Cybersecurity Trends

UK edition n.1 / 2023

Quantum Security...
Compliance and Governance...
2023 Predictions....

IN THE SPOTLIGHT
with CHUCK BROOKS

BLOCKAPT™

ONE INTELLIGENT PLATFORM

ONE POINT OF TRUTH

ONE UNIFIED VIEW

blockapt.com

Contents

EDITORIAL

COMPLIANCE & GOVERNANCE IN A RISKY WORLD

IN THE SPOTLIGHT - CHUCK BROOKS

QUANTUM SECURITY: A PARADIGM SHIFT

CYBERSECURITY PREDICTIONS - 2023

The stakes have never been higher....

Authors: **Raj Meghani, Marco Essomba, Laurent Chrzanovski**

Welcome to our first edition in 2023 of Cybersecurity Trends UK, where in the world we operate in, the stakes have never been higher. In today's risky world, compliance and governance are no longer optional, they are essential components of cybersecurity risk management. But compliance alone is not enough to keep up with the ever-evolving threat landscape.

As we enter the age of quantum computing, businesses must prepare for a paradigm shift in cybersecurity. The rise of quantum computers presents a real threat to the security of businesses as they will be able to break existing encryption algorithms rendering current cybersecurity measures useless. Organisations must start planning for post-quantum cryptography and adopt new quantum-secure technologies to mitigate this risk.

Looking ahead, 2023 is likely to amplify known cyber threats we see today along with new cybersecurity challenges and threats. With the rise of the Internet of Things (IoT), we can expect to see an increased threat surface for targeted attacks on IoT devices. We also learn that whilst Artificial Intelligence (AI) and Machine Learning (ML) can be a great cyber defense strategy, it can also be a double edged sword…

Sadly, the ongoing global geopolitical instabilities will continue to result in more cybercriminals exploiting vulnerabilities. Buckle up and brace yourselves for the inevitable chaos ahead. The incessant instability of our global politics is the perfect breeding ground for cybercriminals to launch their nefarious attacks, exploiting vulnerabilities and wreaking havoc on critical infrastructures, institutions, and organisations. State-sponsored attacks will become more frequent, causing widespread disruption and leaving us vulnerable to untold amounts of damage. The question is not if, but when the next attack will strike. Are we prepared to face the consequences of our inaction?

To stay ahead of the curve, organisations must adopt a proactive and holistic approach to cybersecurity, which includes risk assessment, vulnerability management, and incident response planning. This approach will help organisations to better identify and mitigate risks, reducing the likelihood of a cyber-attack.

So you see, cybersecurity is not just about technology. It's also about people, processes, and raising cybersecurity awareness. As Bruce Schneier said, "Security is a process, not a product." Cybersecurity is a constantly evolving process that requires a new business mindset and culture with ongoing vigilance and adaptation to new threats. So, let's stay ahead of the curve and protect ourselves from emerging threats.

We hope this editorial has been thought-provoking and insightful, motivating readers to take a proactive approach to cybersecurity risk management. And don't miss our VIP "In the spotlight" interview with **Chuck Brooks**, where we delve into the mind of a cybersecurity expert and gain insights into the future of the cybersecurity landscape.

Enjoy - over to you! ■

Cyber compliance. A safe bet.

Author: Raj Meghani

Cybersecurity and compliance are two essential components of a secure digital world. With the increasing reliance on technology and the internet, organisations must ensure that they are protected against cyber threats and are compliant with relevant regulations. In the UK, a number of high-profile organisations have suffered from cyber attacks in recent years, highlighting the importance of cybersecurity and compliance. In this article, I look into the importance of cybersecurity and compliance - both which should not be taken lightly.

BIO

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

LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/

Twitter: https://twitter.com/blockapt

Company website: https://www.blockapt.com

Cybersecurity refers to the measures that organisations take to protect their digital systems, networks, and information from unauthorised access, use, disclosure, disruption, modification, or destruction. With the rise of cybercrime, it is becoming more important for organisations to implement robust security measures to protect their digital assets. This is particularly important for organisations that hold sensitive information, such as personal data or financial information, as a data breach can have serious consequences for both the organisation and the individuals affected.

Compliance refers to the process of ensuring that an organisation adheres to relevant laws, regulations, and standards. In the UK, organisations must comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018). These regulations set out the rights and obligations of organisations with respect to the processing of personal data and the protection of privacy. Organisations that fail to comply with these regulations can face significant fines and damage to their reputation.

The importance of cybersecurity and compliance in the UK can be seen by examining recent cyber attacks on UK organisations. Two recent examples of breaches in the UK include:

December 2022/January 2023 - Cyber attackers demanded £15m in ransom money (thought to be cryptocurrency) from 16 British schools which got hacked during the Christmas holidays. With no access to their network, staff were back to the good old pen and paper planning method albeit not for long as systems were being brought back online…

February 2023 - Vesuvius PLC, a London Stock Exchange listed company which is a global leader in molten metal flow engineering and technology suffered a cyber incident where there was unauthorised activity on their network. Possible ransomware attack?

Both of these breaches would have been likely to have been caused by a vulnerability in the organisation's systems, which would have allowed the attackers to access sensitive information on the network and cause business disruption. This highlights the importance of implementing robust security measures and regularly assessing the security of digital systems to prevent similar attacks from occurring.

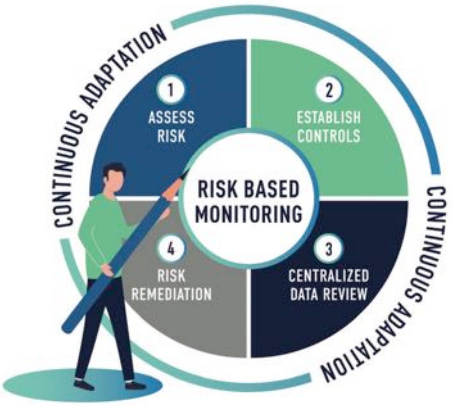
Organisations can take a number of steps to ensure that they are protected against cyber threats and are compliant with relevant regulations. Organisations should adopt a risk-based approach to cybersecurity, which means that they should assess the risks associated with the processing of personal data and implement appropriate measures to mitigate those risks. They should also implement effective security measures, such as firewalls, encryption, and access controls, to protect their digital systems and information. Additionally, organisations should have in place processes for incident response and data breach management, so that they are prepared to respond quickly and effectively if a breach occurs.

The importance of cybersecurity and compliance cannot be overstated.

The UK has a robust regulatory framework in place to ensure that organisations comply with best practices and regulations in the field of cybersecurity and data protection. However, as we continue to see cyber attacks on UK organisations like Royal Mail, the message is clear.

Organisations must have proactive measures to protect their digital assets and ensure that they are compliant with relevant regulations.

Organisations must adopt a risk-based approach to cybersecurity, implement robust security measures, and have in place processes for incident response and data breach management to prevent similar attacks from occurring.



Organisations can no longer point the finger solely at 3rd party partners as we have also seen in recent cyber attacks. It's time for them to wake up and smell the coffee and take accountability.

So in the interest of sharing best practice - here are 10 pointers organisations should implement to ensure cybersecurity compliance:

1. Conduct regular security assessments and audits to identify potential risks and vulnerabilities.

2. Implement robust access control policies and ensure that only authorised personnel have access to sensitive data and systems.

3. Encrypt sensitive data and communications to prevent unauthorised access and theft.

4. Regularly update software, systems, and applications to protect against known security threats.

5. Educate employees about cybersecurity risks and best practices to reduce the likelihood of successful attacks.

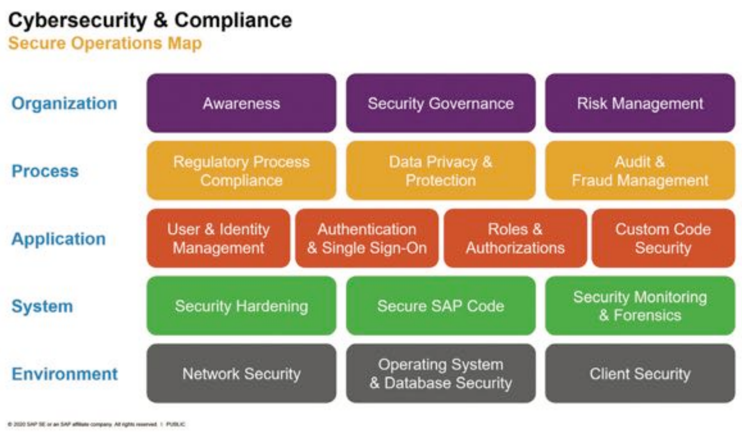
6. Develop and implement incident response plans to quickly and effectively respond to security breaches.

7. Regularly backup critical data to protect against data loss in the event of a security breach.

8. Monitor network activity for unusual patterns or suspicious activity that could indicate a security breach.

9. Use multi-factor authentication to add an extra layer of security to sensitive accounts and data.

10. Stay informed about current cybersecurity threats and best practices and regularly update your security policies and procedures accordingly.



Cybersecurity & Compliance
Secure Operations Map

Organization	Awareness	Security Governance	Risk Management	
Process	Regulatory Process Compliance	Data Privacy & Protection	Audit & Fraud Management	
Application	User & Identity Management	Authentication & Single Sign-On	Roles & Authorizations	Custom Code Security
System	Security Hardening	Secure SAP Code	Security Monitoring & Forensics	
Environment	Network Security	Operating System & Database Security	Client Security	

© 2020 SAP SE or an SAP affiliate company. All rights reserved. ǀ PUBLIC

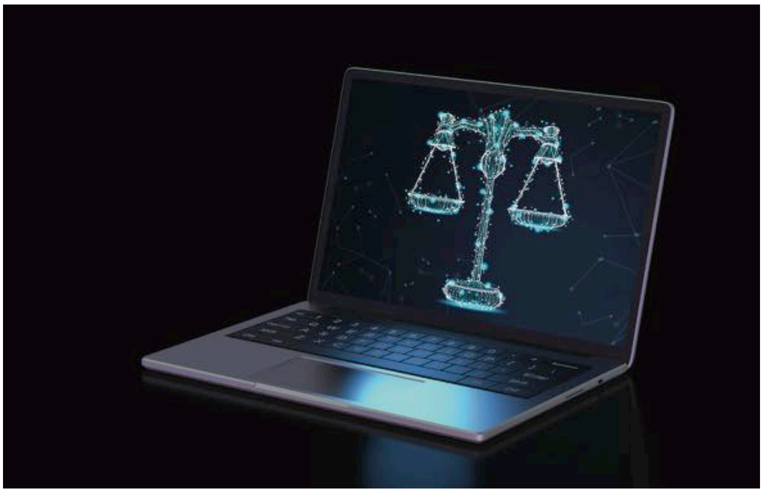
So here's my message simply put. Strong cybersecurity is not just about technology, it's about creating a culture of security and compliance from the top down. ■

The balancing act - Innovation vs Regulation.

Author: Kurt Sanger

The promise of innovation and the benefits of regulation are at odds in ways they never have been before. Individual and organisational dependencies on information technology, further advancements, and the risks that regulations seek to mitigate, will have greater impact on daily life and business activities across the world than perhaps any other regulatory effort. Balancing the promise and risks will take creativity and foresight, but most of all it will take what is in shortest supply… expertise.

As governments work to protect their citizens from the worst effects of information technology, the private sector must be ready to inform and advocate as regulations develop. If governments do not access private sector knowledge during this effort, private subject matter experts must be ready to insert themselves to ensure regulatory development is well informed and effective. If the private sector does not put in the work during the developmental phase, it will certainly regret it when it is time for the enforcement phase.



Information technology tools that have developed and spread globally in the last 30 years have improved life and made it easier. To name only a few of their benefits, they have created beneficial and productive connections between people and organisations and increased the pace of commerce and scientific discovery. However, the risks that have come with these advances have multiplied as well, and the risk borne by one information technology user, or one network, can bring harm to countless users and networks.

Defeating the externalisation of risk is perhaps the main purpose of regulation. It is meant to create safe and fair development of systems, protect participants in those systems, limit potential damage to those who are unable to control risks, and place responsibility on those best positioned to handle and mitigate those risks. There is no need to revisit the failure

BIO

Kurt Sanger served in the U.S. Marine Corps for over 23 years as a cyber operations attorney, criminal defense counsel and prosecutor, advisor to the Afghan National Army, international law instructor at Marine Corps University and National Defense University, and as a planning officer with U.S. Central Command. He earned a degree in National Security Law from Georgetown University in 2015.

From 2014 to 2017, Kurt was General Counsel for U.S. Marine Corps Forces Cyber Command. He served with U.S. Cyber Command from 2017 to 2022, first as the lead attorney for plans, policy, domestic and international partnerships, and legislative affairs, later as lead attorney for operations and intelligence, and finally as the Command's Deputy General Counsel. He retired from the Marine Corps in November 2022.

As a well-respected military industry veteran, attorney, speaker and instructor, Kurt is now Founder and Director of Integrated Cybersecurity Partners, LLC, an information technology and national security consultancy, which advises on national security and cyberspace operations for public and private sectors.

to prioritise security in most information technology development over the past three decades, but we have arrived at a moment in which many governments are recognising the scope of information technology threats and understanding that the benefits of making innovation the highest if not sole priority cannot be sustained without enormous costs.

Many western governments, even those with a distaste for regulation, are looking to the private sector for increased reporting of vulnerabilities and breaches, setting standards for organisations responsible for critical infrastructure, and penalising individuals and entities failing to meet their obligations. The appetite for regulation is almost certain to increase in the near term with more breaches, ransomware, and other incidents surely to come. As these regulations develop, the level of cybersecurity and information technology expertise in the public sector relative to the private sector will become a significant factor.

All organisations, public and private, share the same concern regarding cyber and IT expertise… no one has enough of it and everyone is looking for more of it. The public sector, however, cannot match the incentives and benefits that the private sector can offer. With more expertise in the private sector than public, it may be difficult for government bodies to develop regulations that are effective, enforceable, and fair without private sector assistance.

Do governments have the expertise necessary to regulate the full range of information technologies? To name only a few challenging areas, regulations are under consideration with regard to social media, artificial intelligence, privacy and law enforcement access, incident reporting, and the cybersecurity of diverse institutions ranging from brokerage houses to critical infrastructure operators to small businesses with relatively limited resources.

The question of whether governments have the expertise necessary to regulate these issues is underscored by the fact that governments' systems are breached regularly. Notorious incidents have befallen many of the institutions that are now charged with regulating others (for example, it's quite possible that the Chinese Government has better records on many Americans than the U.S. Government). This by no means indicates that regulators may be unqualified in this regard, but governing institutions should lead by example. At the very least, they should hold themselves to the same standards they expect others to realise, and they should never punish an organisation for failing to reach a level of security that they have not achieved themselves.

Jen Easterly, Director of the U.S. Cyber and Infrastructure Security Agency, recently said that "if companies are doing all the right things and still get breached", they may yet be protected from regulatory penalties. This is easier said than done though.

If a typical household suffers a fire in its kitchen, having a nearby extinguisher available to put it out is a reasonable expectation. If the same house's roof catches fire, no one expects the inhabitants to have the resources to handle that level of catastrophe on their own. It's what we have fire departments for.

Will government officials be able to recognise the difference between a cyber kitchen fire and a cyber roof fire? What criteria will they use? How will they gather evidence? What level and depth of access to a system will they request or require in order to investigate?

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

THE WHITE HOUSE

The Biden Administration released its National Cybersecurity Strategy in early March. A remarkable document in its entirety, perhaps the most noteworthy statement regards a shared duty to develop workable cybersecurity regulations: "A collaborative process between industry and regulators will produce regulatory requirements that are operationally and commercially viable and will ensure the safe and resilient operation of critical infrastructure." This is a welcome statement that should be viewed optimistically and reflect an aspiration for all representative governments.

It is one thing to say this from the top and another to ask rank-and-file regulators to look at the private sector not merely as "the regulated" and to view them instead as collaborators. Government employees should put aside their roles as law makers, law enforcers, and leaders in this effort. They should see themselves as peers and fellow network owners, operators and defenders... and look to develop regulations from that united foundation. ■

Health data: From raiding to reselling.

Author: Stéphane Mortier

In September 2020, the German government announced that a patient in a Düsseldorf clinic had died as a result of a cyber attack. Since then, cyber attacks on healthcare institutions have never stopped and are increasing in number. The attacks are mainly ransomware or Distributed Denial of Service (DDoS) attacks. Are cybercriminals acting out of opportunity ? Or are they trying to destabilise the health systems of the states concerned ? Or are they preying on health data with a view to reselling or using it? Although several laws and regulations attempt to protect health data, there are many technical and human vulnerabilities that make them particularly vulnerable to malicious actors.

