as this is their core focus and area of expertise. So, we are talking weeks here – not months. It's what they do day in and out.

Added to this is the point that MSSPs can be more flexible and agile to align to your business' growth, unlike the in-house option where you would be up against resourcing constraints. **SCALABILITY** is a key benefit here, MSSP's will always collaborate with their client to ensure a win-win situation for both parties involved. Their experience working with other clients gives them a much bigger pool in which to analyse the latest hacker attempts, trend analysis, and take proactive action to mitigate against cyber-attacks.

Most businesses even with an in-house cybersecurity team will struggle to keep abreast with the latest or emerging threats, industry trends, up to date security technologies and policies, legislative changes, risk exposure, incident response management, etc whilst firefighting and keeping afloat from alert fatigue. The **EXPERTISE** and **BANDWIDTH** of the MSSP place them well ahead of the curve to benefit from new ways of working, integration of new applications to help automate workflow processes, etc.

But having an MSSP as an extended part of your security team also has its challenges. Dealing with a third-party provider is not as simple as walking to your security team in house to discuss a key issue. There's a **'MIDDLEMAN'** now within your communication channel which is most likely to be via email or the phone.

There is often a **LEAD-TIME** associated with query/support responses as they are managed through a ticketing system. Your SLA will stipulate response times, but chances are it won't be immediate if you need an expert to address your specific problem. You will need to be prepared and patient if you are used to having someone jump on demand.

So, which one is best? Well, my view is that there isn't one solution which fits all. If you are an SME for example, both cases above are not a feasible or viable option – unless as an MSSP they can offer a fully outsourced service tailored to meet SMEs needs which is genuinely affordable and gives them peace of mind.

Considering the increasing transition towards cloud migration, sophistication and frequency of emerging threats, the cybersecurity skills shortage and increasing threat surface as the digital footprint of businesses continue to evolve and grow, it may be prudent to see if there is a balance between both worlds. ■

Is our memory becoming a melting-pot of "unknown knowns"?

Author: Laurent Chrzanovski

Last year, in a socio-psychological essay in memory of Donald Rumsfeld, the popular philosopher, Slavoj Zizek recalled the 2002 speech of the late US Defence Secretary prior to the Iraq War. In this talk, intentionally or not, Rumsfeld mentioned essential concepts of ancient philosophy, i.e., the *unknown unknowns,* the *known unknowns* and the *known knowns*. Yet a very recently born concept was missing: the ***unknown knowns.***

As the German philosopher Jürgen Habermas (2) pointed out since 2020, our mind is so saturated with information that our memory is full of knowns we have just... forgotten. This phenomenon is deeply rooted within the *"media-connected individuals",* i.e., most of us in developed countries. The quantity of daily "fresh news" absorbed invades our critical mind and pushes into oblivion older information, often vital, mainly if one had not to apply in real life all the knowledge received.

Coming to the cybersecurity domain, the very root of the problem generating the human behaviours just described by philosophers has become a real concern. The *"over-information"* problem (measured by the quantity of materials uploaded and then downloaded/read on the web each minute, worldwide) is subject to no less than a whole chapter in last week's released World Economic Forum's *Global Cybersecurity Outlook 2022* (3).

New data created in one minute.
© Global Cybersecurity Outlook 2022, p. 12, figure 3

From the top to the bottom: business experts versus security experts

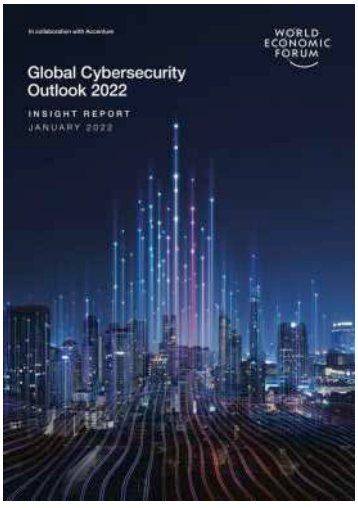
The WEF report underlines, within the "unknown knowns", the average gap between the board members ("business executives") confidence on the policies and in consequence by the systems used within their company and the security teams ("security-focused executives") fears is bigger than ever, a topic around which a large chapter of the report is built "Cyber leaders are increasingly finding themselves in a precarious position as the gap between business and security leaders widens".

