Cybersecurity Trends

UK edition n.3 / 2021

Special edition:
Geo-focus on security

visit us:

Milipol
PARIS 2021

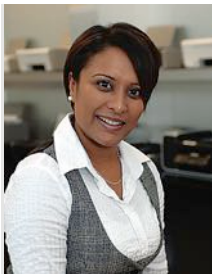
BLOCKAPT™

The cyber threats of tomorrow, tackling ransomware, security automation... and more.


BLOCKAPT™
Supercharge your SOC, NOC
& Remote Operations.
Single platform experience
info@blockapt.com
blockapt.com

Contents

On the front lines of global security.



Authors: Raj Meghani, Marco Essomba, Laurent Chrzanovski

We are back with Cybersecurity Trends UK issue 3. It has been quite a year for us (and for you the readers too, we presume).

This is a very special edition as we have extended our reach, spoken and engaged with renowned and industry leaders across the globe to bring you a global geo-focused cybersecurity state-of-play that includes interesting views, thought-leadership and research.

The UK is a 'second-tier' cyber power

Tier distribution of 15 countries with developed or developing cyber capabilities*

Tier 1	Tier 2	Tier 3
World-leading strengths in all categories	World-leading strengths in some categories	Strengths or potential strengths in some categories but significant weaknesses in others
United States	Australia	India
	Canada	Indonesia
	China	Iran
	France	Japan
	Israel	Malaysia
	Russia	North Korea
	United Kingdom	Vietnam

* Capabilities assessed: strategy and doctrine; governance, command and control; core cyber-intelligence capability; cyber empowerment and dependence; cyber security and resilience; global leadership in cyberspace affairs; offensive cyber capability

Source: International Institute for Strategic Studies TECHMONITOR

Are they all facing similar challenges? Or do they have a different take on things? And if, so how are they addressing these? Stay tuned to find out.

Beyond this, we continue with a shining light on Ransomware, which as you know has taken many forms and will continue to do so. The emergence or rather the easy procurement of an outsourced Ransomware-as-a-Service (RaaS) model has meant that extortion for money is now easily accessible to less technical folk and is becoming the go-to method.

For the ever-transforming industries and organisations, automation is a key win in streamlining workflow processes across security and the way to address the forever struggle of resource shortage or constraints or simply to manage to utilise resources better. This is another area we will be looking at.

Across the many industries we speak to, automation is still perceived as an expensive exercise and thus left as an afterthought for the future. We hope to bring security automation to the forefront from security teams to the board.

We will also delve into some of the emerging threats of the future. We say 'future' but when it comes to cybersecurity the time to plan, prepare and take action starts 'now'. Nevertheless, it is good to think broadly as some of these emerging patterns are eye-widening alarming.

Last but not least, we look at how to future-proof security for customers. Not as easy as it sounds and the ramifications for not staying ahead of the cyberattackers exposes not just their supply chain but opens a can of worms on fines, legal proceedings and reputational damage. We covered off 3rd and 4th party supply chain risks in our previous issue. This issue takes a closer look at safeguarding customers' security now and for the times ahead.

We hope you will enjoy reading from our extended guest writers lined up from around the globe.

Happy Reading!

We would love to hear from you! Whether you would like to share an opinion piece, insight or simply contribute to our publication, please feel free to get in touch with us. Email us at info@blockapt.com with attention to raj.meghani@blockapt.com. ■

Ransomware on a Rampage: Time to act.

Author: Raj Meghani

Ransomware is a malicious form of malware which manifests its way into an organisation's technical infrastructure in order to restrict or block access to sensitive data until a ransom is paid.

It's one of the fastest growing cyber attacks today with demands for ransom causing major disruption and damage on a number of fronts.

BIO

Raj Meghani is the Chief Marketing Officer and Executive Director at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with an advanced, intelligent cyber defence platform through its unique Monitor, Manage, Automate & Respond (MMAR) framework and single pane of glass view.

Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 20 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans.

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

Twitter: https://twitter.com/blockapt

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

COVID hasn't helped – we have seen a 600% increase in malicious emails. Figures suggest the UK has encountered 14.6 million ransomware attack attempts this year alone. The first half of 2021 has already reached 304.7 million ransomware attack attempts – it's the worst ever recorded year for ransomware attacks and we still have 3 months to go…

Global ransomware damage costs are predicted to reach $20 billion by the end of this year, up from $325 million in 2015 (Cybersecurity Ventures). That doesn't include reputational brand damage, legal costs, loss of productivity and the list goes on. It's difficult to actually put a figure on the overall damage a ransomware attack can cause.

The average cost to recover from a ransomware attack in 2021 is $1.85 million.

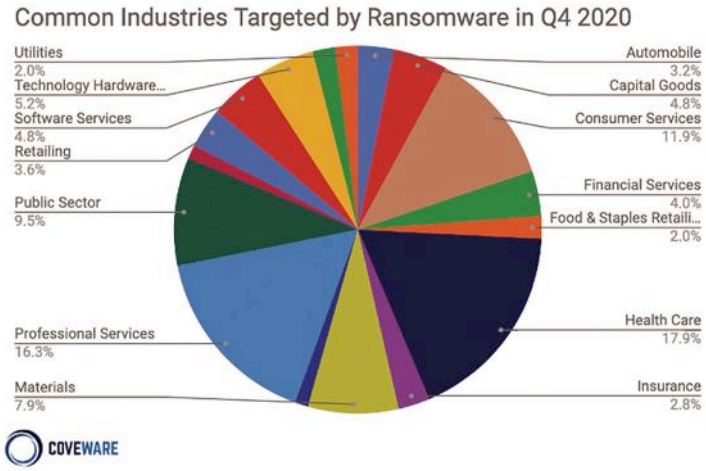
The average downtime (complete lockout to partial) from a ransomware attack is 19 days.

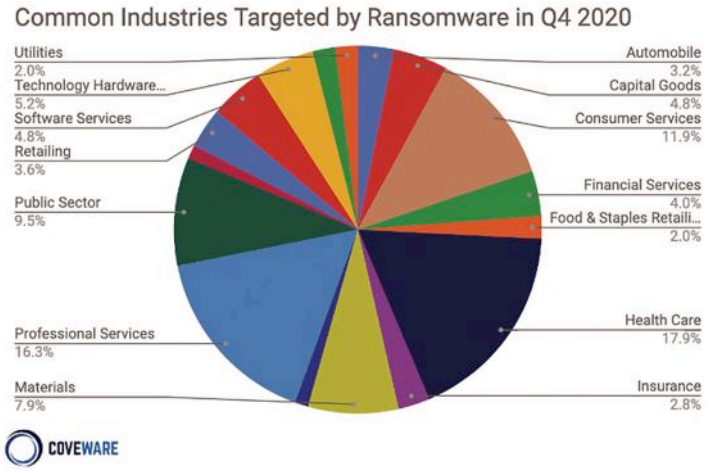
The average pay-out by a mid-sized organisation in 2021 was $170,404.

So with ransomware on a rampage with increasing frequency and severity, are organisation's defences really up?

I don't think so.

Certain industries which have been impacted and compromised heavily by the pandemic such as healthcare, education, etc have opened the attack surface for cyberattackers especially with remote working added into the mix.





Like most organisations think, ransomware is something that happens to others. They are not seen to be on the cyber attackers radar because they are too small, not an institution, are convinced their security is locked tight, etc.

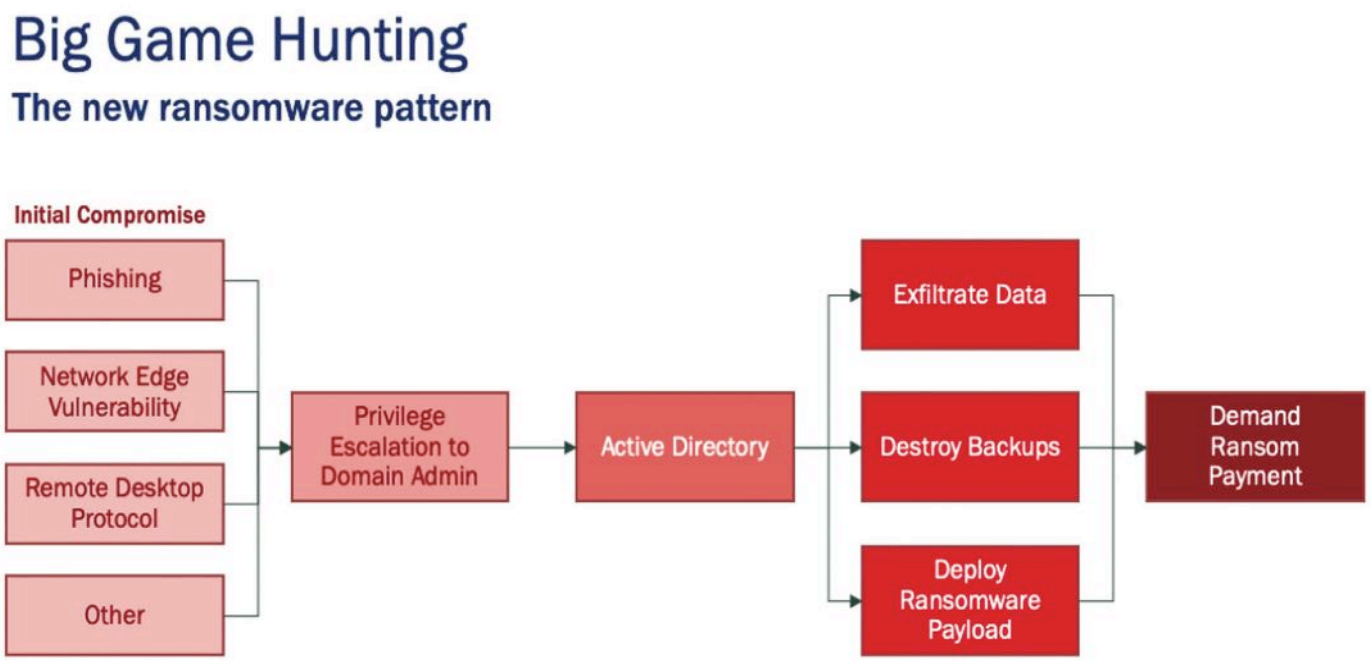
That's what CNA Financial (a large US insurance company) probably thought – until they got a ransomware attack and reportedly paid $40 million to the hackers in March 2021.

We have Ransomware and Ransom-as-a-Service (RaaS) where affiliates use developed ransomware tools in exchange for a percentage of the payment – sometimes up to 80%.