BIO

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

More and more attacks

One only has to read the specialised or general public press to understand the extent of the phenomenon. Health establishments in most European countries (and more widely in the West) are affected. Recently, the Dutch National Cyber Security Centre (NCSC)[1] reported that hospitals in Europe, particularly in the Netherlands, have been targeted by a group of hackers. British, German, Polish, American and Scandinavian hospitals have also been targeted in recent months. In May 2022, Italian hospitals based in Milan were also the target of a cyber-attack, which affected both hospital and emergency departments, as well as certain vaccination centres, such as the one in Piazzale Accursio in Milan[2].

In November 2022, in Belgium, after the Groupe Santé CHC in Liège, it was the Saint-Pierre hospital in Brussels that fell victim to a cyber attack in March 2023. In May 2022, the intercommunal healthcare organisation Vivalia had already been the victim of a large-scale cyber attack[3]. *"Hackers are looking for information, especially sensitive medical information, and hospitals are therefore priority targets"* said Yves Smeets, Director General of Santhéa, the professional and employers association of Walloon and Brussels healthcare institutions.

In France, more than thirty hospitals were affected by a cyber attack between 2021 and to date.

Finally, on 13 March 2023, at the Hospital Clinic in Barcelona, the cybercriminal group Ransom Home demanded a ransom of $4.5 million not to publish the data to which it had gained access[4].

A classic modus operandi for accessing high value-added data

To get into a hospital's computer network, hackers use the usual loopholes. Either they take advantage of a vulnerability in the network, or they use social engineering techniques, or a combination of both, explains Michele Rignanese, spokesperson for the Belgian Centre for Cybersecurity (CCB). It is clear that most of the equipment today is a connected device that very often contains vulnerabilities. The same applies to laboratories where the security of connected equipment does not always seem to be a priority[5]. In short, awareness of the sensitivity and strategic nature of health data is not yet systematically accepted by professionals in the sector.

However, the purpose of collecting health data is probably based on the possibility of using it in massive quantities to feed automatic medical recognition AI[6], either directly or by selling it to the right people or organisations. It is therefore a matter of massive raids on the health data of citizens of countries with efficient health systems.

In a report on personal data produced by France Télévision in May 2021[7] Sarah Spiekermann, Director of the Vienna Institute of Information Systems, stated that "our personal data is worth its weight in gold" and that some companies hold up to "30,000 data points for each individual they track". Among these data, health data! On a global level, "the potential of e-health data is estimated by the GAFAMs at $7,100 billion", according to Eugène Favier-Baron of Grenoble Alpes University. This leaves great opportunities for cybercriminals...

What status and protection is there for health data?

The General Data Protection Regulation (GDPR), sheds some light on health data (Article 35): Personal data concerning health should include all data relating to the health status of a data subject which reveals information about the data subject's past, present or future physical or mental health.

This data falls under the special character of personal data as provided for in Article 9-1 of the Regulation, the processing of which is prohibited except within a particularly strict framework justifying the necessity :

- The processing is necessary for the purposes of preventive medicine or occupational medicine, the assessment of the worker's capacity to work, medical diagnosis, health or social care, or the management of healthcare or social protection systems and services (Art. 9-2-h);
- The processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or for the purpose of ensuring high standards of quality and safety of healthcare and medicines or medical devices (Art. 9-2-1).

In this case, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Art. 32-1) and particular account shall be taken of the risks represented by the processing, in particular those resulting from the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed (Art. 32-2). This raises the responsibility of the controller of health data and the level of security to be added to it. To control this level of security, healthcare professionals can rely on several ISO standards (27001, 27002 and 27799).

The ISO 27001 standard relates to information security, cybersecurity and the protection of privacy, as well as to information security management systems. It is complemented by ISO 27002 (Information technology - Security techniques - Code of practice for information security management) for which an organisation must identify its security requirements according to :

- The organisation's own risk assessment;
- The legal, statutory, regulatory and contractual requirements that the organisation and its business partners, contractors and service providers must meet;
- The set of business principles, objectives and requirements for handling, processing, storing, communicating and archiving information.

Finally, ISO 27799 transposes ISO 27002 to the health domain, taking care in considering the appropriate application of security measures for the protection of personal health information.

Beyond the GDPR and this normative environment, health actors are also covered by the NIS 2 directive and are included as highly critical sectors and therefore constitute essential service operators. These include healthcare providers, laboratories, research and development entities, pharmaceutical manufacturers and manufacturers of medical devices are considered critical. Being dependent on computer networks or information systems, the disruption of which would have a significant impact on their operations, they are obliged to put in place internal cybersecurity risk management measures and to submit to reporting obligations.

Conclusion

The increasing use of connected medical devices and equipment is generating a wealth of health-related data. Although this data is considered sensitive, numerous flaws in both the medical devices and in the management and storage of this data make it particularly attractive to malicious actors.

Cybercriminals become predators of health data because the financial windfall it represents is immense: theft or misappropriation of data, resale or use in innovative artificial intelligence systems. The race for data represents a field in which the competitiveness of the players concerned depends on agility and the fastest possible response. The temptation is therefore great to acquire, legally (less quickly) or illegally (very quickly), the necessary quantities of health data to achieve the desired objectives.

It is likely that an increasing interpenetration of legal and illegal economies, as in other sectors of activity, will become a reality in the near future with regard to health data, despite the inflation of standards in this area. ■

[1] https://www.whatsupdoc-lemag.fr/article/les-hopitaux-des-pays-qui-soutiennent-lukraine-pris-pour-cibles-par-des-hackers-prorusses
[2] https://librexpression.fr/ransomware-attaques-des-hopitaux-en-lombardie
[3] https://lequotidien.lu/a-la-une/belgique-des-hopitaux-de-la-province-de-luxembourg-victimes-dune-cyberattaque/
[4] https://lepetitjournal.com/barcelone/cyberattaque-contre-lhospital-clinic-barcelone-rancon-de-45-millions-de-dollars-357705
[5] https://www.rtbf.be/article/pourquoi-les-hopitaux-sont-ils-des-cibles-privilegiees-des-cyberattaques-11166485
[6] https://usbeketrica.com/fr/article/hopitaux-laboratoires-pourquoi-le-secteur-de-la-sante-est-victime-de-cyberattaques
[7] https://www.france.tv/france-2/cash-investigation/2450927-nos-donnees-personnelles-valent-de-l-or.html

BLOCKAPT™

QDex labs™

MicroToken Exchange (MTE®) Technology

The next level quantum secure communication capabilities for Data-in-Motion and Data-at-Rest in strategic alliance with QDex Labs™.

- **FIPS 140-3** validated standard technology
- Requires no changes to **user experience**
- A **real-time** command & control panel
- Satisfy **data protection compliance** standards
- **Secures** data inside the platform with a layered defence
- Fully secured **2-way channel** for communications

blockapt.com

VIP Interview with Chuck Brooks.

Interviewer **Raj Meghani**

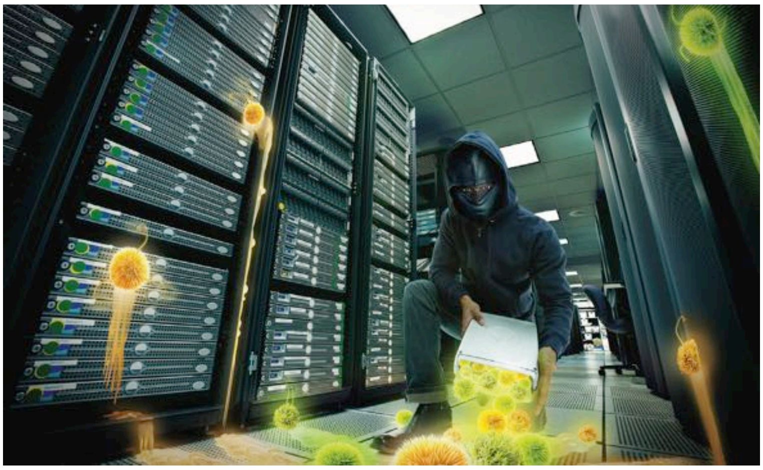
RM: Hello Chuck - let's start with what inspired your cybersecurity career, and how has your passion for this field evolved over time?

My initial involvement in the cyber world came two decades ago while I was with the Science & Technology Directorate at the Department of Homeland Security (DHS). At the time, the primary focus at the agency was on CBRNE (Chemical, Biological, Radiological, Nuclear, and Explosive) as the digital age was just in its infancy. However, it was clear that internet connectivity was growing and the security aspects of communications were of high interest. After DHS, I continued the pathway of working on both emerging tech and cybersecurity topics and projects with several public companies, including SRA, Xerox, and Rapiscan in senior executive roles. I retired from General Dynamics Mission Systems where I scouted and analysed cyber technologies and trends and opened my own firm, Brooks Consulting International, during the initial stages of the Covid pandemic.

The cumulative work from both the public and private sectors, plus my role as faculty and Georgetown University's graduate programs in Cyber Risk Management and Applied Intelligence has kept me current on the policy and technological developments in the industry. In addition, writing over 300 articles on cybersecurity and appearing on dozens of panels, events, and in speaking keynote roles has only further whetted my appetite for learning more about cybersecurity trends and applications.

RM: As a renowned expert in cybersecurity, what are some of the biggest threats facing organisations and people today, and how can they better protect themselves?

The reality is that we live in an increasingly hyper-connected world. The exponential rate of cyber-threats and breaches require a clearly defined security strategy for who and how to handle this constantly evolving landscape of cyber threats — from phishing scams, bots, distributed denial of service attacks, ransomware, and a host of insider threats. Moreover, criminal hackers are now automating targeted attacks with artificial intelligence and machine learning making the landscape even more vulnerable for exploiting. And the threats will continue to grow, primarily from phishing and ransomware because it continues to work for the hackers and it is easy to deploy in cyber-attacks.



When addressing cyber-threats, it begins with risk management. For an organisation or consumer, it requires being vigilant and encompasses practicing cyber-hygiene (strong password, multi factor authentication, fire walls, encryption, back-ups, and pen testing) Every situation is somewhat different, but every risk management plan should focus on identifying gaps, assessing vulnerabilities, developing strategies to mitigating threats, and having updated resilience plans to respond to incidents.

RM: How can individuals and organisations balance the need for data privacy with the need for security in today's digital age?

Unfortunately, the concept of privacy is fleeting in the digital world. One of the creators of the internet, Vint Cerf, Chief Evangelist of Google has stated that privacy does not exist anymore. The only way to not put data at risk is to not be on the internet.

I think that Europe has done a good job with creating GDPR that at the minimum provides users with a reminder that what they click on may be shared. Ultimately, it is up to the individual or company to determine what data they make accessible. Segmentation of data, encryption, and "Zero Trust" are ways to better protect privacy. Also, one needs to be aware of what they share on social media because it can be eternal. For younger generations, privacy does not seem much of a priority and that may come back to hurt them in the job world. Like everything else in life, what personal information you share with others requires circumspection and balance.

RM: What role should the government play in cybersecurity Chuck, and how can public-private partnerships help?

Certainly, a high level of Public-Private Partnership (PPP) collaboration is needed to address growing cyber-threats. Preparation and commitment from both government and industry leadership is critical. Industry should collaborate with the government to best utilise risk management models and prepare resiliency plans.

PPP is dependent on information sharing, planning, investment in emerging technologies, and allocation of resources coordinated by both the public and private sectors in special working partnerships.

The specifics of an industry security approach may vary according to circumstances, but the mesh that connects the elements is situational awareness combined with systematic abilities for operational management and critical communications in cases of emergency. Government needs to take an increased role in sharing threat intelligence and cybersecurity tools with the private sector who operates much of the critical infrastructure. The fact is that most companies do not have the security resources or expertise to combat the type of threats emanating from state actors.

RM: Let's talk about ethics. What ethical dilemmas do you face in cybersecurity, and how do you handle them?

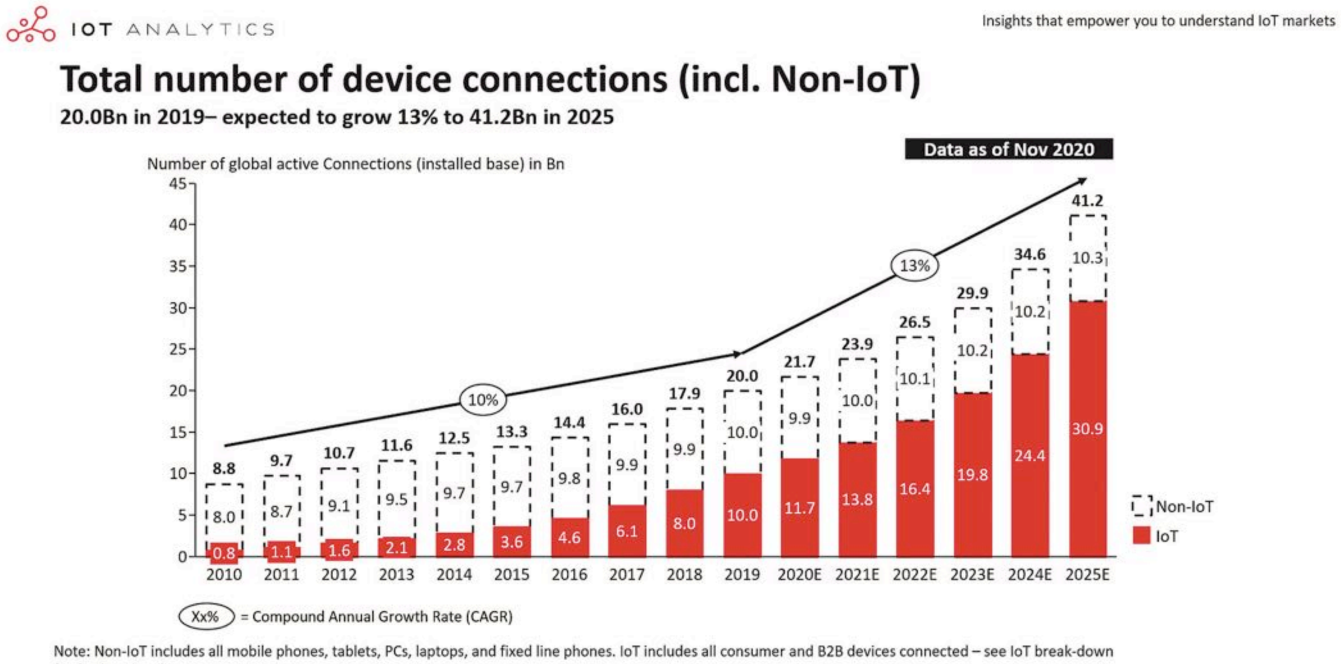
There are many ethical dilemmas in the cyber world, including who should and has provided access, what data should be shared. Perhaps the most challenging is what to disclose if a company is hacked as it can impact stock prices or lead to a loss of confidence in reputation. And with ransomware, the ethical dilemma is should you pay or not pay the ransom. The best way to handle those issues is usually via corporate governance and C-Suite discussions.

RM: How has the cybersecurity landscape evolved over the years, and what trends do you see emerging in the near future?

IT has evolved in so many ways it is hard to mention them all. One trend we are seeing now is digital connectivity driven by the adoption of industrial Internet of Things (IoT) and Operational Technology (OT) that has further expanded the attack surface. IT/OT/ICS supply chains in CI can be particularly vulnerable as they cross pollinate and offer attackers many points of entry and older Legacy OT systems were not designed to protect against cyber-attacks. The Colonial pipeline attack exemplified the intertwining of OT and IT and the risks associated with supply chains.

The Internet of Things is also a huge cybersecurity challenge. By 2025, it is expected that there will be more than 30 billion IoT connections, almost 4 IoT devices per person on average and that also amounts to trillions of sensors connecting and interacting on these devices. That is a whole lot of IoT devices and protecting such an enormous attack surface is no easy task, especially when there are so many varying types and security standards on the devices. The prevailing perspective from a security operations perspective on those billions of IoT devices is that anything connected can be hacked.

And Artificial Intelligence (AI) and Machine Learning (ML) are greatly impacting cybersecurity. AI can provide a faster means to detect and identify cyber-threats. Cybersecurity companies have developed software and platform powered by AI that monitors in real time activities on network



Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details

Source(s): IoT Analytics - Cellular IoT & LPWA Connectivity Market Tracker 2010-25

by, scanning data and files to recognise unauthorised communication attempts, unauthorised connections, abnormal/malicious credential use, brute force login attempts, unusual data movement, and data exfiltration. This allows businesses to draw statistical inferences and protect against anomalies before they are reported and patched.

AI threat hunting tools can cover cloud, data center, enterprise networks, and IoT devices. AI tools can allow for automatic updating and threat vetting of defense framework layers (network, server, payload, endpoint, firewalls, and anti-virus) and diagnostic and forensics analysis for cybersecurity.

The reality is that emerging technologies are impacting cybersecurity planning in many ways. At the annual World Economic Forum meeting in DAVOS, it was announced the combined value of digital transformation -- for society and industry -- could be greater than $100 trillion by 2025. That transformation includes the immersive inclusion of digital technologies and cloud-based platforms. It also includes analytics, sensors, mobility, and a new era of automation impacting all industries and verticals including financial, energy, security, communications, and health.