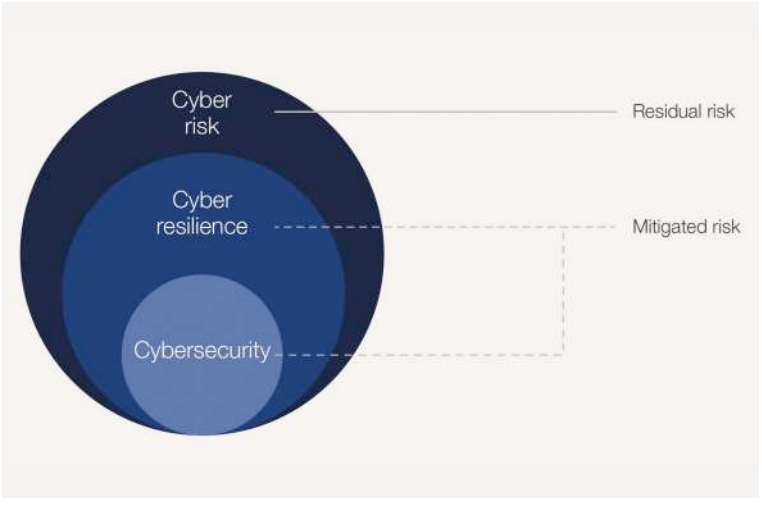
Confidence in priority and integration of cyber resilience, business versus security specialists. © Global Cybersecurity Outlook 2022, p. 19-20

The outlook underlines a series of very important measures to be taken immediately in all business sectors, to bridge this gap which, as **Raj Meghani references in her previous articles as a 'mindset and cultural change',** is one of the principal reasons of the overall weakness observed by the success of very primitive forms of cyberattacks during the pandemic (phishing, scams, etc.).

Again, the focal point is one of the topics we have covered since way back: the lack of including the CISO and/or the CSO among the board members or having their compulsory presence at decisional meetings creates cybersecurity consequences.

Moreover, the biggest difference of *modus cogitandi* between business leaders and security specialists and the source of many problems, is an ever-growing misunderstanding by the business specialists between cybersecurity and cyber resilience: most business leaders consider the two domains as a whole and do not correlate the differences, the specificities and the needs of each of them, exactly as **Sarb Sembhi's article in this issue** within the wider frame of cybersecurity governance.





Relations between cyber risk, cyber resilience and cybersecurity. © Global Cybersecurity Outlook 2022, p. 16

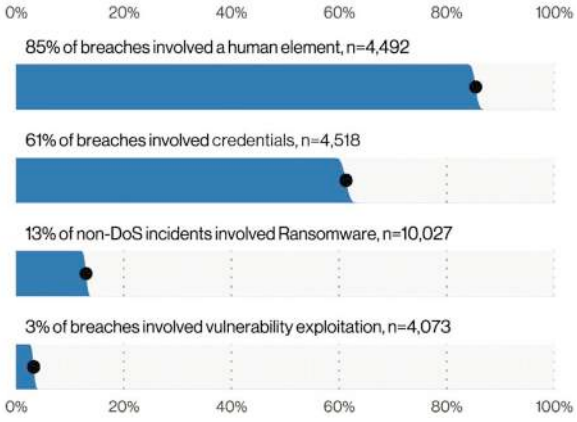
The 2021 record quantity of successful cyberattacks takes its roots, according to all reports, in a whole series of unappropriated decisions during lockdown times, added with a persistent transformation of many jobs going from office working to smart working without radical security changes.

The WEF outlook and the other reports also mention that we reached a critical point of cybersecurity jobs shortage, which could be reduced following the clues given **in this issue by Dr. Andrea Cullen**. Yet, on this topic, we should mitigate a little bit the numbers given by Forbes, the WEF and others as they also reflect the incapacity of too many learning institutions to deliver much more wide-spectrum buildings, exactly as those described by **Marco Essomba in a previous issue** of our publication: assuming that cybersecurity has seven stacks, the new generation of cybersecurity experts should be able to master at least two if not three of them, helped by the new technologies available on the market.