We know the top types of Ransomware varieties that are the repeat offenders and the routes they take to expand their reach:

1. Sodinokibi
2. Maze
3. Netwalker
4. Phobos
5. Cryptolocker
6. GoldenEye
7. Jigsaw
8. Snatch
9. Locky
10. NotPetya
11. Petya
12. Ryuk
13. Wannacry

We know there has been an increasing trend of ransomware attacks through software vulnerabilities or



Source: Security Boulevard, February 2021

email phishing and that hackers are getting more sophisticated targeting multiple clients through one channel – Managed Service Providers (MSPs).

We know there will be a continuing influx of State-Sponsored Ransomware to disrupt and cripple economic infrastructures around the world from the usual suspects – Russia, China, North Korea, etc.

We know the US has been the main recipient of recent Ransomware attacks and according to Atlas VPN, there have been about 865 ransomware threats every minute in the first half of 2021. Staggering. I predict that this is only going to get worse as more and more countries get targeted. I predict a ransomware attack will occur every 9 seconds as we move to the end of 2021.

We know that even if you have paid, there is no guarantee that there won't be a second extortion event or worse the hackers will still go ahead, exfiltrate and publish sensitive data even if payment has been made.

So we are far beyond the time to act. We are in a war where we are playing catch up and the delta between the ransomware cyberattackers and us is getting wider.

So what can we do to better defend against these ransomware attacks? We are past the days of the classic 'defend and respond' with the level of sophisticated ransomware attacks we are seeing today. We should be gearing up for more predictive analysis and putting in place preventative methods to fight back. Not sitting in a reactive mode.

'Ransomware is not just a technical vulnerability – it's a human one too.'
- Raj Meghani

1 Ensure all your business-critical online applications and networks - Endpoint Detection & Response (EDR), firewall, email, anti-virus/anti-malware security software configurations are up to date with the latest patches.

2 Automate threat vulnerability checks with continuous scans that run 24/7 all year round to enable you to see your IT systems the way hackers do.

3 Embed mandatory security awareness and training for ALL your employees to ensure they understand the importance of cyber resiliency and potential risk exposure to them and the business. Ensure they know what to look out for in phishing attacks, insider threats, etc.

4 Formalise an Incident Response Management plan – include crisis management angle too.

5 Ensure robust password security measures are in place and adhered to – 2-factor authentication, etc.

6 Ensure that your entire security devices and business-critical systems are automated for back-up and restore on-demand.

7 Damage control – ensure you try to limit the number of people who have access to sensitive/critical data.

Robert Mueller, FBI Director, summarised it well back in 2012 – *"There are only two types of companies: those that have been hacked and those who will be".* ■

Tackling malvertising with startup innovation.

Author: Saj Huq

The online ad ecosystem depends on trust, but ads that look legitimate and appear on official, trusted websites could include malicious code that can infect devices with malware and spyware.

In many cases malicious ads don't require any user interaction to infect a computer with spyware or malware, allowing cyber criminals to run malicious code and execute ransomware campaigns that can cause significant harm. And if they're able to use an ad on a legitimate site to take someone to a malicious site, the criminal can use that trust to harvest personal data, commit online fraud or sell data to a third party.

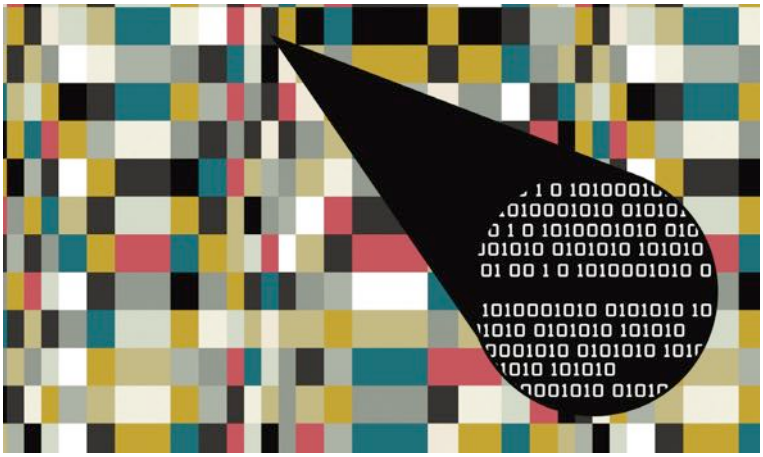
Bad actors find malvertising to be an extremely attractive tactic because it allows them to leverage a complex ecosystem of adtech operators, publishers, exchanges and platforms across the advertising industry. They can harness the power of network effects to scale up these campaigns, reach a large number of people and avoid detection by platforms. It's a black hat dream, so cybercriminals are buying ad space for themselves for nefarious purposes.

This has led to several high-profile websites being compromised with malicious adverts, including trusted household brands and major media outlets. Most recently, an advertising attack targeting Internet Explorer

users showed people fake advice about the pandemic and capitalised on people's greatest fears. And ad security company GeoEdge claims to have found first-of-its-kind malware that was spread to connected smart home devices through a malvertising campaign on mobile.

It's such a pressing issue that the National Cyber Security Centre and Plexal have chosen malvertising as our next challenge for NCSC For Startups. If you're a startup that could tackle this issue with the right support, we want you to apply to work with us as we're bringing on new members throughout 2021.

The online ad industry itself hasn't adequately grasped the threat that malvertising can pose – and even those who are aware of the threat aren't equipped to defend themselves. This is partly because malvertising can take many forms – it can be included in a video, be embedded into the creative of a banner ad itself or be contained inside a pixel on a landing page. In fact, many malversating tactics involve an updated form of steganography: a millennia-old technique that conceals messages or images inside other text or images.



Meanwhile, the complex web of players within the online advertising ecosystem makes it hard to tell who is responsible for combatting malvertising or who orchestrated a campaign. It's easy to see how the balance of risk and opportunity is significantly tipped in favour of the criminals. But this is exactly why we, as an innovation ecosystem, need to come together.

We need to galvanise our startups around the challenge to help us maintain trust and protect people. We also have an opportunity to explore how companies working in adjacent and related sectors, including ad tech startups, can help join the fight against this threat.

BIO

Saj Huq is Programme Director – LORCA (London Office for Rapid Cybersecurity Advancement – UK Government funded) and leads cyber innovation at Plexal. LORCA's aim is to be the centre for industry-led cyber innovation, allow people to stay safe online and make the UK a leading cybersecurity hub. Before joining Plexal and LORCA, Saj spent a number of years as a management consultant at Deloitte and PwC. He then moved into industry, leading strategic change at a PE-backed property finance firm where he helped them operationally scale towards achieving a UK banking license, prepare for the incoming GDPR and improve their cyber and operational resilience in readiness for regulatory authorisation. Saj started his career in the Royal Air Force, where he was a commissioned officer and pilot.

This is especially important as more people come online (often on mobile) for the first time or spend more time shopping online. They are most vulnerable to malvertising – especially if they're using an outdated browser, don't have antivirus software and aren't aware of the cyber risks they might face online. On mobile, it's especially easy for people to click on something without thinking twice because we tend to be in a different frame of mind and aren't as cyber aware. Throw in a crisis like a pandemic and it's a perfect storm.

So innovators, it's over to you.

Apply for NCSC For Startups at: https://www.ncsc.gov.uk/section/ncsc-for-startups/join-the-ncsc-for-start-ups ■

The threats of tomorrow: An outlook into emerging threats.

Author: Marco Essomba

I wear a CTO hat and therefore technology excites me. But unlike the broader technology industry, I cannot say the same about the emerging and future cybersecurity threats, be it technology, techniques or exploits.

Now allow me to switch to my CISO armour.

Yes, I blurred the line between technology and emerging cybersecurity threats a bit. Let me explain this. Simply put, new technology is based on innovative ideas coming to life. Cyber threats, in whatever shape or form it emerges, seem to follow the same pattern as new technology announced. There is an announcement, followed by media attention and lots of coverage across articles, organisations and experts - albeit being a negative coverage. Yet, analysts, students and researchers will study, dissect and observe them for years to come depending on the infamy.

So back to my original point. It is indeed like emerging technology (in some ways) as it even triggers digital transformation! And as disruptive as it is (the imminent arrival of future threats), there is something to marvel at the evolution, ingenuity and advancement of threats. No doubt there are followers of 'this' type of 'bad' technology now that there is 'Anything and Everything as a Service' model.

In this article, we are going to ponder the emerging and future threats. But it is at the end, not an exhaustive list. The important takeaway is our mindset to consider cyber threats but think, listen and act now as much as possible.

Supply chain nightmare into the future...

Since the last publication edition focused on supply chain attacks and threats, I did not want to dive into this. However, although it is a trendy subject, it is still worth a mention as I strongly believe we are only at the early stages of these cyber attacks i.e the Solarwinds, FireEye and so on (ref: our Nation-state attack focused articles).

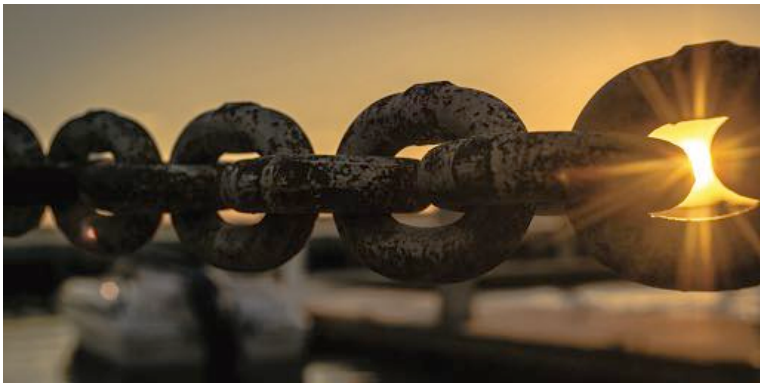
BIO

Marco Essomba is the Founder & CTO of BlockAPT. A leading edge UK based cybersecurity firm empowering organisations with an advanced, intelligent cyber defence platform. The BlockAPT platform allows organisations to Monitor, Manage, Automate & Respond (MMAR) to cyber threats – 24/7. Marco's passion, expertise and knowledge over 15 years of providing cybersecurity solutions has culminated in the design of our unique BlockAPT platform. Developed over time as a toolkit to help small and large enterprises business security issues, BlockAPT's platform brings together threat intelligence, vulnerability management, device management and proactive incident response management to help fight the war against cyber attackers.