RM: Interesting times ahead Chuck. So with all these emerging trends, how can organisations educate their employees about cybersecurity, and what role should individuals play in protecting themselves online?

Given that phishing is still one of the leading causes of data breaches, phishing testing should become standard in employee training nowadays. Training modules can be pre-programmed at the network level and done regularly. They also can be conducted with gamification to make it more memorable and appealing. To stay safer, it comes down to cyber-hygiene, strong passwords, multi factor authentication, timely patching, anti-virus software, and being extra aware of not to click on a phish.

An easy rule to follow is to automatically discard any communications asking you for personal information. Chances are you are not the recipient of long-lost funds found in an obscure bank account, nor did you randomly win a contest. If something is too good to be true, it likely isn't. Also, Individuals should also consider moving and protecting their sensitive data from open networks.

RM: Very true! So how do you stay up-to-date on the latest threats and vulnerabilities, and what resources do you recommend?

I stay updated in many ways, First, teaching cybersecurity like I do requires constant reading of the latest developments. Dark Reading, FORBES, Skytop Media, Cyber Express, Homeland Security Today, GovCon/Executive Mosaic, and CyberTheory are some of my daily readings. In all, I read about two dozen articles a day. DHS CISA also regularly publishes news on

BIO

Chuck Brooks is a globally recognised thought leader and subject matter expert Cybersecurity and Emerging Technologies. Chuck is also an Adjunct Faculty at Georgetown University's Graduate Cybersecurity Risk Management Program where he teaches courses on risk management, homeland security technologies, and cybersecurity. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn." He was named "Cybersecurity Person of the Year for 2022" by The Cyber Express, and as one of the world's "10 Best Cyber Security and Technology Experts" by Best Rated, as a "Top 50 Global Influencer in Risk, Compliance," by Thompson Reuters, "Best of The Word in Security" by CISO Platform, and by IFSEC, and Thinkers 360 as the "#2 Global Cybersecurity Influencer." Chuck was featured in the 2020, 2021, and 2022 Onalytica «Who's Who in Cybersecurity» He was also named one of the Top 5 Executives to Follow on Cybersecurity by Executive Mosaic, He is also a Cybersecurity Expert for "The Network" at the Washington Post, Visiting Editor at Homeland Security Today, Expert for Executive Mosaic/GovCon, and a Contributor to Skytop Media, and to FORBES. He has an MA in International relations from the University of Chicago, a BA in Political Science from DePauw University, and a Certificate in International Law from The Hague Academy of International Law.

many of the latest threats on their website. NIST offers excellent frameworks for risk management. Perhaps the most timely and accessible sources are found on social media. I find the LinkedIn cyber-related groups very useful as top experts and influencers constantly share articles and insights. Attending events and webinars are also a great way to stay current.

RM: How can we foster greater diversity and inclusivity in cybersecurity, Chuck, and what benefits do you think it brings to the table?

A more diverse workforce is a better workforce. Cybersecurity does not need to be a mostly male domain. As we continue to evolve into the new digital era, new opportunities arise, and the real task is outreach and effective communication to bring women into the emerging cybersecurity career realms. The challenge at hand, to ameliorate the huge shortage of cybersecurity professionals and close the gender gap, requires that we educate, train and facilitate women to fill the pipeline for a qualified information security workforce. This outreach should also be made to minorities and especially for those living in economically depressed areas.

RM: I can relate to that, Chuck - as a female leader and ethnic minority working in cybersecurity! So what advice do you have for aspiring cybersecurity professionals, and what qualities are essential for success in this field?

Cybersecurity certainly comprises coding and algorithms, but it is much more than that. It also incorporates executive management, policymaking, diplomacy, marketing research, compliance, intelligence, technology foraging, communications and thought leadership as elements of the discipline. Soft skills are required for success in the field as is an eagerness to learn. It is also a field of opportunity, and many education institutions are incorporating cybersecurity into their curriculums. I highly recommend cybersecurity as a career path as all our futures will become increasingly digitally connected and riskier. ■

Flip the Qubit.

From the bit to the favicon, whether attacking with bit flipping or abusing domains with homoglyphs, cyber criminals continue to engineer ways to infiltrate systems. One of the most prevalent cyber-attack methods is social engineering where the art of deception is involved. As we delve further into how manipulation tactics are employed against their targets, I cannot help but take a step back and view how we could address these attacks today versus the quantum attacks of tomorrow.

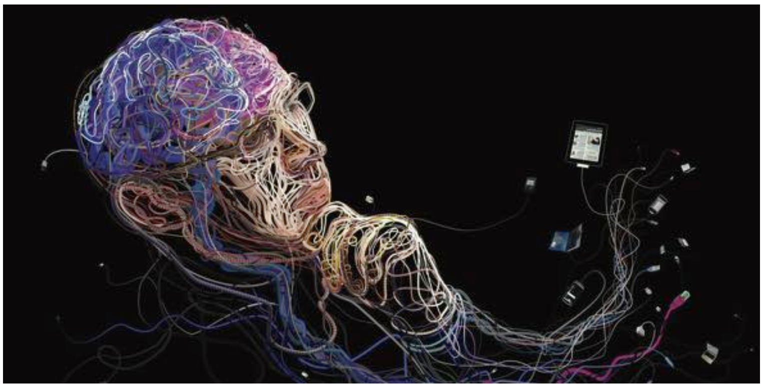
One of the objectives is to align with cybersecurity methodologies and tools that protect the current "Classic Internet" and evolve into a hybrid model for the forthcoming "Quantum Internet." Although there are multiple schools of thought on how to further this alignment, I've taken a multidisciplinary scientific approach which is described in three phases:

- **Quantum Spaces**
- **Data Moments**
- **Sensory Engagements**

BIO

Sunny "Dos" Dosanjh is the CEO of DUSA SPACE. He is a technology veteran in Silicon Valley, California and currently provides consulting for Post-Quantum Cryptography, Salesforce & Multi-Cloud data, application, and network security. He has a Bachelor of Science, Information Systems from San Jose State University and his career began with the US Air Force. Sunny also volunteers as Chaplain with the American Legion in Santa Clara, California and as a Royal British Legionnaire in Isleworth, London England.

Author: Sunny "Dos" Dosanjh



Quantum Spaces: Infrastructure & Protection

The Classic Internet as we know it today relies on the traditional "bit." The forthcoming Quantum Internet, based upon "qubits", will introduce new infrastructure requirements for both applications and the networks. Protection methods will be required to function in both the Classic and Quantum Spaces which will require new cybersecurity tools to function in a multitude of situations, for example:

▸ Multi-Domain	Space, Low-Earth Orbit, Atmospheric, Terrestrial, Subterranean
▸ Multi-Region	North America, Europe, Middle East, Africa, Asia-Pacific, Latin America
▸ Multi-Reality	Physical Reality, Extended Reality including Augmented, Virtual & Mixed
▸ Multi-Cloud	Public, Private, Hybrid
▸ Multi-Destination	Embedded Systems, Wearables, IoT Devices, Core/Edge/Distributed Nodes
▸ Multi-Environment	Production, Pre-Production, User-Acceptance, System, Development, Sandboxes
▸ Multi-Identity	Authentication, Permissions, Behaviour, Auditing

The cybersecurity policies that traverse these multiple situations will require their own segmented spaces to isolate attacks on hybrid infrastructure. As quantum products emerge for Post-Quantum Cryptography, Quantum Key Distribution and Quantum Random Number Generators, new quantum cybersecurity tools will be required for DevSecOps teams. The opportunity exists today to get ahead of quantum computers, sensors and spaces with a gameplan to address cybersecurity situational concerns with early simulation tools.

Data Moments: Analytics, Integrity, Inferences

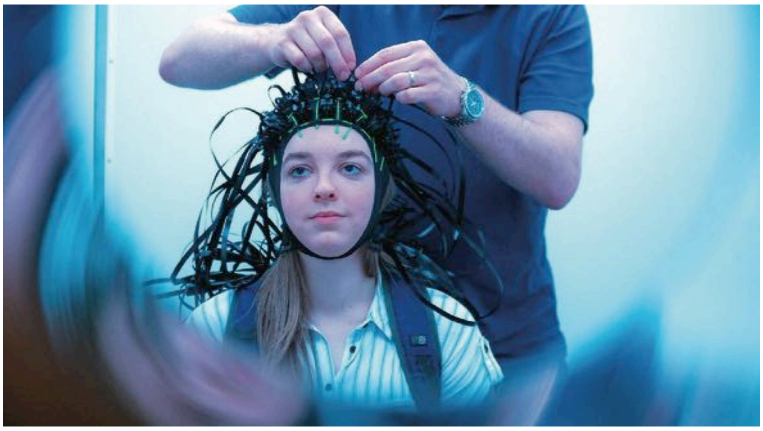
Statistical concepts for scientific data models have existed for quite some time. Our perspective of Data Moments is derived from how data is expressed to how it is experienced. Included in the Data Moment is the data journey from creation to consumption, source to destination, at rest, in use and in transit. The applicability of A.I., analytics and derived inferences are based upon the integrity of data at a given moment in time. Core components include the application logic, database structure and how data is consumed as content.

For example, data integrity is compromised as bit flipping enters the realm of qubits which are in a state of superposition. It will be interesting to discern what is a legitimate cyber-attack i.e., DNS request manipulation versus a natural occurrence due to the energy of a neutron particle. In either case, the existing tools that utilise error correction, for maintaining data integrity, will remain an open question regarding their ability to address quantum situations. Data sourced from quantum computers and related services will require protection from quasiparticle energy bursts which will destroy qubit coherence. Positive strides have been taken by several organisations conducting quantum hardware-aware error correction experiments and implementing bit flip code. These experiments are all part of a global effort in establishing quantum processors designed with qubit error correction to ensure the integrity of a Data Moment.

Sensory Engagements: Quantum Sensors and Human Perception

Quantum Sensors have been available in various forms for several decades. They're utilised to detect and measure small changes in gravity, temperature, magnetic and electric fields as a few examples. Quantum-Precise Time, Quantum Positioning Systems and radar sensors with the ability to see through liquid and solid objects are amongst the latest experiments in this field. These advancements have cybersecurity and military defense teams on notice with their ability to disrupt communication systems and compromise data integrity.

These same sensors are also utilised in understanding human perception with medical patients suffering from trauma and brain injuries. Augmented therapy treatments are in clinical trials based upon Sensory Resonance. Specific brainwave frequencies are combined with data from human sense perceptions to understand how to reactivate those parts of the brain responsible for processing information. Critical to this operation is maintaining identity, data and communication integrity in order to circumvent any false positive indicators.



In summary, organisations have an opportunity to proactively employ cybersecurity measures for the forthcoming quantum internet age. The multidisciplinary scientific approach is meant to combine the domains of outer-space and planet earth with human perception and "inner-space". The security principles of today would still apply, however, they will have to evolve to address Quantum-Compute sourced cyber-attacks. Our recommendation is to account for how Quantum Spaces, Data Moments and how the Human Senses are engaged. These are just a few suggestions on how to align current cybersecurity frameworks into a quantum-resilient solution. ■

Quantum Security: A new era of unbreakable encryption?

Author: Raj Meghani

[Exploring the ways in which quantum technology is poised to transform cryptography, and whether it will lead to unbreakable systems]

In recent years, quantum technology has emerged as one of the most exciting areas of research and development for cybersecurity. With the potential to create "unbreakable" encryption, quantum security is a topic which fascinates me.

Is quantum technology poised to transform encryption? Will it really be unbreakable? What's the potential for quantum security and what are the challenges that come with it?

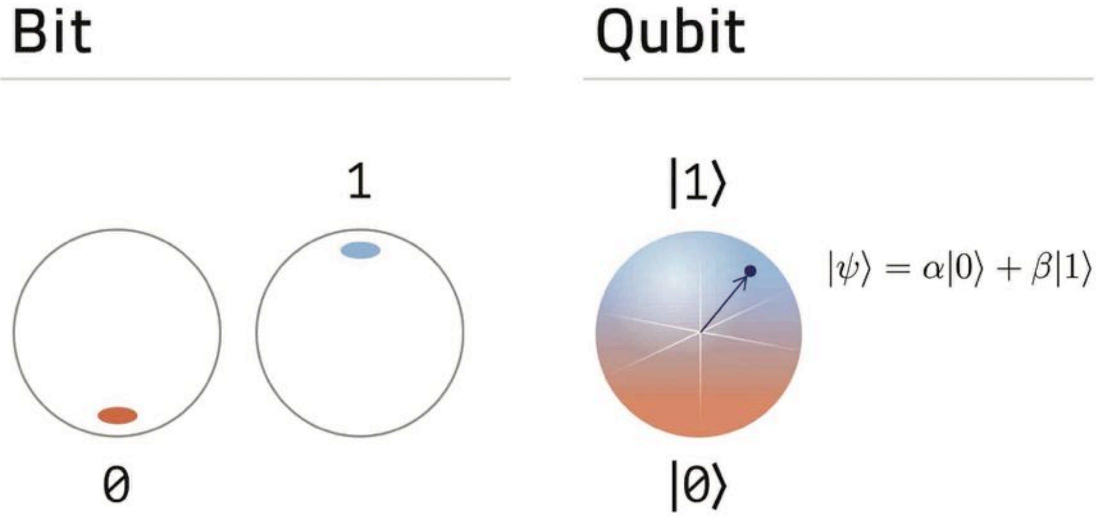
What is Quantum Security?

To understand quantum security, it's important to first understand quantum computing. At a basic level, quantum computing uses the principles of quantum mechanics to create a new kind of computer that can perform certain kinds of calculations much faster than traditional computers. This is due to the fact that quantum computers use qubits, or quantum bits, which can exist in multiple states simultaneously, unlike classical bits which can only be in one state at a time.

Qubits, or quantum bits allow quantum computers to perform certain tasks much faster than traditional computers, as they can perform many calculations simultaneously. For example, a quantum computer could crack the encryption keys used to protect sensitive information much faster, something that would take traditional computers billions of years.

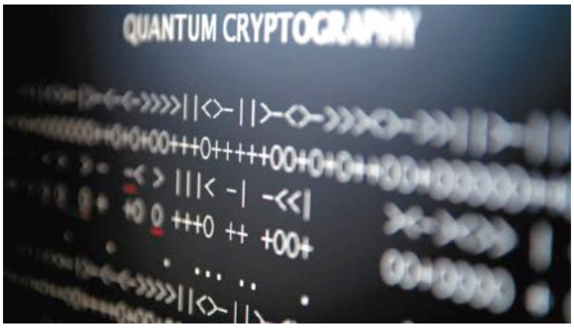
For example, in the case of cryptography, quantum computing has the potential to make current encryption methods obsolete, as it can easily break down complex algorithms that are currently considered secure.

However, quantum technology also has the potential to create new forms of encryption that are much more secure than anything we've seen before.



BIO

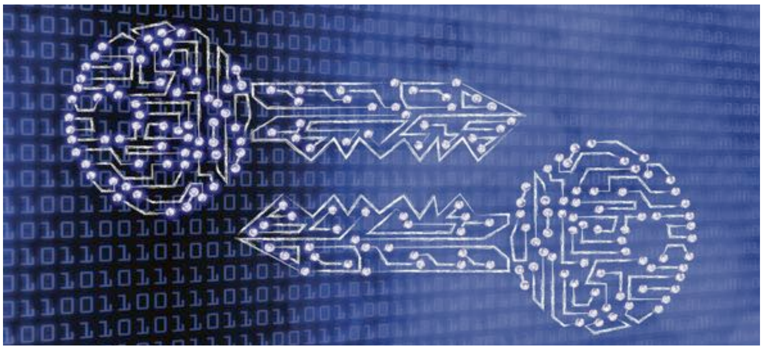
As Editor of Cybersecurity Trends UK, Raj is widely recognised as a thought leader and cybersecurity influencer. Raj is the Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25+ years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. She's esteemed as a successful brand builder and a business growth hacker. Her unique expertise in scaling start-ups and disrupting markets with new tech has earned her recognition as a «One in a Million» female founder by The Entrepreneur's Network and placed her in the Top 44 "Cyber Power Women" by Top Cyber News Magazine. Raj is also Non-Executive Director on the Board of Money Matters Community Bank.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com



This is where quantum security comes in. Quantum security refers to the use of quantum technology to create encryption methods that are virtually unbreakable, even by quantum computers.

How does quantum security work?

To understand how quantum security works, I've had to get my head around the basics of encryption. Encryption is the process of transforming information into a code, or cipher, that can only be read by someone who has the key to unlock it. This key is usually a string of characters that is used to encrypt and decrypt the message.



In traditional encryption, this key is usually a long complex combination of letters, numbers, and symbols that are used to scramble the message. However, with the power of quantum computing, this kind of encryption is vulnerable to being broken down.

Quantum encryption, on the other hand, uses the principles of quantum mechanics to create a key that is virtually unbreakable. This is because quantum encryption relies on the principle of quantum entanglement, which is the idea that two particles can be connected in such a way that the state of one particle affects the state of the other particle, no matter how far apart they are.