All the above-mentioned factors will have severe consequences on the insurance costs, which is the third of the 2022 Top-10 cybersecurity challenges pointed out by E. Saygeh in his yearly predictions published by Forbes (4). Many insurances, whose premiums for coverage have skyrocketed in 2021, will refuse to accept companies which do not have a strict and comprehensive cybersecurity policy, technological as well as human, starting with continuous awareness-raising training delivered to every single employee.

From the bottom to the top: a constant lack of all-inclusive all-level awareness training

The costs of incidents for businesses, during the pandemic years, reached records. As Verizon's *Data Breach Investigations Report 2021* (5) pointed out, 85% of the breaches involved the *"human weak link"*.



Verizon, Data Breach Investigations Report 2021, fig. 7, p.7

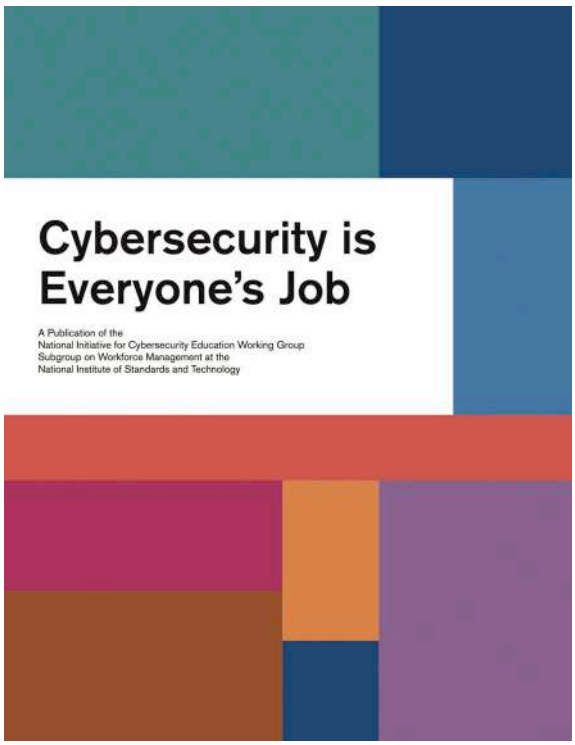
BIO

With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu State University and holds postdoctoral courses within several major EU Universities. He is the author/editor of 32 books, of more than 150 scientific articles and of as many general-public articles.

In the frame of cybersecurity, Laurent Chrzanovski is member and contractual consultant of the ITU roster of experts. He founded and manages the yearly "Cybersecurity Dialogues" PPP Congresses (Romania, Italy, Switzerland), organized in partnership with the highest international and national authorities . In the same spirit and with the same partnerships, he is co-founder and redactor-in-chief of the first cyber security awareness quarterly journal, Cybersecurity Trends, published in Romanian language since 2015, with English and in Italian versions since 2017. His main domains of study are focused on the relationship between the human behaviours and the digital world as well as the assurance of finding the right balance between security and privacy for the e-citizens.

Despite being a major worry for all sectors of business, very few except security companies, high-tech or luxury branches undertook the long-lasting task of educating all the staff, from the night cleaner to the CEO, on a regular base. As Clive Madders (6) pointed out recently, it is only through cultivating a culture of cybersecurity awareness that a company could really become safe. Besides the necessary technology, the author insists on the fact that *"Fortifying the front-line (read: the employees) is often the best method of defence"*, recalling the poor use made by too many companies of the vital guidelines published by the NIST already in 2018, *"Cybersecurity is everyone's job"* (7).