LinkedIn - https://www.linkedin.com/in/marcoessomba/

Twitter: https://twitter.com/marcoessomba

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



In the coming years, I expect an uprising in nation-state led supply chain attacks even going after the wider IT services such as ISPs, computer chips, project management/operational tools, applications, etc to penetrate further into organisations; particularly the government firms.

I recently visited a Cyber, IoT, AI and Cloud Expo, and noticed that everything revolved around IoT. Smart everything from air filters to cars can be exploited by infecting their software supply chain, such as source code libraries. We will see things like remote devices disabling in effect (scary stuff!).

On a similar note, we can expect to see business-as-usual supply chain attacks on retail or entertainment e-commerce platforms. Such industries see their future online and thus rely on services for their digital transformation.

For example, you may have read about the Magecart gangs. They exploited Magento (an open-source e-commerce platform) in a campaign that hit over 2,000 online stores!

Magecart is one of the most serious and financially damaging cybersecurity threats to eCommerce retailers. Users of numerous platforms are at risk of attacks from Magecart gangs. Magecart attacks have successfully compromised thousands of web and mobile applications. Victims include dozens of global brands such as British Airways and Macy's. British Airways paid a $20 million fine for failing to protect its customers against a Magecart attack.

Interesting to note that this attack campaign was largely automated. And don't think your traditional tools like Web Application Firewalls (WAF) can help, as they do little for customer side attacks. By then cybersecurity would be looking into Machine Learning tools to help look for patterns and behaviours in order to act faster.

Superfast Internet fuelling superfast attacks…

Moving on, let's talk about 5G. Yes, I know that the 5G hype so far has been massively underwhelming. But eventually, we will get there and the rollout of the promised higher and faster connectivity will be widespread. Sure enough, it will be a streamer's delight but on the other side, it will also be cyber criminals paradise.

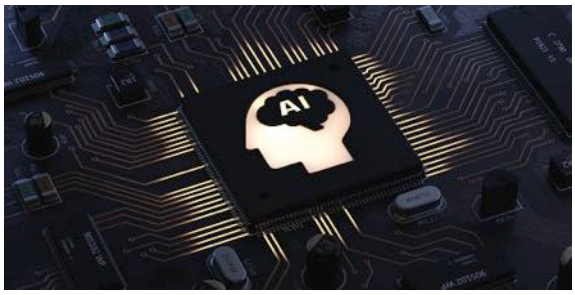
This also means we can expect to see equally powerful and high-speed attacks ranging from device-to-device targeting, large scale data thefts and stronger controlled botnets. These botnets could then be used as weapons in cyber-attacks; and a Distributed Denial of Service (DDOS), which overwhelms a network or website with more volume than it can handle.

Ultimately, time will tell but with 5G there are new and potentially greater security risks to consider as cloud, data and IoT threats merge. But as it stands there is limited visibility, tooling or resources to fully manage and secure large-scale public or private 5G networks. For the adversaries, the attack motive will be monetary or political and so the attacks could be launched from local

to the nation-states which means the range would be really wide.

Malicious Artificial Intelligence (AI)

The other talking point of the aforementioned expo I recently visited was AI. The application of AI is huge for enterprises but this is equally a lottery for the cyber criminals groups as well. Smarter and automated AI could change the landscape by predicting user behaviour as well as security tools to beat passwords (and password security measures) as well as launching creative phishing and convincing social media exploits.



This could also lead to the next-gen deep fakes that replace the current CEO impersonation as well as political exploits.

An AI Security Compliance Program is imminent in the future but this will take time. In the interim, we will see enterprises to government organisations rapidly leverage AI-based tools to enhance services, operations and engagements, particularly across their digital estate.

The use cases for AI are great across visual perception, speech recognition, language translation, content delivery, pattern-reading to decision making, etc. But you see where I am going with this - more attack routes to launch AI-based attacks.

Destructive Malware

Malware by its name, is a blanket name for malicious software across the digital spectrum.

Unlike Ransomware, where the endgame is usually financial gains, malware on the other hand is pure destruction or disruption. This means not having another chance to get that crucial 'data' back even by paying a ransom or corrupting/disabling national infrastructure, medical equipment or simply getting locked out of systems (or even cars or houses!).

We will see more Wiper Malware attacks in the upcoming years. A Wiper Attack involves wiping, overwriting, erasing data from the target. It is already wreaking havoc as you may recall, during the 2013 South Korea cyberattack, and the 2014 Sony Pictures hack or the Iranian oil companies as well as Saudi Aramco (Shamoon Wiper).

The fact is that this cunning cyber threat which is not financially motivated is not just for state actors but terrorists, activists, disgruntled individuals and more. This makes it deadly.

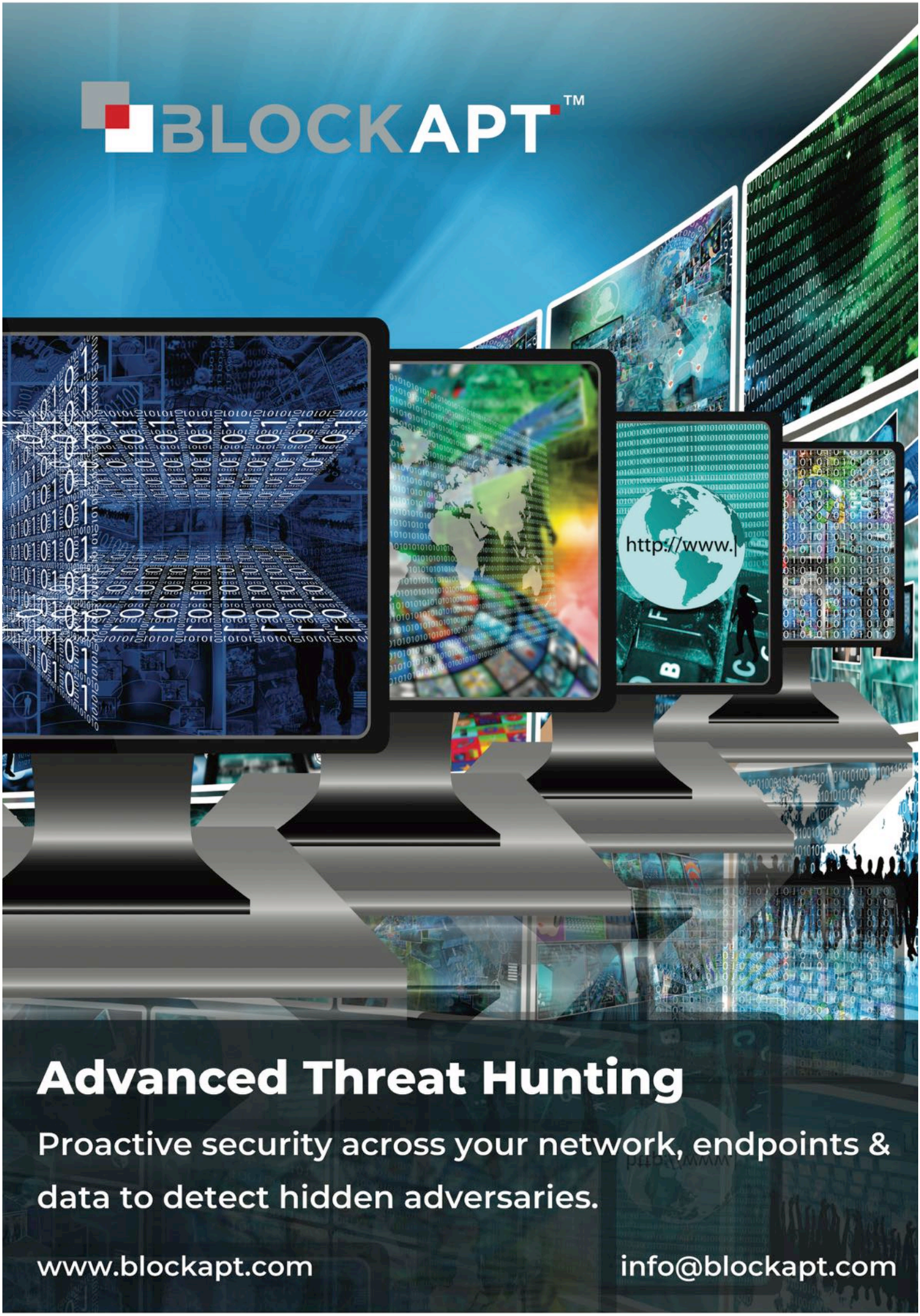
Various other dishonourable mentions

And of course, there is Ransomware which we have extensively covered across our last 2 editions of the publication. Ransomware will remain in the spotlight but at least there is now a better awareness of this threat industry-wide albeit through the damage and disruption caused.

Everyone uses a smart device and application of some kind. Smart devices and IoT makers push out firmware upgrades to enhance user experience, features as well as security. Firmware updates are bridges between software and hardware. This makes it another goldmine route to launch cyber attacks through updates. The return on investment on these attacks will be huge as firmware upgrades reach millions of users and devices. The possibilities are scary as cyber criminals can control not only laptops and phones but also heavy machinery, industrial plants and even vehicles. It has already begun but I suspect this will be another one to be vigilant about from a cyber security control point of view. You can recall the Ukraine power grid attack in 2016, which is an example of precisely this.

To conclude, is the future of cyber threats bleak? Yes, it is.

But the fight is not lost yet and doing nothing is not an option. Breaking down a cyber attack using detection, prevention, and defensive disruption methods at the earliest opportunity of an attack chain is key. I always preach 'Defence in Depth'. A holistic approach to cyber defence using a multi layer approach. It works! ■


BLOCKAPT™
http://www.
Advanced Threat Hunting
Proactive security across your network, endpoints & data to detect hidden adversaries.
www.blockapt.com
info@blockapt.com

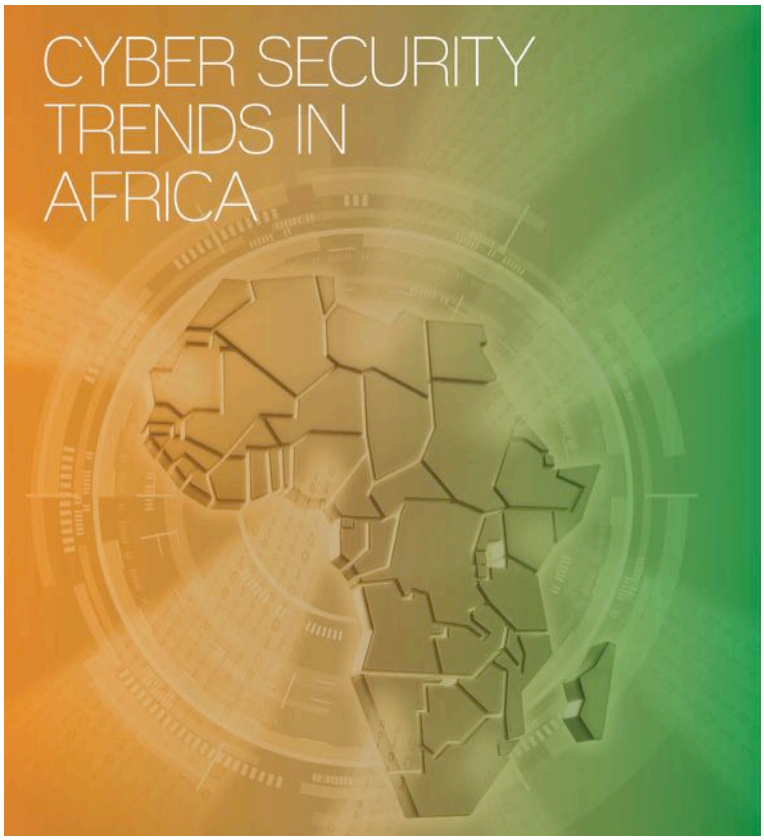
Cybersecurity in Sub-Saharan Africa: A risk we cannot afford to ignore.