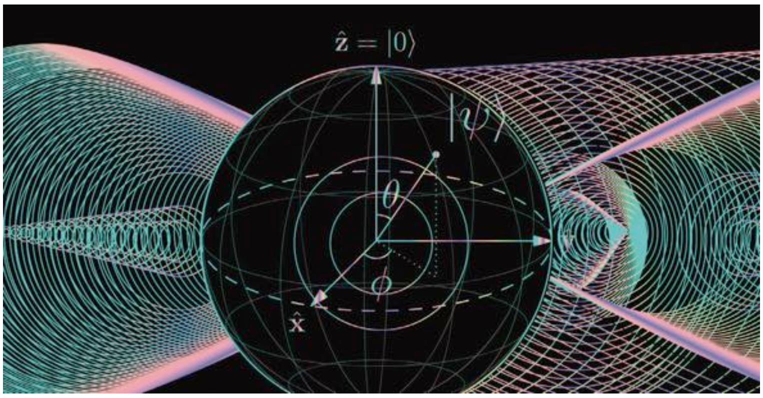
In quantum encryption, two entangled particles are used to create a key that is shared between two parties. This key is then used to encrypt and decrypt the message. The key is generated in such a way that any attempt to intercept it would cause the particles to become unentangled, thereby destroying the key and rendering the message unreadable.

The result of this process is a form of encryption that is virtually unbreakable. Even with the power of quantum computing, it is impossible to break the key without destroying it in the process.

What are the benefits of quantum security?

The benefits of quantum security are clear. With the potential to create unbreakable encryption methods, quantum security has the potential to protect sensitive information and data from prying eyes - whether they are criminals or state-sponsored hackers.

In addition, quantum security could also help to protect the integrity of data, as it can detect attempts to tamper with data-at-rest or data-in-motion. This could be particularly important in industries where data is critical, such as finance, healthcare, and government. In a nutshell - it has the potential to transform the way we think about data security.



In finance, for example, quantum security could be used to create a more secure payment system that would be resistant to fraud and data theft. In healthcare, it could be used to protect patient data and medical records, which are currently vulnerable to cyberattacks. In government, it could be used to protect national security secrets and classified information.

In addition to these benefits, quantum security also has the potential to create new forms of encryption that are much more secure than anything we've seen before. This could and is leading to the development of new technologies and applications that would be impossible with traditional encryption.

What are the challenges of quantum security?

However, there are also significant challenges to developing and implementing quantum security. One of the biggest challenges is the fact that quantum computers themselves can also break quantum encryption. This means that the race to develop unbreakable quantum encryption is not just about creating new encryption methods, but also about developing quantum computers that are secure.

In addition, quantum security is still in the large part in early stages of development, which means that it is not yet widely available. This makes it difficult for companies and organisations to implement, as I understand they will need to upgrade their entire infrastructure in order to support quantum security.

Then there's the issue of cost. How much is it going to cost an organisation to implement this quantum security over and above their traditional encryption methods?

Finally, there is also the challenge of educating people about quantum security. Because it is a new and complex technology, many people may not fully understand what it is or why it is important. I must admit I'm still on a steep learning curve in this area but one thing which I do know and passionately believe in is this. There is a widely recognised shortage of people with cybersecurity and quantum security skills and expertise so we must continue to raise awareness and share knowledge to bring our generations of tomorrow up to speed. This will help to promote the adoption of quantum security measures and create a more secure digital world.

Quantum security is an exciting and promising new area of development in the world of information security. With the potential to create unbreakable encryption methods, it has the potential to revolutionise the world of information security, offering unbreakable encryption and enhanced protection for sensitive data and information from cyber criminals.

I believe there must be strong collaboration and cooperation between researchers, developers, businesses and government bodies. Public-Private Partnerships (PPP) as Chuck Brooks mentions in his insightful interview with me, will need to be addressed. By working together, it is possible to accelerate the development and implementation of quantum security, making it more widely available and affordable.

By promoting awareness and understanding of quantum security, we can create a more secure, digital world for everyone.

Allow me to be direct - quantum security is not just a matter of protecting data, it's a race against time and the inevitability of progress is something we should all be looking forward to. ■

Quantum Security: A Paradigm Shift

The race towards a Quantum future.

Author: Aron Seader

Quantum computing continues to loom over us as an uncertain entity of our near future. We understand the power quantum computing has and its benefits over today's classical computing. Still, many unanswered questions exist about how it will affect cybersecurity.

BIO

Aron Seader brings nearly 15 years of technical and leadership experience to Eclypses as the Senior Director of Core Engineering. Aron has experience working as an engineer in multiple sectors including solar energy, fiber optics, and mechanical engineering. Across his experience, Aron has led and organized teams on in-depth projects, which required maintaining and building relationships with clients, information and research gathering skills, and hands on technical and mechanical work. At Eclypses, Aron leads the Core Engineering team, overseeing implementation and software development projects and conducting product management of Eclypses' MTE technology. Aron works closely with the technical, sales, marketing, and executive teams to ensure that the Eclypses core technology and messaging operate smoothly with the most up to date software and information. Aron and his team have led the way in Eclypses' FIPS 140-3 validation.

LinkedIn: https://www.linkedin.com/in/aron-seader-60978120/
Email: aron.seader@eclypses.com
https://eclypses.com/about/team/aron-seader/

The power of Quantum Computing

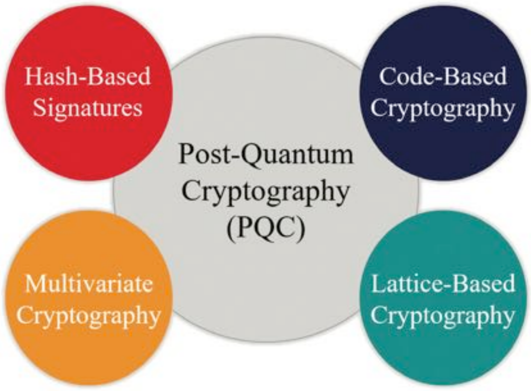
With the incredible power of quantum computing comes an overwhelming fear that today's securities will become obsolete. This fear is very legitimate and should drive security decisions today. Quantum computing has an undeniable advantage in computing the mathematics that current security is based upon. With this advantage, it is speculated that quantum computers can brute force current security best practices at an astonishing rate.

With this said, it is essential to recognise what aspects of current security practices will be affected. No, not all of what we currently use today is in danger; it is primarily the key exchange algorithms. The basis of most encryption is the Advanced Encryption Standard (AES) algorithms. These algorithms are considered to be resistant to the methodologies of quantum.

This is good news as the industry has countless hours involved in its refinement and use. The trouble is that AES encryption requires a key to execute its methodologies. That key must be available to both parties that wish to encrypt and decrypt data. But the key cannot be sent around the internet in plain text, someone would then have the key right along with the encrypted data, and you might as well not have even encrypted it. The safest way to exchange encryption keys would be a physical transference. My colleagues and I refer to this as a «sneaker net» because you get up from your computer and walk, using your sneakers, over to the receiving side of your message and manually enter your encryption key. It is easy to see that this is out of the question in our world of interconnectivity. This is why public key exchange methodologies were created.

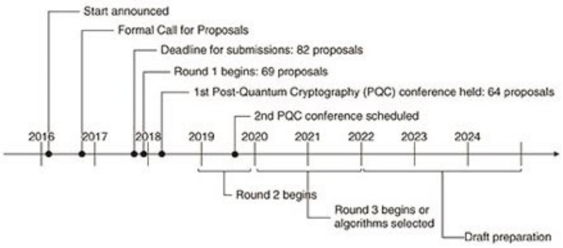
These exchange algorithms allow each communicating side to execute an initial handshake establishing public/private key pairings. These key pairings enable each side to encrypt and decrypt messages in a one-way fashion. Party A can encrypt a message with Part B's public key. The only way to decrypt that message is with Party B's private key, which hopefully only Party B can access.

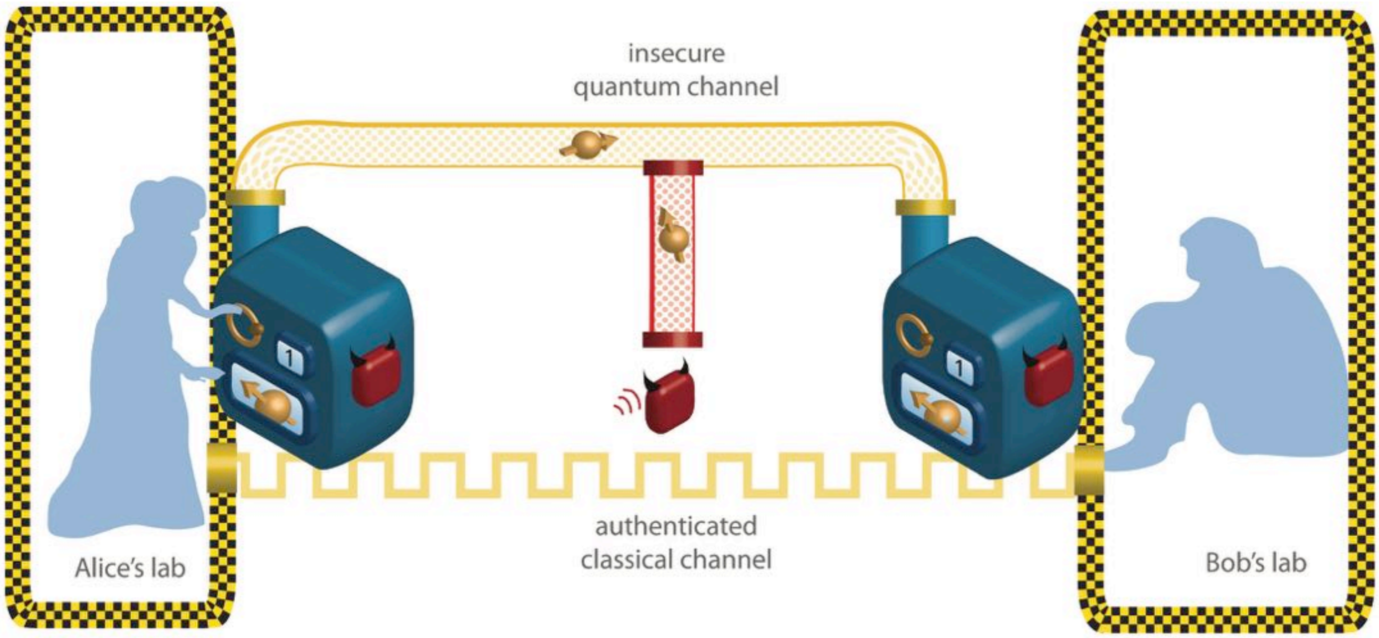
While these current key exchanges are based on outstanding and complex math, they are no match for quantum computing. Quantum computers are based on qubits instead of traditional bits. Traditional bits are binary and can only exist as a 1 or a 0. Conversely, qubits can exist in a superposition of 1 and 0. This means a qubit can represent numerous combinations of 1 and 0 simultaneously. So instead of systematically guessing one key at a time like a classical computer, quantum computers can try many keys simultaneously. The results of this operation can then be analysed, all wrong information being swept away, leaving only behind the correct key. This takes time to hack contemporary key exchanges from thousands of years to seconds. It was never that classical computers could not perform the operations to hack the key exchanges; it is merely the fact that the hacks would take far too long to be valuable.


Hash-Based Signatures
Code-Based Cryptography
Post-Quantum Cryptography (PQC)
Multivariate Cryptography
Lattice-Based Cryptography

Post-Quantum Cryptography Standardisation Project

Realising that quantum computing can exponentially speed up the time it takes to compromise public/private key pairings has led to a focus on quantum-resistant key exchanges from the academic mathematics community. In 2016, the National Institute for Standards and Technology (NIST) embarked on the «post-quantum cryptography standardisation project.» The project started with over sixty-five submissions and is currently in the fourth round of review and submittals. The proposals get put through the wringer each round, and even as late as round four, submissions have been deemed insecure. Two algorithms, SIKE and SIDH, which seemed very promising, were found to be insecure by way of a relatively simple hack in August of 2022, 6 years after their original submission. This shows how difficult it is to develop and test these quantum-proof algorithms. The





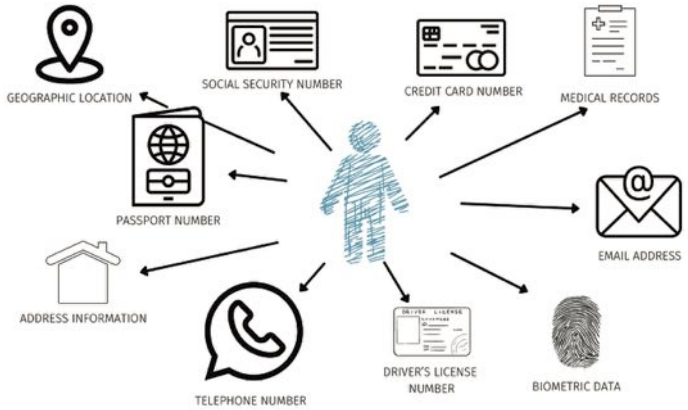
project from NIST is still active, with three other fourth-round submissions being evaluated and one being recommended for standardisation, CRYSTALS-Kyber. This is an extensive process full of significant testing and analysis – still, the pace at which post-quantum standards are set leaves a hole in data protection.

While some argue that this is acceptable because quantum computers are not widely available, I would submit a challenge to this thought. Cybercriminals are very intelligent and some of the cleverest minds around. So, while they might not have a quantum computer at their disposal, they still realise the ability for quantum computing and are preparing for the day they do. Instead of waiting for access to a quantum computer, cybercriminals are capturing large amounts of data today in anticipation. Once access to quantum is available, the criminals hope to decrypt the information they have been storing, gaining tons of sensitive data.

Your Personal Identifiable Information (PII)

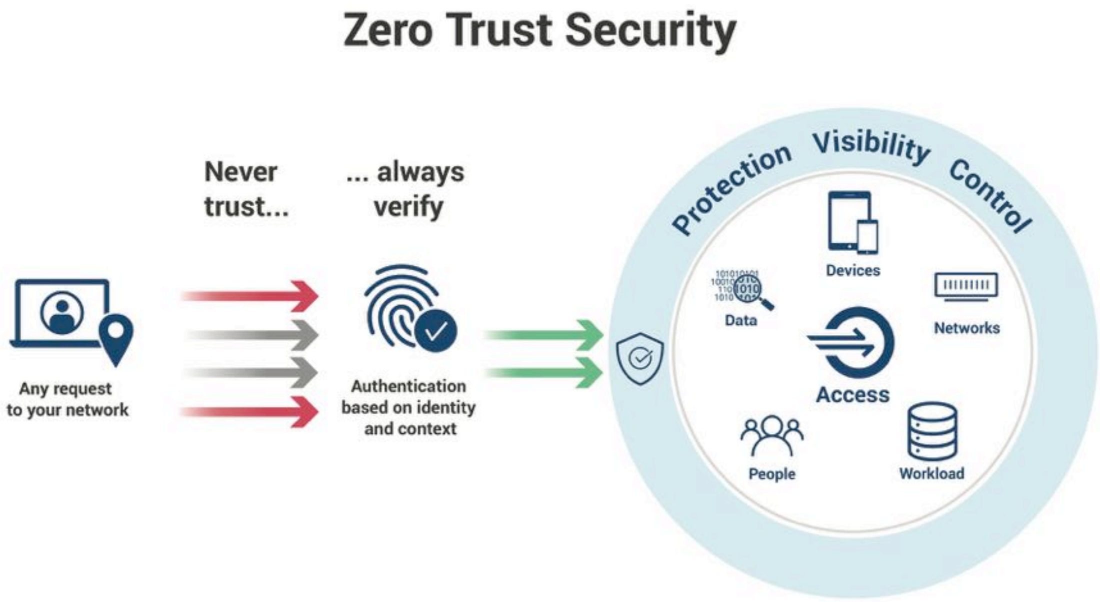
You might be thinking, 'well, that might be years from now, so will that information still be relevant?' M answer is yes. Here is an anecdote: I opened my checking account in 1996 and have the same account and routing numbers today. Some of the most sensitive and personal information in our lives rarely, if ever, changes. A few commonly accepted Personal Identifiable Information (PII):

- Name
- Address
- Email
- Telephone number
- Date of birth
- Passport number
- Fingerprint
- Driver's license number
- Credit or debit card number
- Social Security number



When was the last time these critical pieces of information changed? Some may happen more often than others, but it is rare. This compellation of data makes you who you are, which means it is used to prove identity. At some point, you must send some or all these pieces of information to different parties during significant life events. No more are the days of only handling consequential matters in person.