The consequences of years of badly-distributed security awareness, in the form of pdf documents or one-page adverts, have been widely unveiled during the pandemics. These "knowns" have been largely forgotten by too many remote-working employees, who exchanged passwords, user ids, clicked on malicious links and opened any kind of phishing mail. Stress

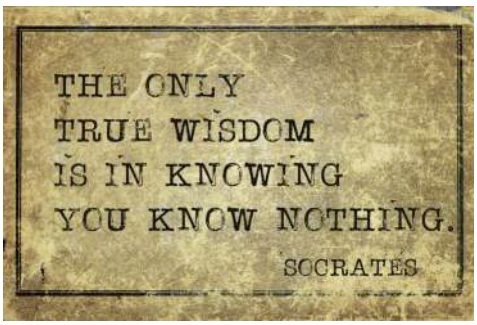


coupled with ignorance, as it is well underlined by the just released study *"Why employees violate cybersecurity policies"* made by Harvard University (8), made that possible. In the context of stress, the three main reasons recognised by the employees who bypassed the security policies were:

- "to better accomplish tasks for my job"
- "to get something I needed"
- "to help others get their work done"

To better understand the Harvard research, a more in-depth psychological research entitled *"The Role of User Behaviour in Improving Cyber Security Management"* (9) is a must-read. It allows us to understand, taking apart the "malign insider", to understand the different categories of egos each human employee can have, leading to major mistakes and hence unsecure behaviours, running to over-confidence to impulsiveness and to an ever-growing desire to be pro-active (i.e. "future thinking") to face better the stress linked to the quantity of demands daily received by a direct superior. All those factors lead to forgetting the basics and not to apply security policies which are too often very poorly explained and hence understood since the day of their implementation.

To end where we started, there no more luxury time to try to remember the *"unknown knowns"*. To cope with the ever-growing quantity of new technologies we use as well as every single product's specific way of use, strengths and of course weaknesses there is a need of a fresh, new strategy (even by gamification) and bottom to



top awareness building, starting with the weakest tool, the smartphone. Employees, if well coached, should find satisfaction by feeling they are learning something very useful. If starting from the Socratic paradox described by Plato: **"ἔν οἶδα ὅτι οὐδὲν οἶδα" (all I know is that I know nothing)**, i.e., an attitude of humility coupled with open-mindedness, employees will realise how to evolve and to feel secure both in their job as well as in their personal life, by learning about cybersecurity. The role of the business leaders will also have to change, rewarding teams and individuals not only for productivity but also for well-applying security policies. ■

(1) Slavoj Zizek: How Donald Rumsfeld's catastrophic 'unknown unknowns' approach on Iraq can help us deal with Covid crisis, RT, 04.07.2021
https://www.rt.com/op-ed/528359-donald-rumsfeld-iraq-covid/

(2) Jürgen Habermas über Corona: „So viel Wissen über unser Nichtwissen gab es noch nie", Frankfurter Rundschau 10.04.2020
https://www.fr.de/kultur/gesellschaft/juergen-habermas-coronavirus-krise-covid19-interview-13642491.html

(3) World Economic Forum, Global Cybersecurity Outlook 2022, January 2022
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

(4) E. Saygeh, Predicting What 2022 Holds For Cybersecurity, Forbes, January 6, 2022
https://www.forbes.com/sites/emilsayegh/2022/01/06/predicting-what-2022-holds-for-cybersecurity/

(5) Verizon, Data Breach Investigations Report 2021. DBIR, Fall 2021
https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report

(6) Clive Madders, Protect Your Organization by Cultivating a Culture of Cybersecurity Awareness, December 28, 2021
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/protect-your-organization-by-cultivating-a-culture-of-cybersecurity-awareness/

(7) NIST, Cybersecurity is Everyone's Job, 2018
https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job

(8) C. Posey, M. Schoss, Research: Why Employees Violate Cybersecurity Policies, Harvard Business Review, January 20, 2022
https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies

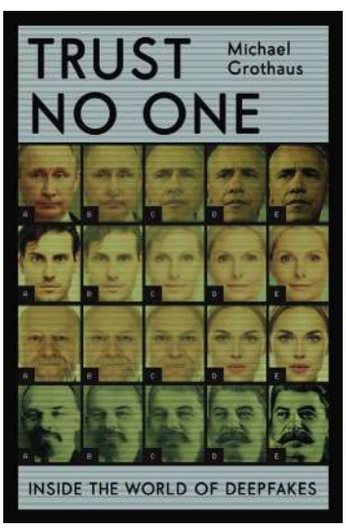
(9) A.A. Moustafa, A. Bello and A. Maurushat, The Role of User Behaviour in Improving Cyber Security Management, Frontiers in Psychology 12 (2021),
https://www.frontiersin.org/article/10.3389/fpsyg.2021.561011