Author: Serge Wamba Fosso

Sub-Saharan Africa is entering the digital space:

The world is changing as new ways of working are taking place across the globe. In Sub–Saharan Africa, companies are starting to realise that they will not survive or compete internationally if they do not start to embrace some form of digital transformation. Financial and industrial sectors are taking the lead to implement internet-based applications. We are also seeing a significant push in the government of Central and West Africa countries to have the full fiscal and tax payment system managed through the net. In Cameroon for example, taxpayers can process their fiscal duties fully online.

In fact, in most Sub-Saharan countries, tax payment is majorly collected through the internet or cloud-based applications. Another factor is the stiff growth of mobile usage in Africa leading to an increase of mobile apps. According to the Symantec report, Cyber-crime & Cybersecurity Trends in Africa of November 2016, Africa also leads the world in money transfers using mobile phones, with 14% of all africans receiving money through mobile transfers.



BIO

Serge Wamba Fosso has over 22 years' experience in the oil & gas industry and is a thought leader & expert in HSE / Risk Management. With a Masters degree in Civil Engineering, a Masters degree in Physics and a Post-Graduate in Applied Mathematics, Serge has successfully completed several international assignments for companies like Schlumberger – a leading global provider of technology and services to the energy industry. Today Serge is Vice President for NESR (Oil & Gas) and is the Founder & CEO of PRODEOS (QHSE Operational Risk Management software) which helps businesses reduce operational risks.

Cyber criminality is growing:

This growing environment has attracted cyber criminals to Africa. According to the above-mentioned report, Africa could be viewed as a permissive environment for cyber criminals due to a lack of security capabilities, absence of relevant legislation and general lack of awareness of cybersecurity measures. These cyber-attacks include Ransomware, social media scams, & various email threats.

Crypto ransomware which is a type of harmful program that encrypts files stored on a computer or mobile device in order to extort money has increased more than 35% in the last 5 years.

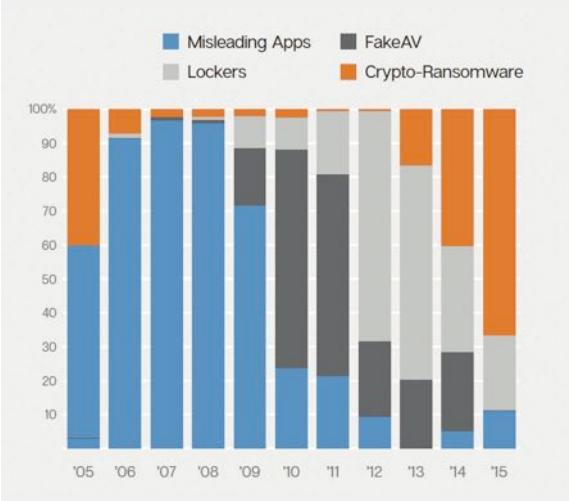
We are clearly facing a risk we cannot ignore. The multiplicity of mobile apps exacerbated by the lack of information and legal frame is exposing the government, financial and other industry sectors to unprecedented risk that is growing exponentially.

Another consideration to bear in mind is the cultural factor. Victims of cybercrime do not report any breaches or that they have been a victim to fraud as they feel ashamed or do not want to face what society may think of them. These attitudes and lack of reporting is not helping the situation as there are no tools to report.

Risk is too big for the Sub-Saharan Africa countries:

We cannot continue to ignore this risk for emerging countries where other issues are already threatening the economic growth and poverty is still a major issue.

Take the example of commodities trading or banking where significant transactions are made daily. Any disruption in these sectors can severely damage the stability of any country. Cyber criminals are focusing on crypto-ransomware because in contrast to other cybercrimes, an attacker can obtain a ransomware toolkit from an underground source, and target their intended victims, who may have few alternatives but to pay-up. There are no middlemen for the criminal to pay and nothing to mitigate the losses to the victim, thus maximising the profits according to the Cybersecurity Trends in Africa, Symantec Report published in November 2016 as summarised by the graph shown.



Source: Cyber Security Trends in Africa Symantec Report published in November 2016

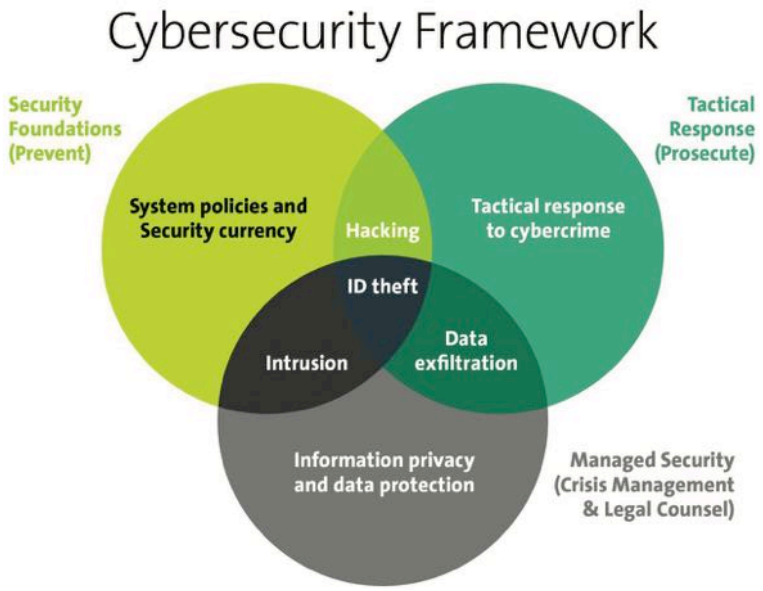
While in Sub-Saharan Africa, there is almost no data available mainly largely due to the absence of reporting and measuring tools as well as no control of cybercrime, a Scidev.net study suggests that, In francophone Africa, the phenomenon is mostly to be found in the main regional economies. According to their publication, in 2013 the estimated cost of cybercrime in the Ivory Coast was 26 billion CFA Francs (3.8 million euros). In Senegal the cost was estimated to be 15 billion CFA francs (22 million euros). These figures have significantly grown over years and would represent today close to a double digit % of the GDP of these countries. The exposure is big and will continue to be as attackers are becoming more and more clever.

Path for potential solutions:

Raise awareness, reporting and training:

The first step in addressing cybersecurity in Africa is awareness. This can be achieved through conferences, webcasts, articles in newspapers, online or TV ads. Also training and auditing plays a key role. Major firms in the world are now making cybersecurity training mandatory for all employees with random phishing tests to identify vulnerabilities and increase awareness.

The second aspect is reporting. Something which does not get measured cannot be managed. Reporting includes incidents where no loss occurred and accidents where the cybercrime resulted in a loss so that both event types can be investigated, and risk mapping done to avoid recurrence. Numerous tools exist in the market for this purpose including QHSE apps.



Create a legal cybersecurity framework:

It is in the interest of the government of Sub-Saharan countries to create a legal platform for cybersecurity where cyber criminals can be tracked and legally sanctioned. The legal framework should also address the minimum prevention and mitigation measures to be in place for companies of all sizes and based on the risk and exposure.

Implement strong and efficient counter-attacks IT tools:

As stated above, cyber-attackers are becoming more clever by the day. Hence there is a need for companies to have bullet-proof IT tools and solutions in place to prevent and stop cyber-attacks. Several of these tools have been developed and implemented with some strengths and weaknesses. Choosing the right tool and/or the combination of tools is key to ensuring the security posture of organisations is locked tight and exposure to risks and vulnerabilities are mitigated against.

In summary, Sub-Saharan countries are not immune to cyber crime with potential significant consequences to the economy and the country's stability. This risk cannot be ignored.

Raising awareness, reporting, training, creating a legal framework and installing the right IT protection tools are the main avenues for preventing todays and the cyber-attacks of the future. ■

Which came first: Security or Theft?

Author: David Schoenberger

In the cybersecurity world, security experts and cryptographers have generally responded to a malicious hacker after a bad event has occurred. It has proven to be very difficult to anticipate what data thieves will use to steal in the future. Technology improves rapidly and so do the creative, yet criminal methods used for breaching systems, applications, and devices. What can be predicted is that thieves will always want what is not theirs and will do anything to steal. Possession of data is their goal—to steal and use data for nefarious purposes.

So really it isn't a question of IF a malicious hacker will try to steal your data—it isn't even WHEN they will try to steal your data. The question all organisations must accept is HOW will they try to steal the data. Asking this question allows organisations to take a proactive approach instead of the usual reactive approach. More than being proactive, organisations must understand the key to all breaches and hacks is the actual data.

To compound the dilemma of understanding how to take a proactive approach to address these breaches and hacks, organisations are now faced with fraud perpetrated by cyber criminals targeting the external customer on their mobile devices. The COVID-19 era has ushered in the use of millions of mobile applications to manage and perform almost every aspect of daily life. This opens the door to tremendous fraud opportunities for the cyber-criminal to infiltrate organisations using their customer as the trojan horse.

According to a 2021 study by Interceptd, over 21% of iOS mobile apps and over 27% of Android mobile app installs are fraudulent. That means people are downloading apps that they believe are legitimate and safe, but they are actually inviting the cyber-criminal into their device. It has become abundantly clear that if organisations cannot control their clients' device environment, they can't control the consumer behavior online. Future-proofing the client experience has taken on new meaning.