Cybercriminals are strategically trying to capture the secure transmissions that include sensitive data in hopes that they can utilise quantum later to



expose the data for nefarious acts. This circles back to my original point. Quantum is coming, the battle is here, and you should have some fear. The good news is that some steps can be taken to significantly reduce risk while we wait for standards and regulations that force the use and adoption of better security. This responsibility of increased data protection and prep for quantum falls to enterprises that provide applications used in consumers' day-to-day lives. It is hard for consumers to take steps independently aside from limiting the data sent, not downloading suspicious items, using VPNs, etc. Consumers must put trust in the mobile and web applications they use for data transference. With that trust comes immense responsibility for the enterprises providing these services, to keep customer data safe.

A shift in best practices & a focus on the future

So long are the days of reactive cybersecurity and doing the bare minimum best practices to protect data. Today's best practices rely on operating systems and communication protocols to orchestrate data protection. While these are essential, application providers are currently washing their hands of security and giving up control. This is why there are an overwhelming amount of zero-day attacks each year, resulting in millions of records being stolen, and this is without quantum computing. There needs to be a paradigm shift in security. Monitoring for breaches and data leakage is too late; the data is already gone. Organisations need to be more proactive in their approach to data protection. The hacks and breaches will never stop, so why not protect the data in a way that anticipates future vulnerabilities and keeps the data secure regardless?

The answer to this problem is quite simple. Incorporate a quantum-resistant application-level security that compliments securities that already exist. The current security strategies and best practices are great at what they do, but we need to do more. Adding a quantum-resistant data security layer to applications will protect data at its source. This contradicts current standards, where data is only secured once it arrives at the communication protocol via TLS orchestrated by the operating system. Data, in turn, is left unsecured as it bounces around before it is sent, promoting a loss of control for the data owners.

This model keeps application providers in constant catch-up, waiting for the next patch to make their data safe again. If instead, applications incorporate quantum-resistant security toolkits that they control, data can be secured without the reliance or intervention of any outside party. Data can be secured as soon as it exists in the application and only unsecured by the endpoint that interprets it. By doing this, the data remains secure regardless of who is in the middle, the operating system or communication protocol version, what malicious programs exist on a device, the network's security, or how many hops are involved in transporting the data, etc.

This may seem like a tall order, but as mentioned before, the basis of current security methodologies is already quantum resistant. It is only the key exchanges that are thought to be vulnerable. We possess the technology already. Security modules that use these base algorithms uniquely to ensure quantum-level protection exist today. These modules are self-contained, putting control in the hands of the applications, eliminating trust, and introducing redundancy to data security. The time is now for adapting such technologies and shifting the paradigm in data security.

Quantum is coming faster than we think. We see the anticipation spark initiatives for both the positive and the negative. Currently, all our data security eggs are in one basket. From an engineering perspective, this is an astonishingly lousy design. Businesses are proactive and have redundancies in all other facets, so why not in the security of their most significant asset, data? The time to add layers of data security is now, and we don't have to wait for quantum-proof key exchange to be official from NIST. Application-level quantum-resistant security modules are readily available and should be the primary focus of any enterprise's security initiatives. ■

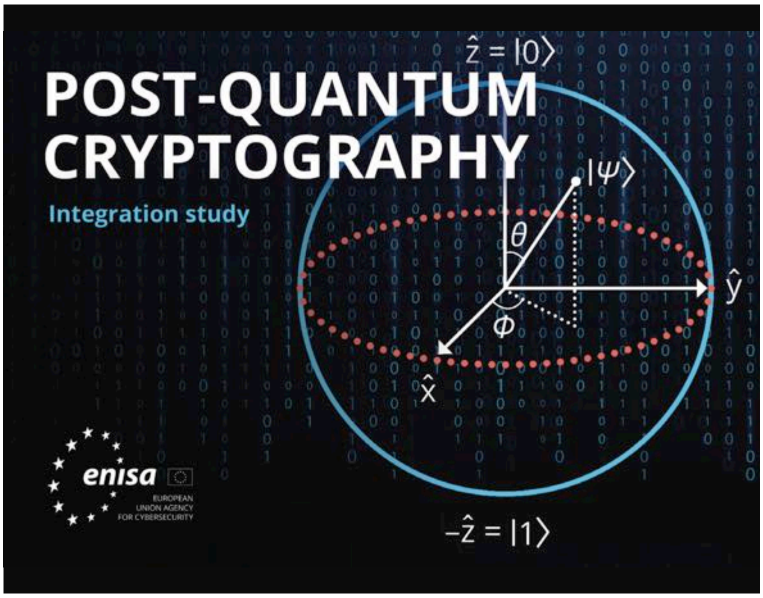
Securing the future: The race for Post-Quantum Cryptography (PQC).

Author: Marco Essomba

As we continue to advance in the digital age, our dependence on technology and the need for secure communication has become more vital than ever. While cryptography has been a cornerstone of digital security for decades, the advent of quantum computing presents new challenges to the security of our digital infrastructure. Post-Quantum Cryptography (PQC) is a promising new field that seeks to address these challenges and protect against the threat of quantum computing attacks.

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



Quantum computing is a revolutionary technology that has the potential to solve complex problems that are beyond the capabilities of classical computers. However, this same power also poses a threat to traditional cryptographic systems. Quantum computers can perform certain calculations that would take classical computers millions of years to complete, including breaking many of the commonly used cryptographic algorithms, such as RSA and ECC.

Post-quantum cryptography aims to develop cryptographic algorithms that can withstand quantum computing attacks. These algorithms rely on mathematical problems that are believed to be hard for both classical

and quantum computers to solve. The goal is to create a new generation of cryptographic systems that are resistant to quantum attacks while maintaining the same level of security and usability as current systems.

The development of post-quantum cryptography is crucial for securing our digital infrastructure against the threat of quantum attacks. While it is still in the early stages of development, it is important for organisations to begin planning for the transition to post-quantum cryptography. This will involve assessing the potential impact on existing systems and developing strategies for migrating to post-quantum cryptography.

However, post-quantum cryptography faces several challenges, including algorithmic efficiency, usability, and compatibility with current and legacy systems.

One of the key challenges in the transition to post-quantum cryptography is ensuring that the new algorithms are compatible with existing systems and standards. This will require a collaborative effort between industry, academia, and government to ensure a smooth, secure transition with minimal disruption. It will also require significant investment in research and development to ensure that post-quantum cryptography can interoperate with existing systems and standards to deliver the same level of security as well as usability as current systems.

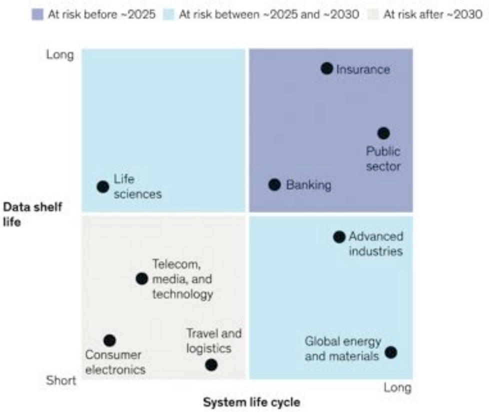
Ensuring algorithmic efficiency is also somewhat of a challenge. Many post-quantum cryptographic algorithms are currently slower and less efficient than existing classical cryptographic algorithms, which could be a barrier to adoption. Research is ongoing to improve the efficiency of these algorithms and to develop new ones that strike a better balance between security and efficiency. The National Institute of Standards and Technology (NIST) is yet to announce its recommendations on preferred algorithms. This is expected in 2024/2025.

Another challenge in the transition to post-quantum cryptography is usability. Ensuring that users have the necessary knowledge and tools to use the new algorithms effectively will be key. This will require extensive education and training programs for both developers and end-users to ensure that they understand the new cryptographic systems, how to use them securely and make it secure and accessible to a broad range of users.

Despite these challenges, there are promising solutions and predictions for the future of post-quantum cryptography. One solution is to develop hybrid cryptographic systems that combine both classical and post-quantum cryptographic algorithms. This would allow for a gradual transition to post-quantum cryptography while still maintaining compatibility with existing systems and standards.

Another solution is to develop new quantum-resistant cryptographic systems that are more efficient and easier to use than current post-quantum cryptographic algorithms. This would make it easier for users to adopt and use these new cryptographic systems, thereby accelerating their adoption.

Risk of quantum-powered attack by industry



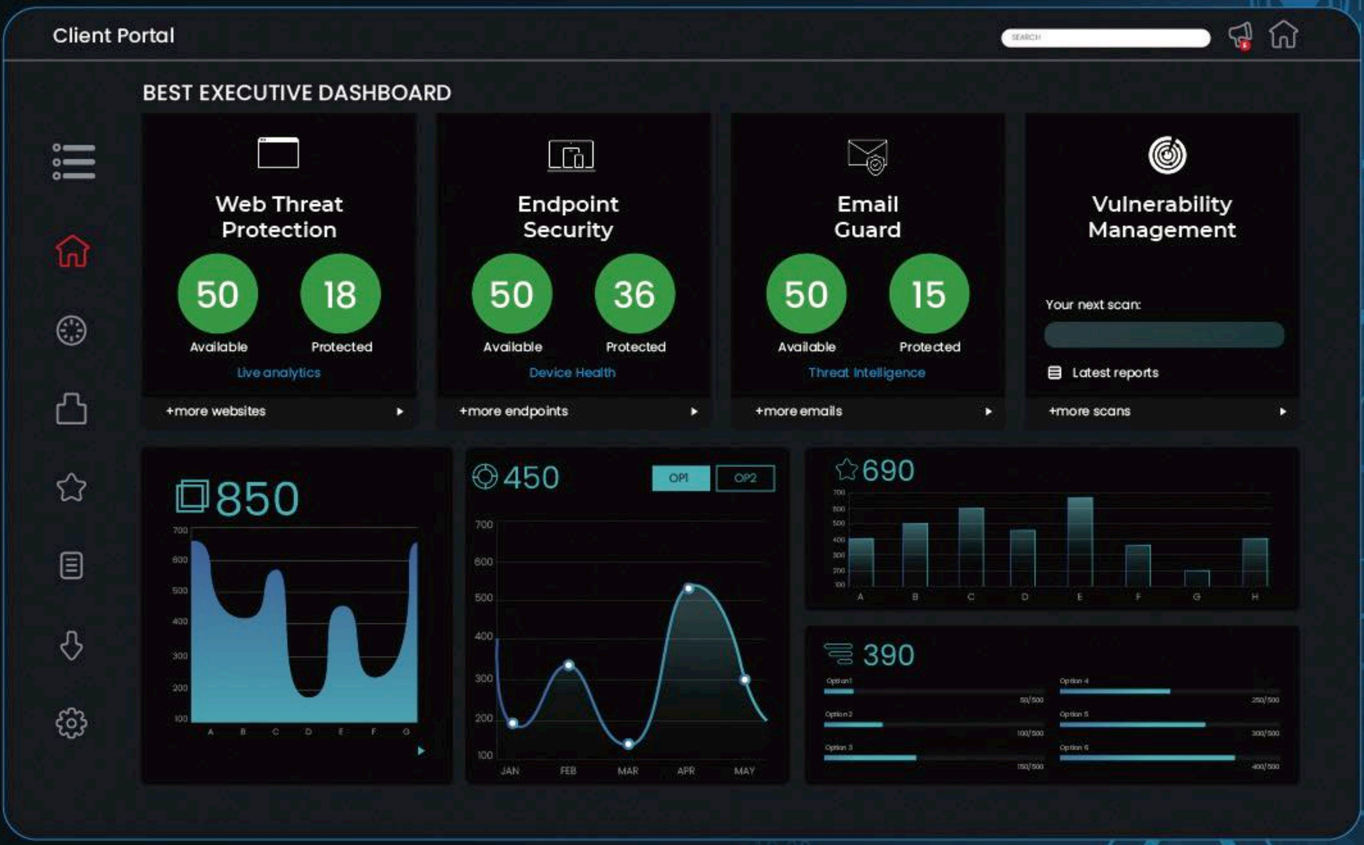
As for predictions, it is likely that post-quantum cryptography will become increasingly important as quantum computing technology advances. The development of quantum computers poses a serious threat to our existing cryptographic systems, and it is essential that we develop new quantum-resistant cryptographic systems to protect against this threat.

In the coming years, we can expect to see continued research and development in the field of post-quantum cryptography to protect our digital infrastructure against the threat of quantum attacks. As the development of post-quantum cryptography continues, it is important for organisations to begin planning for the transition to these new cryptographic systems. This will involve assessing the potential impact on existing systems, developing strategies for migration, and investing in education and training programs for both developers and end-users. By taking proactive steps now, we can ensure a secure and resilient digital future for generations to come. ■

BLOCKAPT™

BEST- Business Executive Security Technologies

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



Client Portal

BEST EXECUTIVE DASHBOARD

Web Threat Protection: 50 Available, 18 Protected. Live analytics. +more websites

Endpoint Security: 50 Available, 36 Protected. Device Health. +more endpoints

Email Guard: 50 Available, 15 Protected. Threat Intelligence. +more emails

Vulnerability Management: Your next scan: Latest reports. +more scans

blockapt.com

Future cyber tech & Future cyber defense.

Author: Chuck Brooks

In 2023, cybersecurity has reached a tipping point, the sheer volume of targeted breaches, attacks, and evolving threats has become overwhelming. This rising threat trend, coupled with the rapid growth of sophistication in malware, ransomware, DDoS, and social engineering attacks has created a conundrum. How do we protect ourselves in an increasingly connected and dangerous world?

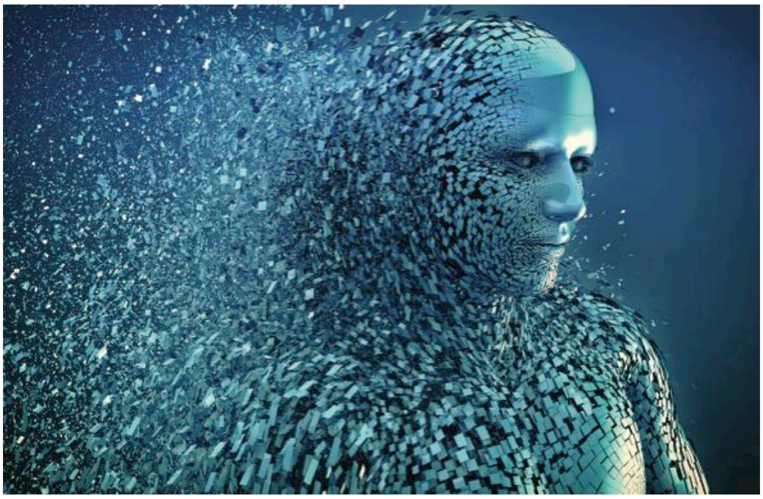
Nothing is completely un-hackable, but there is a myriad of emerging technologies that can help us navigate the increasingly malicious cyber threat landscape. A sampling of these innovative technologies include:

- Artificial Intelligence (human/computer interface) and Machine Learning
- Big Data: Real-time Analytics and Predictive Analytics
- Biometrics and Authentication Technologies
- Blockchain
- Cloud Computing
- Digital Transformation
- 5G
- Internet of Things
- Quantum-Computing and Super-Computing

Artificial Intelligence (AI) and Machine Learning (ML)

When it comes to adapting to new, sophisticated digital environments, AI and ML become key tools or innovative chess pieces in a cybersecurity strategy game. It will depend on the accuracy, speed, and the quality of the algorithms and supporting technologies to survive and thrive. To be competitive in a sophisticated game we need to be vigilant, innovative, and one step ahead.

Gartner describes artificial intelligence as a "technology that appears to emulate human performance typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogs with people, enhancing human cognitive performance or replacing people on execution of non-routine tasks.

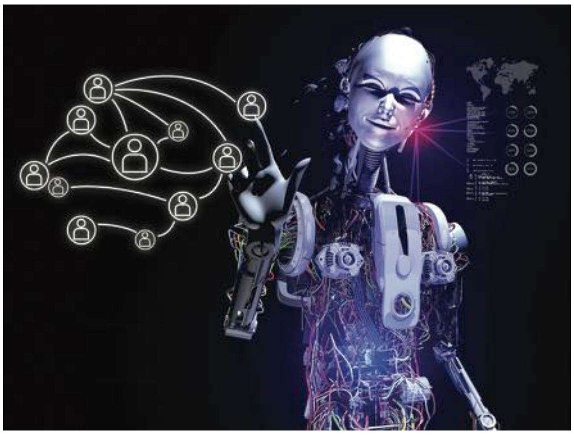


Some of the basic activities computers with AI and ML are designed for include Speech Recognition; Learning / Planning; and Problem solving. For cybersecurity, synthesising data is surely an advantage in mitigating threats. In a cybersecurity context, AI and ML can provide a faster means to identify new attacks, draw statistical inferences and push that information to endpoint security platforms. This is especially important because of the major shortage of skilled cybersecurity workers and growing attack surface.

Both AI and machine learning can be integral aspects of Automation and Adaptive Networks. Applications for automated network security and self-encrypting drives to protect critical infrastructure in all categories. Automation allows for horizon scanning and monitoring of networks that can report on deviations and anomalies in real time. It allows for automatic updating of defense framework layers (network, payload, endpoint, firewalls, and anti-virus) and diagnostic and forensics analysis for cybersecurity. It can also be used for threat vetting through incorporation of analytics in specialised databases.