BLOCKAPT™
Boost Client SecOps.
Single platform experience
SIEM | SOAR | XDR | IR
Vendor agnostic, centrally managed
Command and Control security
platform for MSSPs with full multi-tenancy.
info@blockapt.com
blockapt.com

Book Review

Review of Michael Grothaus's – "Trust No One: Inside the World of Deepfakes". *London (Hodder & Stoughton), 2021, 279 p.*

Author: Laurent Chrzanovski



In a world full of *"information",* the clues for catching the attention of the digital readers, often accessing news through their tiny smartphone screen, is a combination of an image followed by a voluntary exaggerated title. Most people, switching from a piece of "news" to another, will just keep in mind this binary association.

In this frame, the most eye-catching is the image and the more emotionally provocative is the title which are the two keys of success, no matter if the text of the article itself is much more balanced.

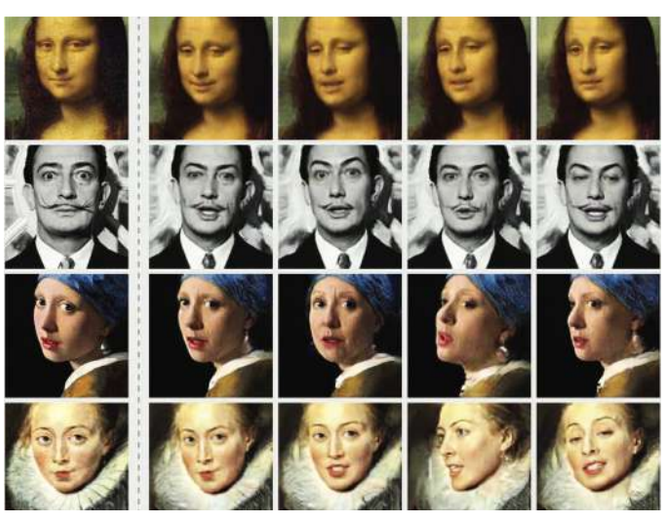
Deepfaking images is a technique born almost in contemporary with photography - and has been used and abused by some regimes - we can recall the Soviet press removing from official pictures all early times communists executed by Stalin's order, this technique evolved dramatically in the last decade.

The author realised the importance and the quality reached today by deepfakers when he asked a friend to *"bring back to life"* his father, deceased in 1998, by making a clip *"as if it was shot today."* This to be done using as a base old VHS videos and extremely sophisticated artificial intelligence tools. The result was more than astonishing, as even the quality of the clip was in ultra-high definition compared to the source.

As journalist, Michael Grothaus decided to investigate the phenomenon and interviewed specialists using the latest available tools for creating artificial pictures and video clips, with the original voice of each personage included. But the most interesting part of the book, to be read as a dark novel, is the increasingly huge part taken by deepfakes within the sheer number of images everyone accesses on the net daily. The perfect narrative, the author's style and the logical sequence of the chapters raised this volume as a best-seller, praised by the most important journals (1) (2).

The most important finding is that we passed the age of deepfake for modelling opinions. In other words, where deepfakes can be used to try to destroy a CEO reputation or in the attempt of influencing an election (hence part of psy-ops). On this topic, the extraordinary campaign made by RepresentUS to warn Americans on deepfakes, with the 100% AI-created broadcasted declarations of President Putin and Chairman Kim Jong-Un, had a formidable effect on boosting the citizen's awareness (3).

We live in a much more perverse world: deepfakes are now commonly used not to change people's minds: as Grothaus articulates perfectly: *"it is about feeding them with what they want",* being often based on narcissism, winning the fear of death, inducing sentiment of a fulfilled sexuality or a mastered self-control. This can turn the digital world so perverse that our innate senses of searching for fact, truth and trust could be seriously undermined, having huge effects on all the aspects of our daily physical life and social interactions. ■