BIO

David Schoenberger is the Chief Innovation Officer at Eclypses with over 20 years of experience researching and developing disruptive technology for financial and data security companies. Previously, David worked as a leader and researcher at multiple fintech and cloud storage companies. He brings extensive technology and leadership experience as one of the Eclypses creators of the patented MTE technology. David is a sought after spokesperson educating people on cybersecurity and risks. He has been a leader with several non-profit organisations working to aid impoverished families and children, and to conduct research in energy sciences. In his free time, David enjoys spending time with his family adventuring in the Colorado mountains.
Email: david.schoenberger@eclypses.com
Eclypses website: www.eclypses.com
LinkedIn: https://www.linkedin.com/in/david-schoenberger-60100a1/

It is important to make another distinction while future-proofing your security plan, which is that keeping hackers away from data is not the same as protecting the data by making it unusable. Instead, it is important to implement both strategies, as both need to be part of a solid future-proofing plan. Keeping malicious hackers away include strategies like antivirus, malware protection, firewalls, threat detection, app shielding, code obfuscation, multi-factor authentication, and others. Even best practices such as redundant and geo-dispersed data centers are critical, but still only fall into the category of "keep out."

Making the data unusable is a different beast altogether and some common practices to protect data include encryption, tokenization, data masking, and other emerging solutions like MTE. The main goal of these solutions is to make this transformed data unusable and indiscernible when stolen, regardless of how it was stolen. If a hacker can't use the data or discern the data, then there can be no threat.

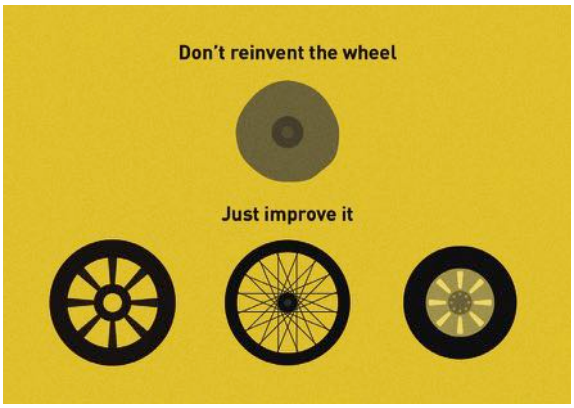
Here are three considerations to future-proof your data and make it impossible for a hacker to use:

1 **Spend time identifying what data (when stolen) would ruin your organisation or compromise the humans you are providing services to.** Whether it's the government or a corporation, a breach ends up being a human cost and not all data in all systems would lead to a human cost. A very basic example is that the data representing the size of the latest pair of jeans you order is much less critical to protect than the payment details and delivery address. In the medical field, if a company collects Name, Date of Birth, Room Number, Treatment Physician, Procedure—and protects Name, DOB, Room Number—then it becomes less valuable to a hacker if they end up stealing the physician's name and the procedure done. These are just basic examples to show that not all data needs protecting when the right data is protected. This is critical when in most cases the very data you are trying to protect is the data that you need available to your applications in real time. Hackers understand this conundrum and take advantage by stealing data the moment it becomes usable and moveable from encrypted storage or at data creation. The best advice is to take the time to identify the data that needs to be protected and focus there.

2 **Determine what applications are most vulnerable to hackers.** Many organisations that have been hacked recently or that respond to various research-based surveys, have an overwhelming conclusion that mobile and web-based applications are most vulnerable. This is directly tied to the human experience and is based on how humans demand to interact with corporations. Mobile devices are instantly accessible and always connected. They are the expected main way that customers interact with most corporations and services, and mobile applications are really just web-connected applications that do very similar things to web applications.

Because the human has installed countless other applications on their devices, it is almost impossible to know if malicious applications are also running on the device and it is expected that hackers are watching Wi-Fi connections and looking for ways to exploit these applications. Applications both produce and interact with sensitive data—desirable by thieves and hackers.

3 **Don't expect to reinvent the wheel!** Developers often are primarily concerned with business outcomes and supporting the user experience and do not devote their sole purpose to the security of data. Therefore, in addition to developers using security best practices and standards, it is recommended to carefully select technology partners and toolkits that can supply security protocols without trying to reinvent what an entire engineering team has dedicated their focus to. Let your developers focus on what the human expects and let security technologists solve the hacker problem!



It's critical to spend time on future-proofing your data to make it impossible for hackers to gain access. Every cybersecurity strategy needs a strong foundation for protecting the data. Find a data security solution that no matter what happens – your data remains secure. ■

The state of the cybersecurity landscape in Japan.

Author: Tsutomu (Yonny) Yoneyama

"What is the state of cybersecurity awareness and efforts in Japan?"

This is a question that is often asked by people from overseas, as they are aware that while Japan has a relatively well-developed social infrastructure such as cheap broadband connections and preparedness against the threat of natural disasters, a strategic approach based on risk analysis has not been widely adopted in terms of cybersecurity measures.

Today, I would like to briefly summarise the current status of cybersecurity in the Japanese private sector, its background and challenges.

BIO

Tsutomu Yoneyama (Yonny), CISM, CISSP, CCSP, PMP, PSM1, SSCP, ITIL, has 25+ years of Enterprise and Service Provider Infrastructure Design & Implementation experience and is presently Representative Director at Novias K.K., a strategic company of BOW Holdings Group providing cybersecurity professional consultancy & managed services with no bias. Yonny's major focus is on facilitating digital transformation (DX) through cybersecurity governance, risk management, business continuity and resiliency consultancy as well as project management and telecommunications & network expertise.
LinkedIn : https://www.linkedin.com/in/yonny/

Cyber risk and the impact of COVID-19:

According to the October 2020 survey by the General Insurance Association of Japan, about 40% of companies responded that they were more likely to be subject to cyber-attacks than before the spread of COVID-19, and specifically, they were concerned about cyber risks such as information leaks associated with the use of teleworking and web conferencing. On the other hand, 43.8% of the companies answered that they were not sure whether their current cyber risk countermeasures were sufficient or not, indicating that the relationship between the perceived risk factors and the countermeasures is not clear.

Cybersecurity measures will not be regarded as an investment for business continuity and will be perceived as an endless cost unless diligently answering to the management's questions of "Are the measures proposed for the risk factors sufficient and appropriate?" "Considering the threats and vulnerabilities to your organisation, are there any other priority risks that need to be addressed?"

Of course, it is not easy to calculate the return on investment for cybersecurity investment, but by translating it into economic value, which is a common language, cybersecurity can be discussed in the same way as other management issues.

For example, the Japan Network Security Association (JNSA) proposes the following six categories to guide the calculation of damage in the event of an incident.

Six Damage Categories

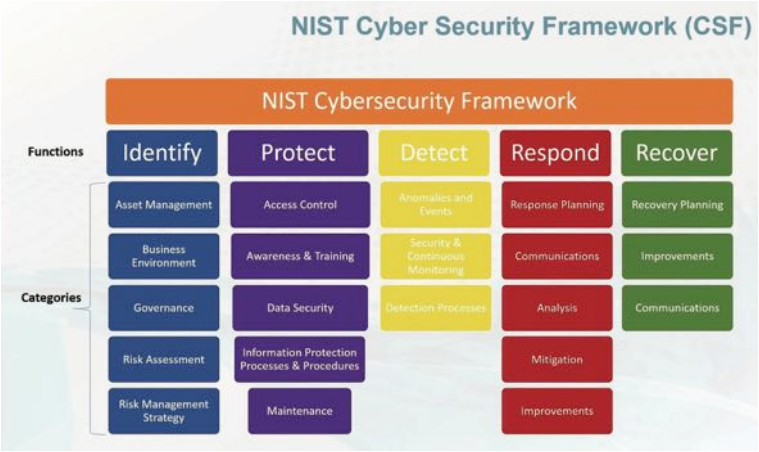
Use of the guidelines and the impetus for implementing security measures:

It has been a long time since there was a shortage of human resources responsible for cybersecurity in companies. One of the effective measures to fill the shortage of human resources and skills gap is the use of frameworks and guidelines. About 23% of the companies indicated that they have opted for ISO 27000-based measures, while a significant number of companies (27.2%) have not adopted any framework or guidelines.

In addition, in the case of Japan, the top trigger for implementing security measures was the company's own security incident, which is very different from the US and Australia where top-down direction from management is used.

(Source: NRI Secure Technologies Ltd. Survey on information security in companies 2020)

As for the trigger, it could be an indication of the tension among the management in the US, where the occurrence of an incident could lead to the risk of prosecution by business partners, etc. However, we believe that the use of frameworks such as the NIST CSF, for example, will contribute to a common understanding of the overall picture of cyber risk countermeasures with a wide range of stakeholders.



Status of cyber risk management implementation:

While anti-virus and software vulnerability management have been introduced in 90% of organisations, and access rights, log management, employee training and data protection have also been introduced to some extent, constant monitoring by SOC and EDR have not been introduced so far. Outsourcing and automation can make a significant contribution to addressing the issue of the lack of quality and quantity of security personnel mentioned above.

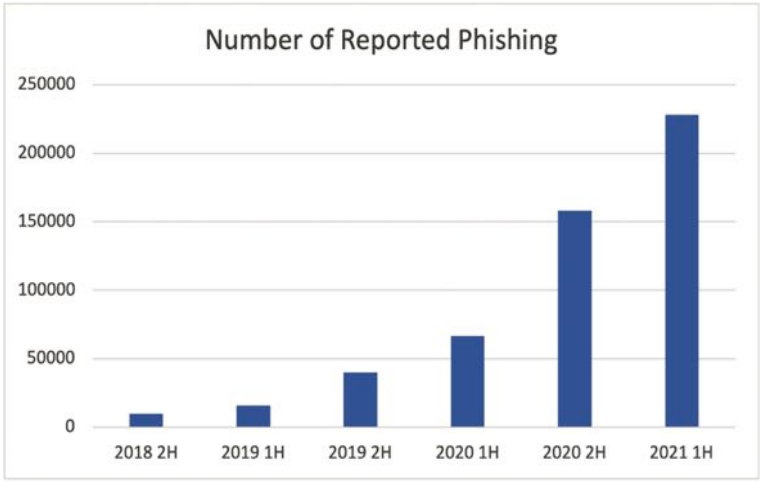
Software Vulnerability Management, Anti-Virus Software	87.4%
Access Privileges and Log Management	54.1%
Employee Training	33.5%
Data Protection (Encryption, DLP etc)	28.1%
Security Certification	17.7%
Continuous Monitoring by SOC	2.0%
EDR	1.6%

Table 1 : Cyber Risk Measures in Place (Extracts, Multiple Answers)

(Source: The General Insurance Association of Japan Survey on cyber risk awareness and countermeasures among Japanese companies 2020)

Phishing attacks as a major route of entry and the response:

Language barriers and cautiousness about the unknown have created a strong human firewall against phishing, smishing and false alerts that exploit human vulnerabilities. Even when phishing emails looked very good from the attacker's point of view, it was often practicable to discard them in the trash because they were written in a language other than Japanese or had a strange title. Unfortunately, this "natural immunity", which works without even checking the email header, does not cope with recent variants, and the number of phishing reports has risen sharply in recent years, according to the Council of Anti-Phishing Japan .