AI – A double edged sword

While AI and ML can be important tools for cyber-defense, they can also be a double-edged sword. While they can be used to rapidly identify threat anomalies and enhance cyber defense capabilities, they can also be used by threat actors. Adversarial nations and hackers are already using AI and Ml as tools to find and exploit vulnerabilities in threat detection models. They do this through a variety of methods. Their preferred ways are often via automated phishing attacks that mimic humans, and with polymorphic malware that self-modifies itself to fool or even subvert cyber-defense systems and programs.



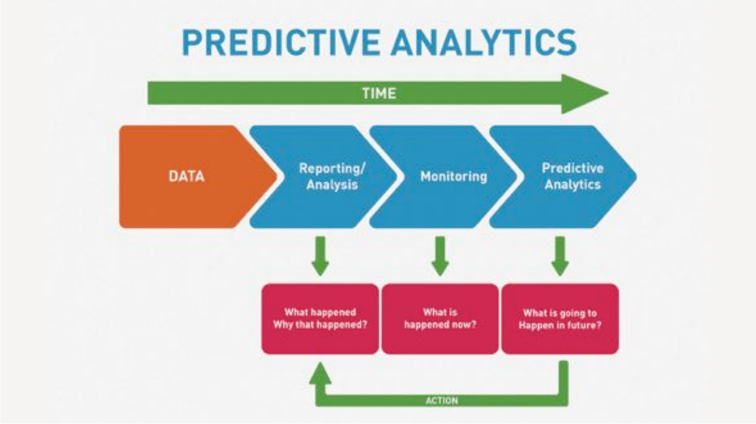
Cyber criminals are already using AI and ML tools to attack and explore victims' networks. Small businesses, organisations, and especially healthcare institutions who cannot afford significant investments in defensive emerging cybersecurity tech such as AI are the most vulnerable. Extortion by hackers using ransomware and demanding payment by cryptocurrencies may become a more persistent and evolving threat. The growth of the Internet of Things will create many new targets for the bad guys to exploit.

There is urgency for both industry and government to understand the implications of the emerging morphing cyber threat tools that include AI and ML and fortify against attacks. And investments are following suit. Markets and Markets estimates the AI cybersecurity market will reach $38.2 billion by 2026, up from $8.8 billion in 2019 — a CAGR of 23.3%.

Big Data: Real-time Analytics and Predictive Analytics provide an important component for cybersecurity threat intelligence. It can be applied to monitor and detect anomalies in the network and identify new threats without known signatures. It can also be utilised to correlate data from silos to understand the nature of attacks and assess network vulnerabilities and risks.

Big Data is comprised of the data governance of everything including geospatial data, 3D data, audio and video, and unstructured text, and social media. Like AI, machine learning, and automation, data analytics flourishes in the world of software algorithms combined with evolving computing firmware and hardware.

According to the Gartner IT Glossary, Big Data is a high volume, high-velocity and high-variety information assets that demand cost effective, innovative forms of information processing for enhanced insight and decision making. Eric Schmidt, former CEO of Google, estimated that we produce more data every other day than we did from the inception of early civilisation until the year 2003 combined. Therefore, organising, managing, and analysing data is more important than ever.



Biometric and Authentication technologies provides cybersecurity screening in both the network and endpoints. Screening can include numerical passwords, facial recognition scanning, and now screening via bio-signature. Every aspect of your physiology that can be measured can be used as a bio-signature. This includes heart/pulse rates, electrocardiogram sensor, blood oximetry, skin temperature. Multi-factor authentication is especially for securing isolated networks and to combat identity theft.

Blockchain is a peer-to-peer network with a shared, distributed ledger. Blockchain's decentralized technology offers cyber-defenses from many types of attacks because it removes single failure points that many often hackers' prey upon. It is already being used in the financial sector and offers selective transparency and privacy.

Cloud computing consists of moving and storing data and applications over the Internet from remote servers. Generally, it offers users cost flexibility, mobility, and increased productivity. For cybersecurity, it allows for firewalling and managed security. An advantage of the cloud is you know where the data resides and who is managing its security.

Digital transformation: Digital transformation includes digitising the customer experience, data flow, supply chain management, governance, engagement, e-government, and virtual government. In its basic description, it is turning paper into electronic records. Going from paper-based to electronically based systems of documentation requires data collection, processing, and analysis.

That transformation includes the immersive inclusion of digital technologies and cloud-based platforms. It also includes analytics, sensors, mobility, and a new era of automation impacting all industries and verticals including financial, energy, security, communications, and health. From a cybersecurity perspective, there are a lot of elements and surface attack space to protect from digital transformation.

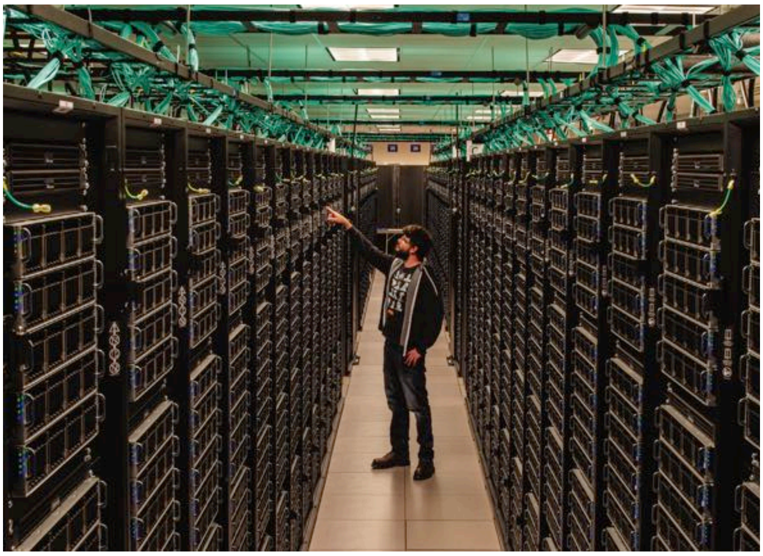
Last year at the annual World Economic Forum meeting in DAVOS, it was announced the combined value of digital transformation – for society and industry – could be greater than $100 trillion by 2025.

5G: Advanced 5G and wireless networks will benefit the government, including higher traffic capacities, lower latency, increased reliability, and by enabling processing and analytics in real-time. In government, 5G communications technology has been recognised as a foundational enabler for all U.S. defense modernisation programs and a priority for other agencies. When 5G is fully implemented, there will be more network traffic, there will be more and faster network wireless traffic, and there will be many more IoT devices. Cybersecurity solutions to keep up with the new "pace" of 5G is and will be a significant challenge.

Internet of Things: Internet of Things (IoT) refers to the general idea of things that are readable, recognisable, locatable, addressable, and/or controllable via the Internet. Gartner lists the pillars of IoT as: People, Data, Process, and Things. Mostly everything nowadays is connected to the internet by sensors. Cisco, who terms the "Internet of Things", "The Internet of Everything," predicted that 50 billion devices (including our smartphones, appliances, and office equipment) will be wirelessly connected via a network of sensors to the internet. IoT is conjoined with the Internet of Everything (IoE) Cisco defines IoE as the networked connection of people, process, data, and things. The benefit of IoE is derived from the compound impact of connecting people, process, data, and things, and the value this increased connectedness creates as "everything" comes online.

BIO

Chuck Brooks is a globally recognised thought leader and subject matter expert Cybersecurity and Emerging Technologies. Chuck is also an Adjunct Faculty at Georgetown University's Graduate Cybersecurity Risk Management Program where he teaches courses on risk management, homeland security technologies, and cybersecurity. LinkedIn named Chuck as one of "The Top 5 Tech People to Follow on LinkedIn." He was named "Cybersecurity Person of the Year for 2022" by The Cyber Express, and as one of the world's "10 Best Cyber Security and Technology Experts" by Best Rated, as a "Top 50 Global Influencer in Risk, Compliance," by Thompson Reuters, "Best of The Word in Security" by CISO Platform, and by IFSEC, and Thinkers 360 as the "#2 Global Cybersecurity Influencer." Chuck was featured in the 2020, 2021, and 2022 Onalytica «Who's Who in Cybersecurity» He was also named one of the Top 5 Executives to Follow on Cybersecurity by Executive Mosaic, He is also a Cybersecurity Expert for "The Network" at the Washington Post, Visiting Editor at Homeland Security Today, Expert for Executive Mosaic/GovCon, and a Contributor to Skytop Media, and to FORBES. He has an MA in International relations from the University of Chicago, a BA in Political Science from DePauw University, and a Certificate in International Law from The Hague Academy of International Law.



Cybersecurity is and will continue to be a major factor in both IoT and IoE. The Internet of Things (IoT) is directly related to supply chain vulnerabilities. IoT's exponential connectivity is an ever-expanding mesh of networks and devices. The increased integration of endpoints combined with a rapidly growing and poorly controlled attack surface poses a significant threat to the internet of things. With 23 billion IoT endpoints today (and that number is expected to triple by 2025), hackers can use DDoS (Distributed Denial of Service) attacks to devastating effects.

Quantum-Computing and Super-Computing have already arrived. IBM, Google, Intel, are all developing quantum computers. It works by harnessing the special properties of atoms and subatomic particles. Physicists are designing quantum computers that can calculate at amazing speeds and that would enable a whole new type of cryptography. Super computers are the engines for future automation. The future is promising.

There are many other emerging technologies that are part of the future cybersecurity toolkit. Security investments continue to be driven by persistent threats, policy remedies, workforce shortages, and technological innovation inside and outside security areas. They include edge computing, encryption, virtualisation, photonics, hypervisors, hardware-based trust anchors, anti-malware detection systems, and converged software defined environments. All will be needed in various applications for "security by design, "defense in depth," and "zero trust" as our world of connectivity morphs into a trillion-sensor economy with infinite surface attack vectors.

Unfortunately, it is not only the good guys who will have the new tech. Many of these emerging customisable cyber tech tools will also be available for exploitation by non-democratic sovereign states, organised criminal hackers, and malicious actors. In the future, cybersecurity just as it is now, will come down to a battle of skills, resources, and dedication by trained technicians and leaders orchestrating new tech tools. ■

Cybersecurity forecast: Stormy skies.

Author: Marco Essomba

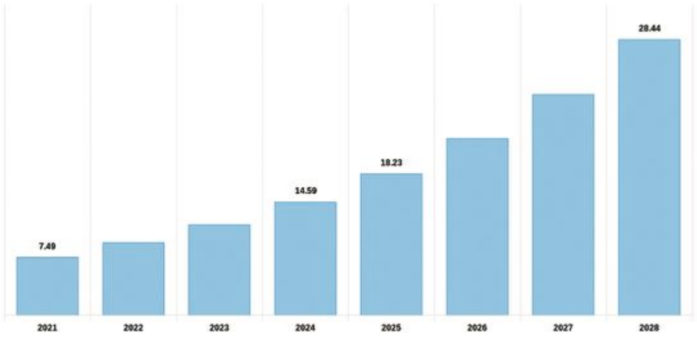
Cyber insurance

It is estimated that the global cyber insurance market will double in size by 2025, to reach a total market size of approximately 22 billion U.S. dollars. Generally, cyber insurance is designed to protect businesses from risks arising from the use of data and technology in business operations.

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

Cyber Insurance Market Size, 2021 To 2028 (USD billion)



During the past few years, cyber insurance has become a hot topic due to rising costs and compliance requirements. Insurers have experienced heavy losses by paying ransoms, which has led to increased costs and stricter security requirements for customers. In 2023, we anticipate that some industries, including healthcare, critical infrastructure, finance, managed service providers, and cybersecurity vendors, will face even more stringent regulations and higher costs from insurers. Some insurers may even require companies to use security solutions from recommended vendors before underwriting their policies. As a result, companies that do not follow cyber recommendations from insurers in targeted verticals should prepare for increased premiums and stricter compliance regulations.

To obtain affordable cyber insurance coverage, businesses must provide evidence of compliance with cybersecurity standards and best practices. They can conduct enterprise risk assessments to determine the maturity level of their cybersecurity program and proactively address underwriting concerns. Risk assessments can guide decisions around insurance gaps, limits, and coverage, and identify acceptable and unacceptable risks to be transferred to insurers.

It is anticipated that cyber insurance premiums will rise, along with the deductibles, while the coverage and pay-outs for claims are expected to decrease. Moreover, recipient eligibility may become more limited, with certain security benchmarks required to be met prior to coverage, which could prove unrealistic for smaller or less well-resourced organisations. Some sectors or types of organisations may also face exclusions from coverage, along with certain types of cyberattacks. In response to these changes, more companies may emerge as ransomware «brokers,» acting on behalf of victims to negotiate ransom payments. This trend could result in an increasing number of organisations seeking assistance from such brokers during times of need.

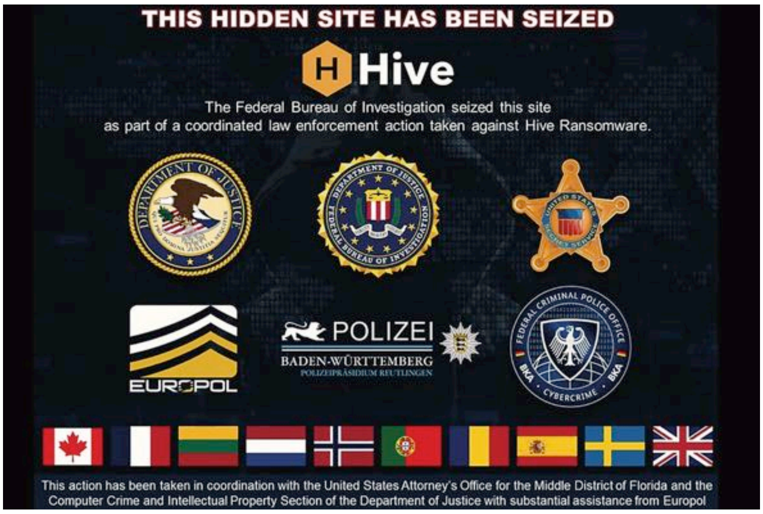
Ransomware

Gartner predicts that nation-states are likely to enact legislation about ransomware payments. In 2021, Gartner estimated that less than 1% of global governments have rules around ransomware but forecasts that figure will grow to 30% by 2025.

In 2023, cybercriminals will target data since it can be used for many purposes, such as ransom, identity theft, and targeted advertising. Breaches of Windows and Linux machines will be a critical data threat, and database breaches will continue. Ransomware will be a major vector for data theft and may be used to blackmail enterprises by threatening to expose data breaches publicly. Ransomware groups will adopt different operational models and new attacks, such as cloud-aware ransomware, as more businesses store their critical data in the cloud. Cybercriminals react to security strategies from law enforcement, governments, and private industries, such as cloud adoption and hardening networks.

All you need to do to get the pulse of the ransomware threat today is pull it up as a search term in the news on any given day of the week. Ransomware attacks happen in one of two ways: by opportunistic means, or by targeting someone or something. Targeted attacks are way more sophisticated and specific, and we have seen an increase in reports that indicate custom ransomware has been launched against an organisation's specific technology stack. In the crosshairs have been large organisations that are multinational, and through the definition of its services cannot endure a prolonged outage. More companies, more municipalities, and more core service businesses must be on the lookout, and ensure they are comprehensively protected by a triad of methods: secure the environment, have a plan to elegantly recover from a breach, and an ongoing assurance plan of security and compliance.

Ransomware is a destructive tool that cybercriminals frequently use. According to US security agencies, the Hive ransomware has extorted about $100m from companies since June 2021.



THIS HIDDEN SITE HAS BEEN SEIZED

Hive

The Federal Bureau of Investigation seized this site
as part of a coordinated law enforcement action taken against Hive Ransomware.

This action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol

DEPARTMENT OF JUSTICE
DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
EUROPOL
POLIZEI
BADEN-WÜRTTEMBERG
POLIZEIPRÄSIDIUM REUTLINGEN
FEDERAL CRIMINAL POLICE OFFICE
BKA
CYBERCRIME

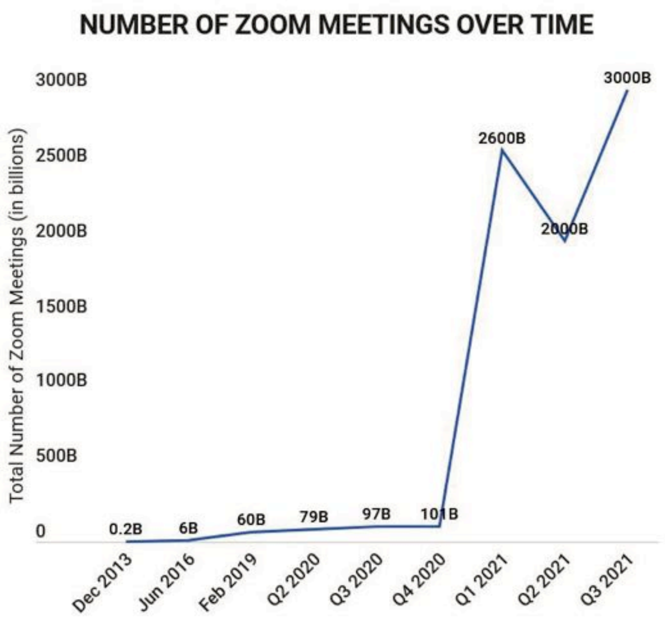
Miri Marciano, a cybersecurity expert, indicates that ransomware is increasingly dangerous due to its double extortion tactics, ransomware as a service and massive DDOS attacks. As a result, businesses are forced to seek managed security services providers to cope with the high competition for cybersecurity experts. To eliminate ransomware, Adam Brady, director of systems engineering for Illumio's EMEA operations, believes that governments and the industry must work together and eliminate the payment of ransomware. While new legislation is unlikely in the next year, discussions may arise about how to address ransomware.