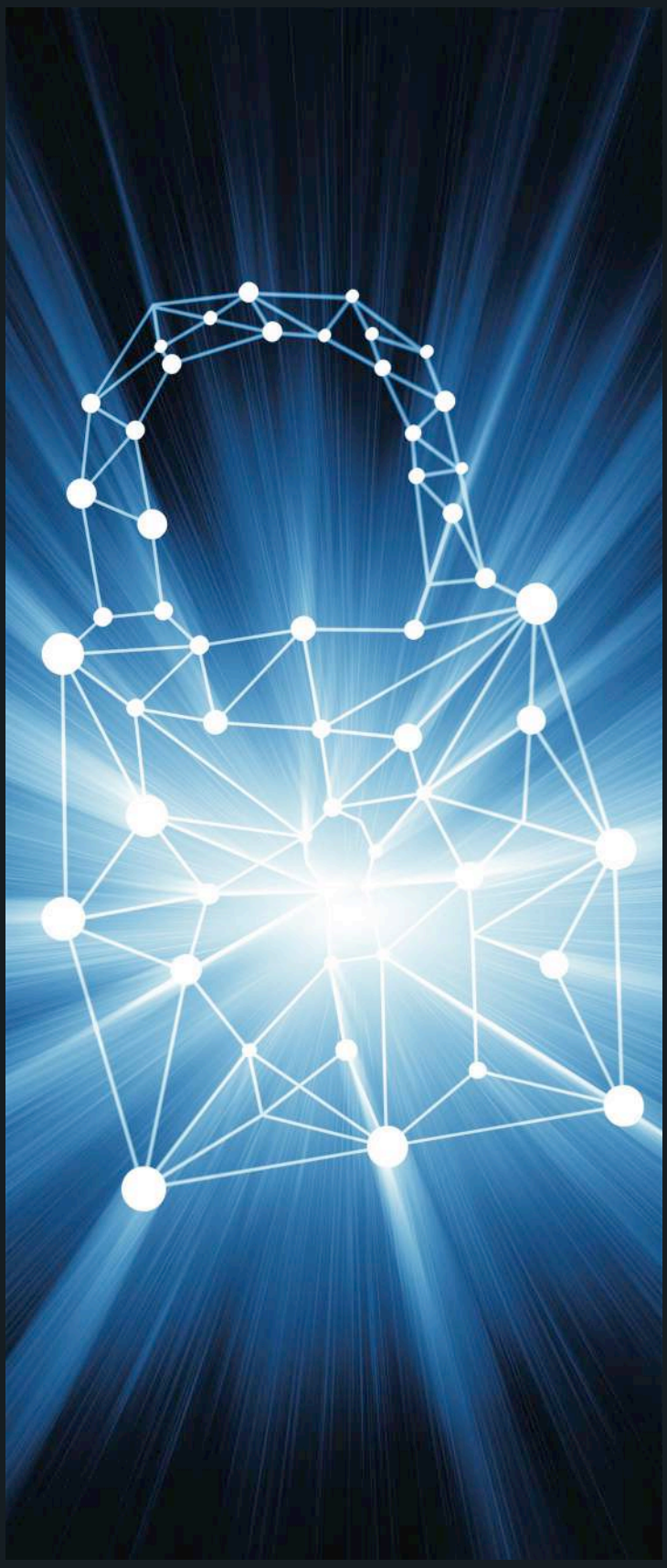


(1) Peter Pomerantsev, Trust No One: Inside the World of Deepfakes by Michael Grothaus review – disinformation's superweapon, The Guardian, 16.12.2021
https://www.theguardian.com/books/2021/dec/16/trust-no-one-inside-the-world-of-deepfakes-by-michael-grothaus-review-disinformations-superweapon

(2) Shanti Das, Trust No One by Michael Grothaus review — an alarming look at deepfakes, The Times, 07.11.2021
https://www.thetimes.co.uk/article/trust-no-one-by-michael-grothaus-review-an-alarming-look-at-deepfakes-q233pldf6

(3) Karen Hao, Deepfake Putin is here to warn Americans about their self-inflicted doom, Harvard Technology Review 29.09.2020
https://www.technologyreview.com/2020/09/29/1009098/ai-deepfake-putin-kim-jong-un-us-election/

Cybersecurity Trends



A publication

web for your 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. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

BlockAPT Limited
14 East Bay Lane,
The Press Centre, Here East,
London. E20 3BS
United Kingdom

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

BLOCKAPT™