Number of Reported Phishing
(Source: Council of Anti-Phishing Japan monthly reports)

In order to make the cybersecurity awareness training more realistic, I have been collecting phishing emails and in recent years, fonts, logos, layouts as well as text expressions have become very sophisticated. Actually, phishing accounts for 30% of account identity theft, making it a significant threat affecting organisations and people today.

(Source: Ministry of Internal Affairs and Communication 2020 Report 000735800.pdf)

Japan, with technology at the heart of its high quality innovation initiatives, is driven by a simple need to keep its people safe and protected.

With the increasing number of remote workers and dangerously sophisticated cyberattacks, it's now not just a business problem but a domestic issue which EVERYONE has a part to play in. ■

Cybersecurity challenges and initiatives in India.

Author: Vikram Taneja

As one of the fastest growing economies of the world, global security trends and scenarios have similar bearings on India and share common grounds. However, due to India's demography, democracy & demand it brings some very unique challenges which are not seen globally. Hence innovation and improvisation are critical for such an ecosystem; Below are some of the common themes & trends and unique challenges we see across India.

BIO

Vikram Taneja is Managing Director & CEO for CyberSRC®. CyberSRC Consultancy is CERT-India empanelled & ISO 27001 certified operating in the cybersecurity space. Vikram is highly accredited with CISA, CIPM, CEH V10, ISO 27001 Lead Auditor, GDPR Practitioner, ISO 27701 (Implementer) and COBIT 5 (F) certified with more than 12 years of experience in IT Risk and Compliance Management, Information & Cybersecurity, GRC consultancy, Incident Management & Response, IT Audits, and Data Protection. Vikram's expertise has been evident across multiple sectors including banking, healthcare, insurance, Management Consulting, Credit Rating Agencies, KPO/BPOs, Internet companies, e-commerce and others. He has worked for organisations including Tata Consultancy Service, HCL & Wipro Technologies Ltd.

Digitalisation (development of digital economy):

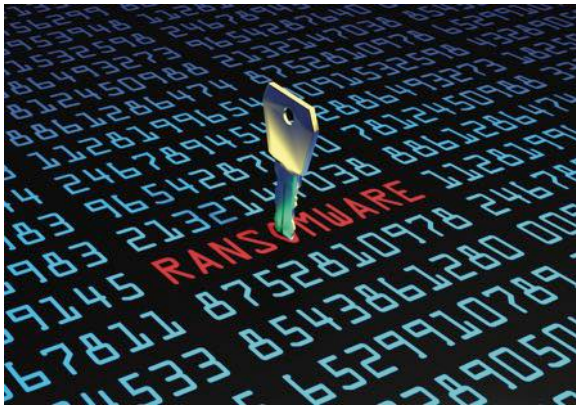
Digitalisation is one of the most important business trends for the future of economy. It increases productivity and efficiency while reducing costs. About 68 per cent of indian Small and Medium Businesses (SMBs) seek to digitally transform to introduce new products and services, differentiate themselves from the competition, and grow, while 60 per cent recognise that competition is transforming and they must keep pace, and 50 per cent seek digital transformation due to customer demand for change according to a Cisco report. Adoption of digital technologies by SMBs could add $158-$216 billion to India's GDP by 2024 and contribute to the country's economic recovery post COVID-19 according to the Cisco India SMB Digital Maturity Study 2020.

Cyber-attack uptrend:

With the growth of digitisation, cybersecurity issues have become a day-to-day struggle for businesses. While the trend was already on the rise,

COVID-19 has accelerated it. The pandemic has ramped up remote workforces, making inroads for cyber-attacks. As more and more people go online for work and to do simple everyday things like banking and shopping, it paves the way for a huge increase in hacks and data breaches. Most of the companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss.

Cyber criminals are using social engineering, phishing, identity theft, spam emails, malware, ransomware and whaling to compromise their targets. Over the last few weeks, there have been some major ransomware attacks around the world. Since the start of the pandemic, ransomware attacks have increased by nearly 500 per cent. The first big infiltration was at Colonial Pipeline, a major conduit of gas, jet fuel and diesel to the East Coast.



And then there was J.B.S., one of the world's largest beef suppliers. CNA Financial was attacked and paid a ransom of US$40 million - one of the biggest payments on record.

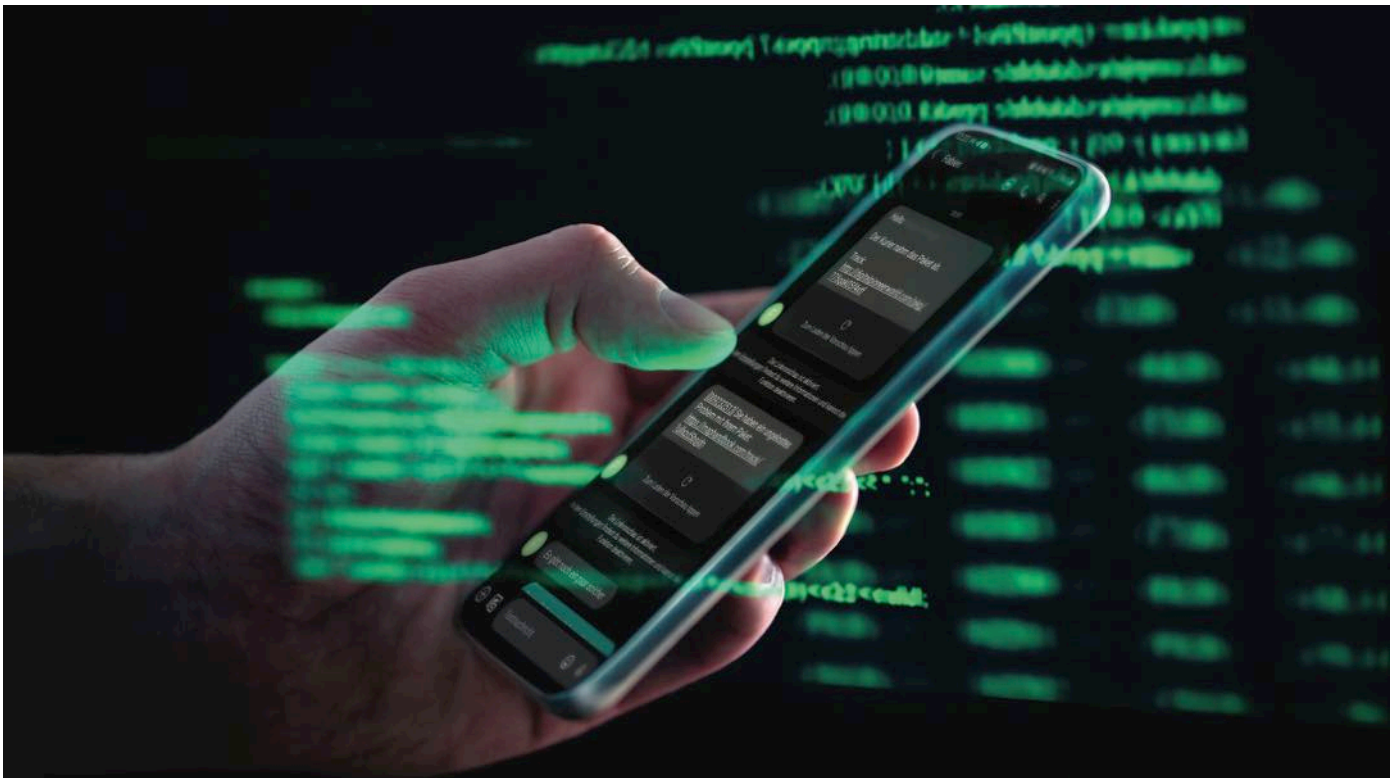
During the same time in India, Air India reported that hackers had compromised their servers and accessed personal data of 4.5 million fliers. In March 2021, there was an attack on Pimpri-Chinchwad Municipal Corporation, Smart City project in Pune district (Maharashtra).

Unique challenges:

There is a challenge between balancing convenience vs security vs cost of security especially where India is concerned due to high price sensitivity and culture of convenience.

SMBs which are the backbone of India's economy, are under attack from malware, ransomware, external threats and data breaches. Cybersecurity incidents in India increased 193% from Rs 3.94 lakh in 2019 to Rs 11.58 lakh in 2020, as per data from Indian Computer Emergency Response Team (CERT-In). For instance, 73% of indian SMBs claimed they lost internal emails, 71% lost employee data, 74% suffered loss related to intellectual property, and 75% claimed financial information loss. Due to the lack of sophistication around most SMBs security stance, the prospect of remaining unaffected by attacks is bleak.

With digitalisation playing a key role in India's growth, it has rewritten the Small and Medium Business story. Digitalisation has blurred geographical boundaries for SMBs. SMBs are becoming a lucrative target for cyber-attacks because most do not have sufficient defences in place to protect, detect or react to attacks. Amongst key attack vectors for SMBs systems, malware attacks accounted for 92% of surveyed SMBs in India followed



by phishing at 76% for SMBs. In fact, only 14% of SMBs rate their security as 'highly effective'. There are multiple reasons for this such as the lack of resources, lack of expertise, lack of information, lack of time, lack of training although they are all very relevant and real. Sometimes most SMBs do not have a sufficient IT team. Before the current public health crisis, they were increasingly the target of cyber-attacks due to the lack of resources to implement comprehensive cybersecurity solutions.

However, there is a ray of hope as the SMBs in India are taking a planned approach to understand and improve their cybersecurity posture through strategic initiatives. 89% of SMBs have completed scenario planning and/or simulations for potential cybersecurity incidents in the past 12 months, 91% have a cyber-response plan and 92% have recovery plans in place according to a survey.