Remote work

Research suggests that the chances of data breaches occurring are higher when employees work remotely. This could be due to factors such as less secure home networks, increased reliance on personal devices, and potential lapses in adherence to security protocols.

According to Zoom's user statistics, the platform experienced substantial growth throughout the COVID-19 pandemic. As of 2021, the number of daily active users surpassed 300 million, representing a staggering increase of 2,900%.

The pandemic caused many companies to shift to remote work in 2020, resulting in new vulnerabilities for businesses. Hybrid models of working will further alter traditional security architecture and expand the attack surface, says Kelly Ahuja, CEO of Versa Networks. The security technologist of VMware, Chad Skipper, warns of "island hopping" in 2023, where a threat actor hijacks an organisation's infrastructure to attack its customers. Remote desktop protocol is a top threat and must be a priority for all organisations, particularly in healthcare given the sensitive nature of personal health data and the regulations across the sector.



Many employees are now familiar with hybrid work, switching between working from home and the office. This means work devices move between secure and unsecured zones, making security a challenge. Enterprises will adopt zero trust models to combat these security issues. However, we anticipate that threat actors will increasingly target home devices connected to enterprise resources, with attackers pivoting into home networks connected via VPN to move laterally into the enterprise network. This tactic allows attackers to compromise the current network and potentially target multiple networks in the future.

Zero Trust

PWC's 2023 Global Digital Trust Insights Report reveals that over a third of CISOs (36%) have already initiated the deployment of elements related to zero trust, while an additional 25% plan to do so within the next two years.

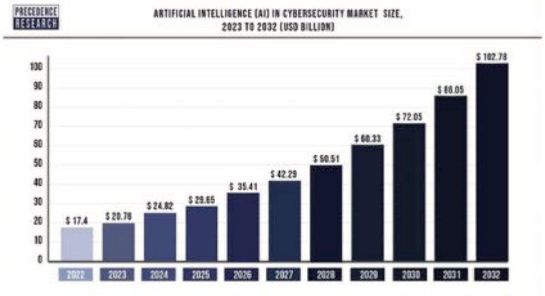
Many sources cite that the industry is still under utilising Zero Trust cybersecurity principles. Updated security platforms and tools are broadly adopting Zero Trust integration and for the most part, this appears to be a cultural and educational matter that will see increasing adoption in the year ahead. While Zero Trust is not the proverbial 'silver bullet' of cybersecurity, it is part of the foundation of evolving cybersecurity that strives to authenticate users everywhere possible in a modern cloud infrastructure.

Remote work is expected to continue, and VPNs may not be able to keep up with scalability demands and cybersecurity threats. The "zero trust" approach provides both scalability and high security by continuously validating and re-evaluating users. The Biden administration has mandated federal agencies to implement zero-trust architecture (ZTA) by 2024. Zero-trust network access (ZTNA) is projected to grow 31% in 2023, replacing VPNs entirely by 2025, according to Gartner.

Artificial Intelligence

In 2023, the cybersecurity artificial intelligence market will have a value of USD 22.4 billion, and it is projected to reach USD 60.6 billion by 2028, with a Compound Annual Growth Rate (CAGR) of 21.9%.

Tech companies, such as Cruise, Baidu, and Waymo, are testing self-driving cars, or robotaxis, in many cities worldwide, with claims of successful trips for delighted passengers. The appeal for businesses is cost savings from eliminating gig economy workers. However, there have been accidents, and hacking is a concern since internet-connected cars are vulnerable to attack, and humans can engineer AI. In 2023, it's possible security researchers or grey hat hackers could play a technical prank that causes a robotaxi to become stuck, potentially disrupting traffic. While we do not anticipate dangerous



Source: www.precedenceresearch.com

accidents, we expect at least one cybersecurity incident involving these new autonomous vehicles.

The emergence of ChatGPT and other AI technologies is likely to have a significant impact on the field of cybersecurity, with the potential to improve the ability of organisations and individuals to defend against cyber threats. However, it is essential to carefully assess the potential risks and challenges associated with these technologies and take appropriate measures to mitigate them. This could involve implementing stringent security protocols and safeguards to prevent unauthorised access to ChatGPT and other AI systems, as well as ongoing monitoring and evaluation to ensure their safe and responsible use. A range of intriguing use cases can be found below for reference.

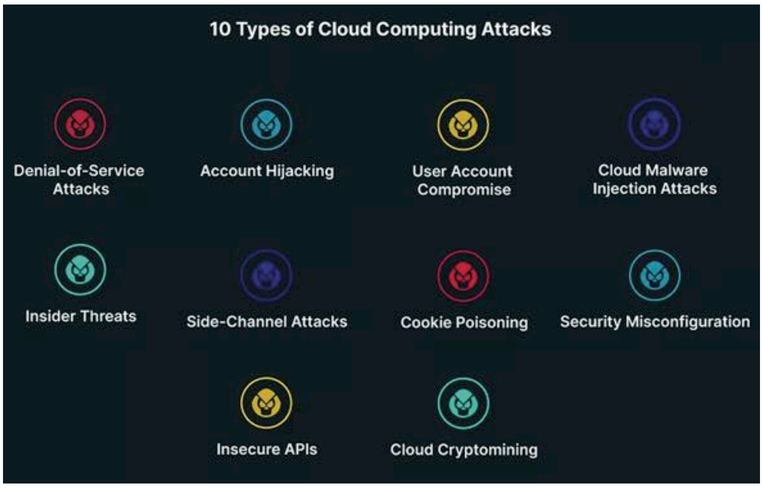
AI technology has rapidly advanced in recent years and while it has the potential to benefit various industries, it also presents new risks, particularly in cybersecurity. Miri Marciano, a cybersecurity expert, predicts that AI and machine learning will make social engineering-based attacks more effective by making it easier to collect data on businesses and employees. However, AI-powered cybersecurity systems like SIEM capabilities could be used to detect and respond to threats more efficiently. Meanwhile, there are growing concerns about deep fakes, which use AI to create fake images and videos of real people, being used for impersonation and social engineering attacks. David Mahdi, the CSO and CISO advisor to Sectigo, advises individuals to monitor their accounts regularly and choose biometric authentication methods carefully.

- Cybercriminals will leverage AI and machine learning to strengthen social engineering-based attacks, making it simpler and faster to gather data on businesses and employees.
- AI-powered cybersecurity systems like security information and event management (SIEM) will enable security teams to detect and respond to threats faster.
- Deepfakes, which use AI to create fake images and videos of real people, are likely to be used by cyber attackers for more social engineering attacks and impersonation. This could make biometric authentication methods less useful, and individuals should monitor their accounts regularly for financial services.
- Adversarial attacks against AI systems will become more prevalent as attackers seek to manipulate or evade detection by the system. This could impact the security and reliability of AI-powered systems, such as autonomous vehicles or medical equipment.
- The use of AI in phishing attacks will increase, with attackers using machine learning to create more convincing and targeted emails. This could lead to higher success rates for phishing attacks and more data breaches.
- AI-generated fake news will become more widespread, potentially impacting elections or financial markets. This could lead to significant social and economic disruption and highlight the need for better detection and prevention methods.
- The use of AI to automate attacks, such as through the use of autonomous malware or botnets, will increase. This could lead to a more significant and rapid spread of malware and more sophisticated attacks.

Cloud Expansion

According to Check Point Research (CPR), there has been a 48 percent rise in cloud-based cyber attacks in 2022 compared to the previous year, likely resulting from the heightened adoption of digital transformation initiatives leading organisations to shift their operations to the cloud.

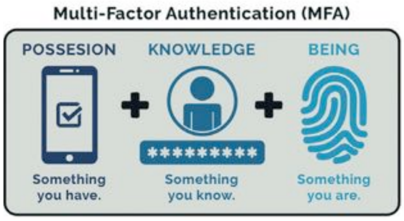
Over the past three years, businesses have rapidly shifted to the cloud and adopted new cloud technology, which has been integrated into the hybrid work environment. However, the biggest challenge facing enterprises is inconsistency across cloud applications due to varying abilities, features, and cost structures of different cloud vendors. This inconsistency could lead to security issues, particularly since many CISOs may not be familiar with new technologies or lack the bandwidth to oversee all cloud vendors. Misconfigurations from users and developers may also arise, as cloud developers may prioritise agility over security. One area of concern is the potential security threats of cloud APIs on connected cars, which are new and complex systems with multiple vendors providing different components. As a result, it may be increasingly difficult to guarantee security for each of these vendors.



In 2023, it is expected that multi-cloud data infrastructure adoption will become the standard as organisations evaluate their current infrastructure, including both on-premises and cloud-based systems. To remain competitive, flexible, and secure, organisations will aim to transform cloud computing into a uniform capability, reducing the overhead and integration complexities of managing cloud services and supporting applications. Security will be a critical concern, particularly when it comes to managing data and configuration in different cloud environments and ensuring unnecessary exposure is minimised through proper control mechanisms.

MFA

In 2023, threat actors will target multi-factor authentication (MFA) users through new vulnerabilities and bypass techniques, relying heavily on social engineering. Increased adoption of MFA, currently at **40%, will require attackers to find ways around these security solutions to succeed**. Attackers may use push bombing and AitM techniques that capture authentication session tokens to bypass MFA. Expect many more MFA-targeted social engineering attacks next year.



MFA is a security practice used by sectors like online banking and social media to enhance cybersecurity. But, hackers have exploited technical and human vulnerabilities in MFA systems. More organisations adding MFA layers has led to "MFA fatigue" among users, and attackers exploit this to overwhelm employees with approval requests. Notification fatigue was used in several high-profile attacks last year, including the Uber data breach. Miles Hutchinson, CISO of Jumio, predicts businesses will seek alternative verification methods, such as passwordless authentication, to avoid MFA fatigue.

Supply chain

Supply chain attacks grew four-fold in 2021 as hackers targeted smaller organisations in the supply chain with weaker defences. **Gartner forecasts a three-fold increase in software supply chain attacks by 2025, with 45% of organisations expected to experience such incidents.** CEOs and boards are pushing for security enhancements in their supply chains, leading to greater demand for solutions and services that can catalogue and monitor cyber risks in third-party vendors and suppliers.

Due to the interconnected nature of tech businesses, supply chain attacks are becoming increasingly common and disruptive. Organisations need to consider the security of external companies they work with, as exemplified by the 2020 breach of Solarwinds, which served as a "wake-up call" for companies, according to Zoom's head of security assurance, Sandra McLeod. Cybersecurity experts warn that in 2023, supply chain attacks pose a massive risk, with attackers becoming faster at exploiting vulnerabilities. To prepare for future risks, proving cyber resilience is crucial, says Kev Breen, cyberthreat research director with Immersive Labs. In response to the wave of supply chain attacks that affected several organisations on its site, GitHub launched a new strategy to enhance the security of open-source projects last October.

Quantum Security

Quantum computers are becoming a reality. They will enable great technology innovations in the future, but equally will bring significant risk in many fields, especially in cyber security. The World Economic Forum (WEF) has identified quantum computers as a significant threat to cybersecurity worldwide. As quantum computers become more and more powerful, the direct threat they pose to current encryption systems is real.

In 2023, organisations will increasingly acknowledge the risks posed by quantum computers and will plan accordingly in order to mitigate that threat. Organisations will start to plan ahead and have deeper understanding in ways in which quantum computers can challenge the integrity of digital documents, break current encryptions, and tamper with sensitive data such as health and financial personal data.

The nature of the quantum threat is such that it cannot be left to the last minute. Organisations must plan years ahead, given that the protocols that we rely on the internet for day to day transactions such as online banking, secure messaging, virtual private networks, etc. are at risk. Switching to quantum secure systems will take years to plan and to implement. For that reason, preparation is key.

The United States has already started the preparation process by initiating the Quantum Computing Cybersecurity Preparedness Act. This legislation re-enforces that the quantum threat is real and must be taken seriously by organisations today. ■

Useful Links:
https://www.forbes.com/sites/forbestechcouncil/2023/01/02/six-cybersecurity-trends-you-can-expect-in-2023/?sh=384e60f24c97
https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2023
https://www.watchguard.com/wgrd-resource-center/cyber-security-predictions
https://www.cisecurity.org/insights/blog/our-experts-top-cybersecurity-predictions-for-2023
https://www.siliconrepublic.com/enterprise/cybersecurity-predictions-tech-trends-2023
https://www.forbes.com/sites/emilsayegh/2022/12/15/top-cybersecurity-predictions-2023/?sh=75b04322383f
https://www.weforum.org/agenda/2022/09/organizations-protect-quantum-computing-threat-cybersecurity/
https://thequantuminsider.com/2022/12/15/quantum-computing-cybersecurity-preparedness-act-passes-senate-awaits-presidents-signature/

Top 2023 prediction? Our industry needs to do more plain speaking.

Author: Ian Kennedy-Compston

If you do an online search on the cybersecurity threats facing individuals, businesses, public sector organisations or governments you'll find many, many opinions on what 2023 may hold. Most of those opinions overlap in some way simply because the threats are fairly obvious and many of them continue to be an issue carried over from previous years.

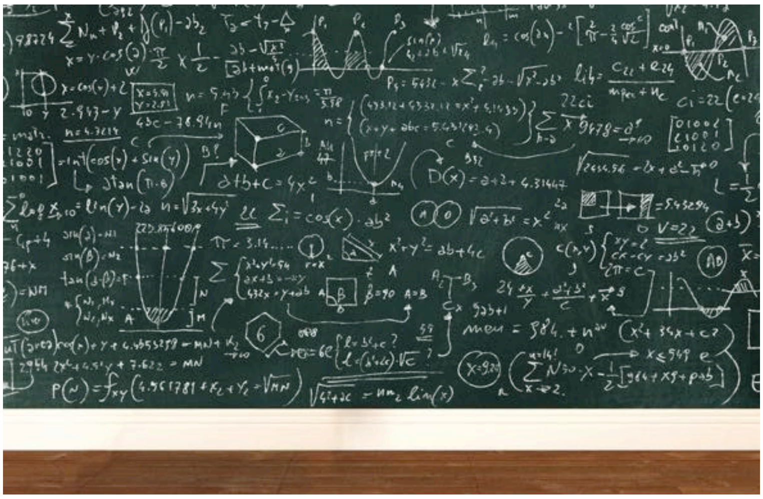
Ransomware, malware, DDoS attacks, system security, multi-factor authentication, lack of employee training - these all continue to be vulnerabilities exploited by cybercriminals. Of course, there are some which are emerging and presenting all sorts of new challenges, like the growth of deep fakes and the recent concerns about cloud storage security. Every new development in technology is a potential cybersecurity nightmare, opening the door for mischievous individuals or wholescale cybercrime organisations to create havoc and a potentially massive income stream from those who fall victim.

Perhaps the thing to consider is not so much the threats – continuing or emerging - for 2023, which have been written about a lot over the past few months, but why some of these threats continue to cause such issues when the cybersecurity industry is working hard to understand and anticipate risks and develop products and services to minimise their impacts worldwide.

Often, when I talk about what I do with people from not within the industry, I'm struck by how many people don't really understand it. Cybersecurity still has the reputation for perhaps being the dark arts, an industry built on smoke and mirrors or scare-mongering.

BIO

Established in 2017, Ian is the CEO of EnterpriseRed, which is rapidly becoming one of the UK's innovative organisations in providing advanced cybersecurity solutions to a broad customer base. EnterpriseRed offers the full spectrum of solutions and services from a managed SIEM to automated PEN testing and more. As members of the MSSP Alliance and working in accordance with Cyber Essentials Plus and ISO-27001 standards, Ian has been the driving force to position market leading products that are solution led, offering the most advanced cybersecurity capabilities on the market. Ian has propelled EnterpriseRed's team in gaining accreditation of 25 of the leading cybersecurity solutions, including BlockAPT, PenTera, Cybsafe, Hornetsecurity, BlackBerry software, LogicGate and many other leading products. Ian and his team's work over the past few years has catapulted EnterpriseRed as a leading trusted advisor in cybersecurity bringing clarity where and when it is needed.