Phishing and Smishing attacks:

Phishing scams are among the most common and dangerous type of attacks that organisations face. Verizon's Data Breach Digest found that 90% of all data breaches involve phishing. India is among the top three countries facing phishing attacks primarily via instant mobile messaging apps like Facebook-owned WhatsApp and highly-encrypted Telegram, a new Kaspersky report has revealed.

The rise of phishing attacks poses a significant threat to all organisations. It's important that all companies know how to spot some of the most common phishing scams if they are to protect their corporate information. Some of the reasons for an increase in phishing attacks are as follows.

Employees are the weakest link of any organisation. Unfortunately, most employees don't receive the necessary training. Indeed, researchers have found that 52% of users receive training no more than twice per year, and 6% of users have never received security awareness training. Not good or robust enough.

Organisations also generally have insufficient backup processes, lack of simulations for user testing and lack of implementation of security solutions to protect themselves from phishing attacks.

Cybersecurity incidents:

For India, the average total cost of a data breach to date is Rs. 165 million in 2021, an increase of 17.85% from last year. The findings were part of the annual Cost of a Data Breach Report, conducted by Ponemon Institute and sponsored and analysed by IBM Security. The rapid shift to remote operations during the pandemic appears to have led to more expensive data breaches. Lack of cybersecurity awareness coupled with lack of incident detection and response strategies contributed to the growth in breaches with most of the breaches going unnoticed until most of the data had been compromised.

Slow growth of Indian Regulations to battle cyber-crimes has also played a huge role in the rise of cyber-attacks. India has the IT Act 2000 with a limited view of data security and privacy. India's Data Protection Act though is a significant improvement but has been in draft stage since 2019 and has not become a formal law. There is no law for companies to report data breaches or being accountable for data breaches. Cybercrime, including phishing, identity theft and fraud, has massively increased as the coverage under the existing laws is neither adequate nor comprehensive.

Critical infrastructure is owned by the private sector, however there is no national security architecture that unifies the efforts of all these agencies to be able to assess the nature of any threat and tackle them effectively.

As there is no National regulatory policy in place for cybersecurity, there is a lack of awareness at both company level as well as the individual level. Domestic citizens can protect and be protected from the cyber-attacks only if there is a guided and supervised legal framework.

Social media these days has become a key tool in displaying and spreading information to the public which is vital hence there is a need to survey motivated use of social media by vested interests for disturbing law and order.

Cybersecurity startups:

India has become a mushrooming ground for cybersecurity startups with a big push from the Indian Government under various schemes & initiatives, such as Make in India, which has motivated software and solution development organisations. There are organisations creating various tools and platforms to protect the security of organisations assets and infrastructure. Some of the areas targeted by cybersecurity startups & solution providers are Threat Intelligence, Honeypot solutions, Phishing Simulations, Antivirus, Data Loss Prevention solutions and others. India has the potential to become a cybersecurity powerhouse for the world.

Government of India initiatives:

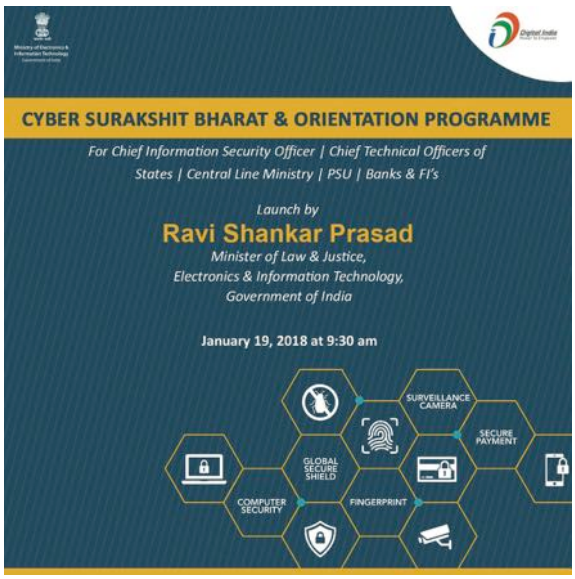
India's government is putting a lot of effort to fight the increase in cyber-attacks. The advancement in The Indian Computer Emergency Response Team (CERT-In), which operates as the national agency for tackling the country's cybersecurity, has helped in lowering the rate of cyber-attacks on government and private organisations networks. The implementation of anti-phishing and cybersecurity awareness training across India's government agencies has assisted government employees in fighting the war against cybercrimes.

Aiming to strengthen their cybersecurity ecosystem, the Ministry of Electronics and Information Technology has launched the Cyber Surakshit Bharat initiative. With such initiatives, there would be a rise of awareness about cybercrime and building capacity for securing CISOs and the frontline IT staff across all departments. Apart from awareness, these initiatives also include a series of workshops to make people cognisant about the best practices, and help the officials with cybersecurity health tool kits to tackle cyber threats.

Another major initiative by the central government is the formulation and implementation of a crisis management plan by all the government departments and critical sectors. The central government has also launched Cyber Swachhta Kendra, which is a cleaning bot used for malware analysis and detecting malicious programs. It also comes with free tools to remove or omit them. With these steps, the government hopes to curb the rise in cyber-attacks, though the effort can only become successful with collective efforts from both the government and cyber-aware public.

With such unique challenges & opportunities, the Indian cybersecurity industry is looked at closely by the world. Successful innovations & technological advancements in India may yet pave the way to becoming the gold standard for cybersecurity industry globally.

Watch this space. ■

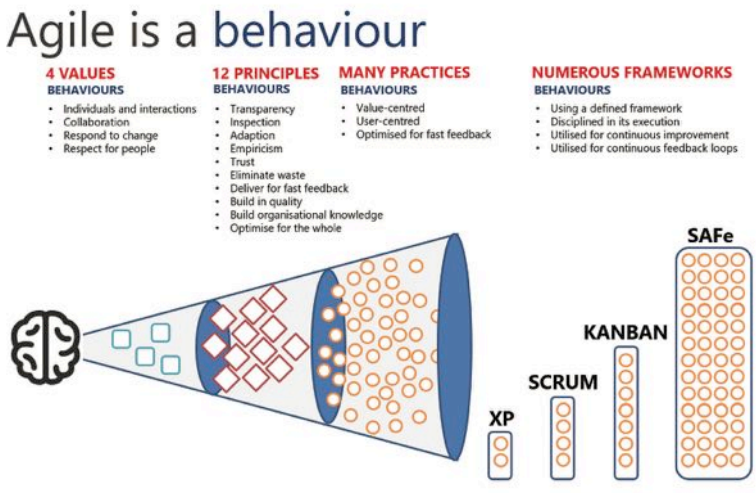


Managing the most critical in a noisy digital world.

Author: Nicola Sotira

Digitisation is making continuous progress in the innovation of products and services, and in the COVID era it has seen a sudden acceleration. Everything is moving quickly online, creating a new economic phase linked to the digital revolution that also risks making victims at a social level.

In this faster and faster transition, today more and more advocated also by the legislator who, having to deal with the state of crisis pandemic, has seen in digital an ally in the management of the crisis, vaccination platforms, green pass, intelligent management of registry, use of App for mobility and booking of health systems just to name a few examples. In this context, the information security sector seems to be struggling, as it is still tied to old schemes that sometimes do not match the agility required by digital transformation, in addition to the chronic problem of being perceived only as a cost.



Often, it must be admitted that the inadequacy in the evaluation of IT risk has, as a result, the pouring of activities and findings of the scanners on the IT departments that do nothing but overload the staff that can hardly manage this number of activities. One of the topics, in the vast catalogue of the security encyclopedia is vulnerability management where we still try to prioritise the countless number of reports using heuristics that are often limited with the result that they often remain resident in the systems for months or years. Just to put some numbers into context, let's use the National Institute of Standards (NIST) report that in 2020 tells us that over 18,000 vulnerabilities were recorded where 57% were classified HIGH/ CRITICAL.

BIO

Nicola is Head of CERT in Poste Italiane . He has been working in information security and network for more than twenty years, with vast experience gained in international environments. He was involved in encryption design and network security in the security area, also working in complex infrastructures like mobile and 3G networks. He has collaborated with several magazines in the computer industry as a journalist contributing to disseminating issues related to Security and legal, technical aspects. Since 2005, he's been teaching on Master in Network Security of the Sapienza University. Member of the Association for Computing Machinery (ACM) since 2004 and promoter of technological innovation, Nicola collaborates with several start-ups in Italy and abroad. Member of Startup Italy since 2014, where he helped companies in their development and design of services in the mobile sector; Nicola collaborates with Oracle Security Council since 2014. He is also General Director of the Global Cyber Security Foundation (GCSEC) from 2016 and member of the CERTFIN (Italy's Financial CSIRT).

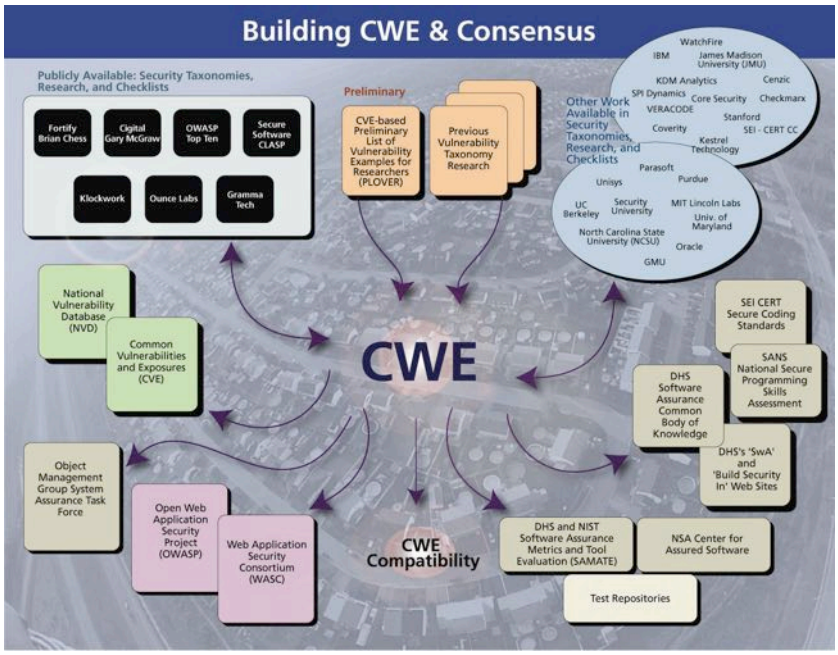
Therefore, on one hand we might be tempted to find methodologies to fix and remediate all vulnerabilities giving us maximum coverage. This option would certainly consume resources inefficiently by fixing even low risk issues. On the other hand, fixing only high-risk vulnerabilities would leave us exposed to other vulnerabilities. The challenge is to find the right combination of these exposed options and reduce the numbers of reports to enterprise IT departments. This area will be one of the arenas we will need to address to increase the effectiveness and value of information security in the new digital environment.