My prediction, therefore, about one of the biggest cybersecurity threats this year is the ongoing failure of those of us within the industry to communicate better with potential customers.

We must focus on simplifying the language we use when communicating with customers. Failure to do so will continue to deter too many of them from engaging with us, leaving them vulnerable to attack or breach. The truth is, the more we simplify things, the more we'll connect with customers and the greater the chance they'll work with us to help them reduce their risks.

Our EnterpriseRed team recently did a bit of an audit among cybersecurity organisations – including vendors, distributors, service providers and resellers, checking out their websites to see how user friendly they are. If you've done this yourself lately, you'll probably have seen that, unless you're an experienced IT professional, the content might just as well be in Swahili. The truth is, many cybersecurity companies employ geniuses who are totally brilliant at understanding the threats and developing products and services aimed at helping reduce risks, but who are not so good at connecting or engaging with potential customers. Websites, product information and marketing materials are complex and hard to decipher unless you're an IT pro.

For a bit of fun, we took a training quiz from one of our vendors and weren't entirely surprised to find that (a) some of the questions were actually hard to understand and (b) the answers were nowhere to be found on their websites no matter how many product fact sheets we scoured. It's clear that their marketing materials are written by IT experts who know those products inside out but who struggled to articulate the features and benefits clearly. Luckily for us, we know what all those acronyms mean and we know what their products can do to help businesses but not everyone who will engage with them has that same level of knowledge and expertise.

This isn't a new thing, of course. Go back 40 years and insurance companies were just as bad. In those days, most individuals or companies didn't actually talk to an insurer but had a friendly, local broker who did the liaison for them – someone who could speak the customer's own language. Then the whole insurance market imploded with the arrival of direct insurers and suddenly the industry realised they had to up their game in terms of making themselves clearer to end personal or commercial customers. Nowadays, most insurance websites are aimed at non-insurance experts, with clear, concise plain English and far easier to understand policy documentation to avoid confusion. There may be room for further improvement but they've put a lot of effort into building better understanding and communication.

This is the kind of approach I think we need to take within cybersecurity. We need to do more to improve the way we communicate and connect with potential customers.

Of course, if your customer is a major organisation with its own IT security professionals, the chances are they understand the myriad acronyms and technotalk they hear or read when engaging with the industry. These people are often the equivalent of the insurance brokers – liaising between their management board and the cybersecurity industry to match needs with solutions. The trouble is, not every business has a Chief IT Officer or Chief Information Security Officer or equivalent.

We often work with small to medium-sized businesses where decisions on cybersecurity are made by a management team who have wide remits, who are experts in their own company's products or services but not fluent in cyberspeak. The first hurdle is getting cybersecurity on the agenda at all, especially at a time when today's economic and other pressures are so great. Who can blame them for prioritising focus on the many other priorities they face every day, especially when we make it so hard for them to engage with us?

At best, for many business leaders, cybersecurity is low on the priority list and is often something they consider as a distress purchase rather than something that can protect and improve their bottom lines. For those who seek to learn more, the information available to them from many industry players must be bewildering.

Cybersecurity is a huge and growing market, worth an estimated $155 billion last year and projected to more than double in worth by the end of this decade. However, this figure could be far higher if we could just work smarter at connecting better with potential customers and helping them understand why spending money on cybersecurity is not only necessary but a good investment.

My years of experience has proven that the best way to help them understand their cyber risks and what to do to mitigate them is to listen to them, find out all about their business and talk in their language, not ours. By speaking in plain English and avoiding all those industry acronyms and cyberspeak whenever possible we aim to build a relationship with them whereby they feel part of the conversation, not alienated by it.

This is what we need to do better as a collective: if we invest in better communications and engagement skills as an industry, if we take time to build relationships and understanding of our customers' businesses, then we will become trusted business partners. It doesn't matter how genius a solution is if a company or its representatives cannot explain it easily.

If we resolve to improve our communications skills, we are likely to gain the attention of more of those businesses who are currently resistant to engaging with us. This offers our industry a huge opportunity for even greater growth and, more importantly, will help us to help them build greater resilience against cyber threats. ■

Cybersecurity: The new playing field.

Author: Nicola Sotira

Since ancient times people have been trying to predict the future and, on issues pertaining to digital, make predictions about technologies. Cinematography in this has long accustomed us in painting despotic scenarios. Many films, in recent years, have provided an apocalyptic vision of the world made up of alien invasions and sick worlds and population crises under oppressive policies. Indeed, dystopia has found fertile ground in cinema and the silver screen by sowing doubts and troubling messages about the future. A dystopia that feeds on characters oppressed by the landscape in which they live made of rigid laws and balances that cannot be shaken. In these scenarios there is no single antagonist; evil is scattered within a sick society that lives in and is subject to certain compromises. Leaving aside this cinematic parenthesis for a moment and returning to those who work in the field of cybersecurity, prediction is based on elements that are already visible and often already present. Therefore, while for the casual reader, the topic of forecasting on cybersecurity issues may sound like guesswork, for those working in the field it is incumbent to anticipate events proactively, anticipating what cyber-crime may be planning. So, let's try in this article to suggest some trends that we are observing, themes that are still immature in some areas, but which technological speed is bringing to the forefront, and which will soon be coming out of the headlines to become themes that CISOs will have to deal with practically.

BIO

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

Staying in the Cloud

I believe that in this transitional period, when many companies are still evaluating and reviewing their infrastructures, both on-premises and in the cloud, the acceleration in favour of multi-cloud infrastructures will take off rapidly in 2023; the key drivers of this will be competitiveness and flexibility of organisations. Cloud computing will be instrumental in simplifying IT spending, streamlining processes, and finally making that digital

transformation run that will be key to generating new business for companies, and greater efficiency in the public administration sector. Let's also prepare for a lot of buzz on the topic of SASE (Secure Access Service Edge) - a technology that is about to get a major boost in the area inherent to cybersecurity as well. Organsations are increasingly looking for simplified solutions, technology stacks that realise an alignment between performance and security in a scenario where user data becomes diverse, distributed and as far as the security issue is concerned more vulnerable. It is legitimate to think of protected data getting closer and closer to the edge of the network effectively zeroing the minimum distance to the end user. Scenarios that will require a rethinking of security operations and the entire monitoring theme.

Ransomware on the rise and increasingly targeted

If anyone still does not have a sense of how this scenario has seen an exponential increase in attacks and victims, they can safely do a search on the search engines to see how news regarding this issue is the order of the day and present now in all the major news outlets. In this context, we have seen increasingly targeted and sophisticated attacks in addition to, the increase in numbers; as reported in various reports, ransomware is increasingly being customised and diversified so as to be effective once launched against a specific technology stack of an organisation. In the crosshairs of these attacks have ended up large organisations, multinational corporations, and services that can hardly afford a prolonged interruption of services. More and more companies, municipalities, public administration, and health care organisations will need to ensure that they are fully protected in addition to verifying the full functionality of backup and Disaster Recovery (DR) processes along with their business continuity procedures. Integrating scenarios that provide for periodic exercises simulating this type of incident and thus testing procedures, people with special attention to the whole topic of communication with the outside world that must be prepared and integrated into the organisation that will deal with incident management and business continuity.

API and 5G

The 5G mobile network is reaching a whole new dimension that can be an accelerated vehicle to many of the existing threats. In addition, automation, and integrations from cloud to app, app to app, ecosystem to ecosystem, and beyond, all imply the presence of different APIs which, for the cybercriminal, means more surface that can be exploited. The design, therefore, of new secure software solutions must move from more security integration in the infrastructure, in the network, all the way down to the application in the stack. Between 5G connectivity, weak IoT cybersecurity standards, and an ever-expanding world of APIs, it won't be long before flaws, yet unknown, result in high-impact incidents.

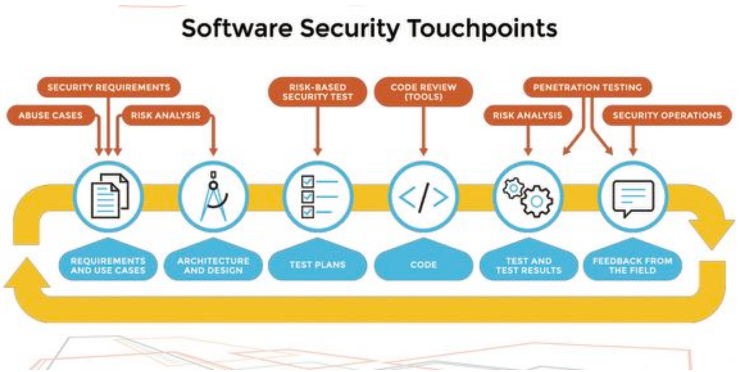
Training and cybersecurity

Training continues to be one of the issues to be taken care of and in case, it has not been done, implemented as a regular measure in organisations. Humans have not evolved to detect dangers in the digital world; we are still very much anchored in the physical world and its dangers. Moreover, the education system does not teach how to defend against the dark arts of

cyber-attacks. Human risk remains, therefore, an organisational problem. It will therefore be our responsibility to equip our employees with the necessary skills to understand how to counter direct-to-person cyber-attacks such as, for example, phishing attacks. Automation, adaptive learning, and artificial intelligence/machine learning can help provide personalised training on a large scale. Certainly, these technologies will support us in increasing engagement so that people can participate in relevant training that stays at the edge of their skill level to improve and stay engaged. It is proven that a long, dry video followed by a punishment-based phishing simulation does not work. Fixating on failure leads to failure. Rewarding people as they acquire skills in a dynamic learning environment confers measurable improvement. This approach broadly describes gamification, whose proven success is based on established behavioural science and business principles and will be critical to protecting organisations of all sizes for years to come.

Software security and procurement

Lately, all nations have begun to address the issue of risks and vulnerabilities arising from B2B and B2C technologies created, developed and operated by foreign countries, a recent example being TikTok, a Chinese cloud software. This has begun to raise many questions about where the code and applications come from, what data is put into these applications, and the sovereignty of this data. In 2023, we will begin to see more scrutiny of the provenance of developers and code and more and more organisations focusing on software composition analysis and secure code development. In essence, it is about questioning every component of our nation's supply chain. Covid has challenged our supply chain in general, and this year we will begin to see more attention to the security risks associated with our supply chain that feeds software development from abroad.


Software Security Touchpoints

Cyber Insurance

In recent years we have witnessed the death and rebirth of the cyber insurance industry. Cyber insurance companies have experienced cost increases in the areas of ransomware and incident recovery. In response, premiums are beginning to skyrocket, new pre-policy cybersecurity compliance standards will become the industry norm, and conditions, I believe will change. Therefore, rising cyber insurance premiums and stricter requirements to obtain cyber insurance can be expected, which are interesting themes to watch in 2023. On the other hand, we are also likely to see an increase in demand resulting from the growing incidence of supply chain problems. Because of these problems, it is likely that companies will begin to increasingly require that the suppliers or third parties they work with have cyber insurance.

Automation

In this year, we will certainly see automation move into the few remaining areas of security operations that still depend on manual processes. These areas include threat exposure management, which helps to holistically answer questions that want to clarify our ability and preparedness to detect and respond to attacks. Another area that will become increasingly automated is detection engineering, which still depends heavily on specialised skills and tribal knowledge. Automation will not only reduce risk for these organisations, but it will also free SOC staff from mundane tasks so that they can focus on more interesting challenges that really require creativity and human innovation, such as threat hunting and understanding new and novel attack behaviours.

Open AI, Chat GPT

Chat GPT, or rather Generative Pre-trained Transformer, is an advanced form of AI technology developed by OpenAI. It is a language model that can understand natural language and generate text indistinguishable from human writing. Chat GPT has been trained on a huge amount of data and can produce coherent and

grammatically correct sentences. How will ChatGPT revolutionise the cybersecurity industry? Chat GPT has the potential to revolutionise the cybersecurity industry in several areas. For example, we can expect a definite improvement in threat detection, Chat GPT certainly can help improve threat detection capabilities by analysing large volumes of data and identifying potential cyber threats. It can analyse data patterns to identify suspicious behaviour and detect anomalies that could be indicative of an attack. Another area will be incident response, here time is of the essence. Chat GPT can support security teams to respond more quickly to incidents by analysing data in real time and making recommendations for countering them. And ultimately, also in improving decision making.

Watch for economy recession

It is very likely that the recession will cause a reduction in spending, and many of the investments in the bellies of organisations will be revised or will be subject to revising. Despite the idea that cybersecurity may be a recession-proof industry, it is likely that staffing and quality will suffer some setbacks during the economic downturn. There are currently no cuts in basic cybersecurity budgets, but it is likely that more discretionary areas, such as training budgets, or driven innovation may be reduced. When it comes to training, the industry is already facing a skills shortage and, unfortunately, this shortage is likely to worsen as the recession arrives in 2023. ■

A publication

swiss webacademy web for business

edited by:

BLOCKAPT™

Copyright:
Copyright © 2023
Swiss WebAcademy and BlockAPT.
All rights reserved.

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

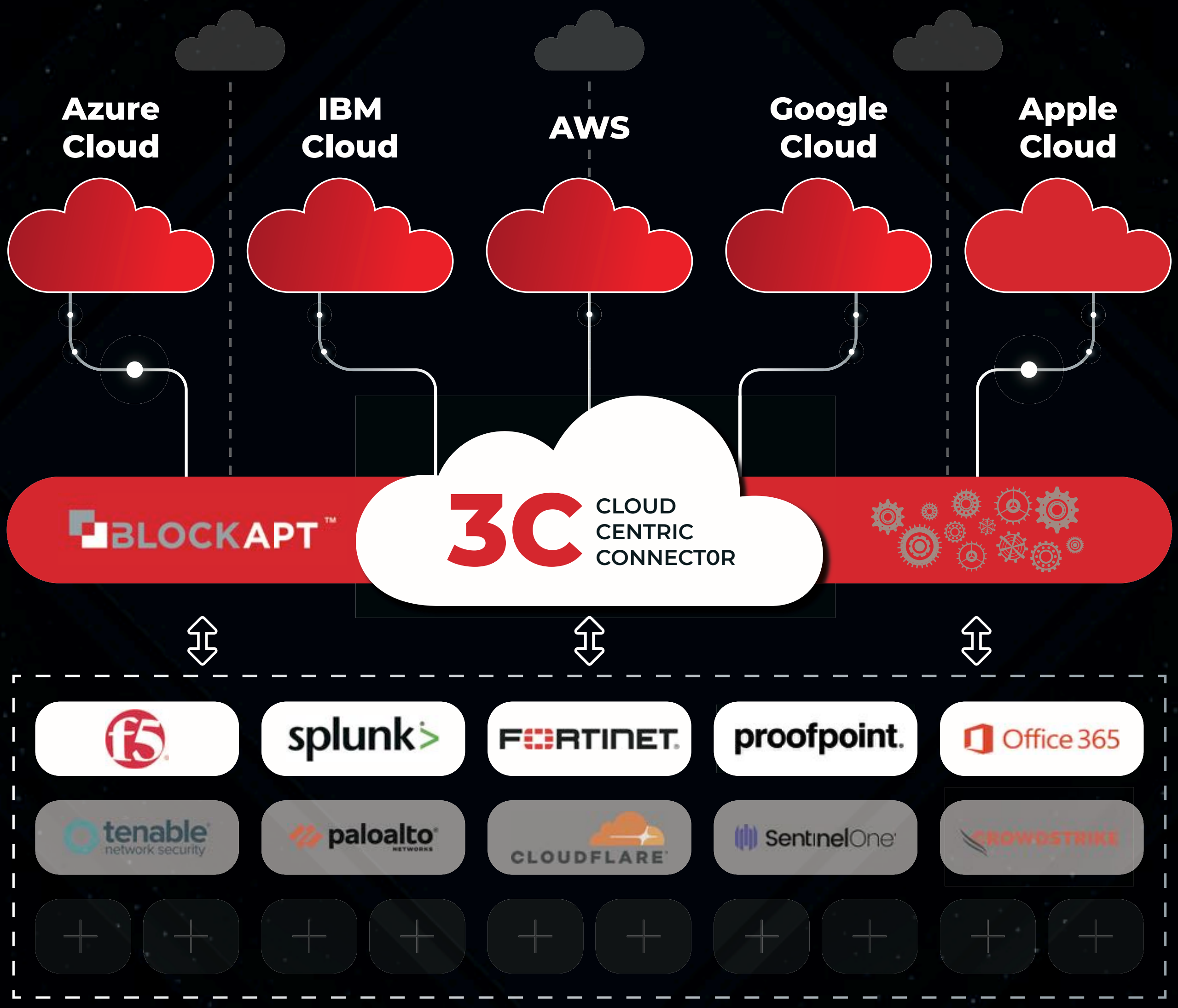
BLOCKAPT™

Swift Response

Against attacks you least expect.

BLOCKAPT™

Centralised Cloud Management & Native Control



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

blockapt.com