NVD, CVE, CVSS and more:

Let's understand some of the acronyms we find when we talk about vulnerabilities and their management. NVD stands for National Vulnerability Database and is the largest public source of vulnerability information. The database is managed by a group at the National Institute of Standards and Technology (NIST) and is based on the work of MITRE. Vulnerabilities in the NVD are called Common Vulnerabilities Exposure (CVE).

CVEs identify cybersecurity issues and are made public. Each CVE has a number that uniquely identifies the vulnerability in the list. CVEs are a trusted source used by all companies to exchange information related to security issues; companies typically use CVEs, and the corresponding CVSS scores, to plan and prioritise vulnerability management programs. In this context, it is important to understand the difference between Vulnerabilities and Exposure. A vulnerability is in fact a weakness that, if exploited, can be used to obtain unauthorised access, for example, to our computer system. In general, vulnerabilities can allow direct access to a system or a network, execute code, install malware and/or access computer systems to steal, destroy sensitive data. An exposure is an error present in the software/ firmware that allows a malicious user to access a system. In the history of computer attacks, often, the largest data breaches have been caused by an accidental exposure. Common Vulnerability Scoring System (CVSS), on the other hand, provides us with a numerical representation (0-10) of the severity of a security vulnerability. It is precisely because of this ranking that security groups prioritise their vulnerability management program.

CVSS is an open framework managed by the Forum of Incident Response and Security Teams (FIRST), a non-profit organisation based in the United States with over 500 member organisations worldwide. CVSS is now in its third version, which addresses some of the shortcomings of its predecessors. Specifically, version 3 introduces aspects of the privileges required to exploit the vulnerability, as well as the ability of a malicious user to propagate through systems after the vulnerability has been exploited. CVSS scoring is composed of three sets of metrics (Basic, Temporal, Environmental), each of which contributes to the ranking of the vulnerability.

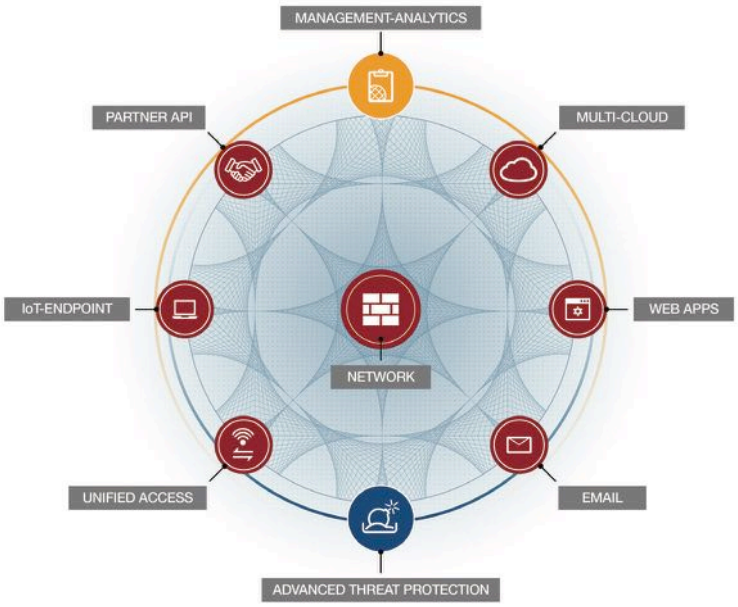


Asset Management, Intel, try to reduce noise:

Several pieces of research show us a scenario in which when a new security vulnerability is released, attackers start a frantic race to scan the network for vulnerable systems while those who defend must implement counter measures in order to protect their infrastructures. Again, from this research we know that on average attackers start scanning within the first 15 minutes of CVEs being released, talking about public vulnerabilities and not zero day. Unfortunately, the number of these CVEs, even just considering the critical ones, is continuously increasing and without proper prioritisation, mitigation actions risk to put even the best IT departments in trouble. Therefore, you need to increase visibility by defining your organisation's assets in a timely manner.

The asset inventory must be complete and dynamic; in this agile digital environment, it is no

longer possible to manage catalogues manually. On this issue we can now help with different tools, in addition to the classic scanning tools, to make the automatic discovery of assets that will then populate a data lake that will integrate the various contributions. Very interesting in this context are also the platforms of External Attack Surface Management (EASM) that can give a valid support in the identification of known and unknown assets facing the public perimeter. All this information can be put in common with CVEs in order to address only vulnerabilities on our "perimeter" and trying to give a weight to our assets for number and relevance in the domain of business critical services. However, it must be kept in mind that vulnerability databases are not keeping up with what attackers are doing to exploit these security holes. Therefore, cross-referencing with good intelligence sources can help us build a prioritisation strategy that also considers the context of public forums, social media, dark web marketplaces, repositories, etc. With these tools and intelligence sources, each organisation will then define its own vulnerability prioritisation scheme and act accordingly.



Scanning, asset inventory, external threat intelligence along with an advanced understanding of exploits is definitely one of the foundations for effective vulnerability prioritisation.

Other ways:

Obviously, the goal is to reduce the number of alerts, as research shows organisations are able to remediate around 5 to 20% of the thousands of vulnerabilities. However, this implies that organisations must be able to keep up with the riskiest vulnerabilities and before they are exploited. An important approach to this issue is one developed by a group of researchers called the Exploit Prediction Scoring System (EPSS) to address this problem. The EPSS algorithm has produced risk scores for all CVEs published since 2017 and can now provide valuable support in predicting the likelihood that a vulnerability will be exploited in the 12 months following public disclosure. Therefore, by applying this system a low EPSS score can suggest to a CIO that despite similar vulnerabilities becoming high profile, this particular one is unlikely to be exploited and therefore not worth wasting valuable time or slowing down business processes to address. The inclusion of EPSS saves resources and allows us to enhance our vulnerability management program.

In addition, advancements in artificial intelligence can offer several opportunities in reducing the manual operation and risk of network vulnerabilities. Increasing network complexity along with the number and sophistication of threats, makes the use of AI relevant to be able to decrease the explosive load on operational and enterprise vulnerability management teams by enabling a combination of intelligent decision making and automation. ■

The digital pandemic years are coming now...

Author: Laurent Chrzanovski

BIO

With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu State University and holds postdoctoral courses within several major EU Universities. He is the author/editor of 32 books, of more than 150 scientific articles and of as many general-public articles.
In the frame of cybersecurity, Laurent Chrzanovski is member and contractual consultant of the ITU roster of experts. He founded and manages the yearly "Cybersecurity Dialogues" PPP Congresses (Romania, Italy, Switzerland), organized in partnership with the highest international and national authorities . In the same spirit and with the same partnerships, he is co-founder and redactor-in-chief of the first cyber security awareness quarterly journal, Cybersecurity Trends, published in Romanian language since 2015, with English and in Italian versions since 2017. His main domains of study are focused on the relationship between the human behaviours and the digital world as well as the assurance of finding the right balance between security and privacy for the e-citizens.

The threat landscape is getting more adverse while, in a paradoxical way, the challenge of raising awareness in cybersecurity and digital hygiene as well as enforcing new laws and rules became scarcely possible to almost impossible.

At this pace, Europeans will very quickly become simple and modifiable items, not even subjects, belonging to the Big Tech giants, in a way we could not resume better than the dialogue between Morpheus and Neo in Matrix – a script written twenty years ago…

Morpheus: *"The Matrix is everywhere. It is all around us. Even now, in this very room. You can see it when you look out your window or when you turn on your television. You can feel it when you go to work... when you go to church... when you pay your taxes. It is the world that has been pulled over your eyes to blind you from the truth."*

Neo: *"What truth?"*

Morpheus: *"That you are a slave, Neo. Like everyone else, you were born into bondage. Into a prison that you cannot taste or see or touch. A prison for your mind."*

The main effect of lockdowns and measures taken in pandemic times is that most people are, much more than before the COVID-19 pandemic, completely lost and confused with their relationship with the real world, the State and the digital world.

"Red flag" alarms come from all disciplines, all domains, all countries, but for the Tech Giants, days are just "business as usual", without limits, without rules, without laws to contain their excesses... exactly now, when, thanks to the 5G implementation, the 4th industrial revolution is achieved.

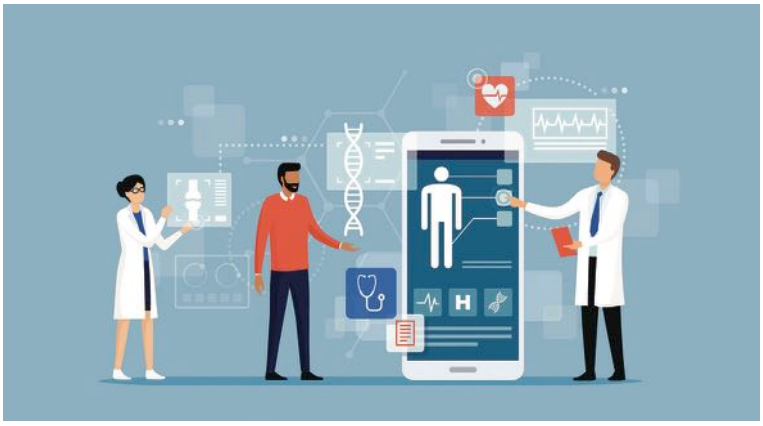
We will try, in this short text, to resume the most important threats we are facing, from a social, humanist and democratic point of view. For this exercise, we will take as a base the yearly milestone report of the IE Center for the Governance of Change (CGC), *"European Tech Insights 2021".*

Published exceptionally in two separate volumes due to the very special moment we live in *(Part I . How the Pandemic Altered Our Relationship with Technology & Part II. Embracing and Governing Technological Disruption),* the report focuses on the fact that a vast majority of the European citizens now have bipolar reactions, approaches and understandings in what they expect from the digital world.

The biggest threat for our democratic system is that if we compare the results on the same issue, we always come to the same dilemma. On the one hand, a huge majority wants laws to tax the High Tech, laws save human jobs vs. automatisation and rules for a stronger control on social media and fake news. On the other hand, most citizens don't trust all the institutions whose duty would be exactly to promulgate those laws, taxes and rules, the parliaments: *"more than 50% of Europeans support replacing their parliamentarians with algorithms. Younger generations particularly support this, with 60% of 25–34-year-olds".*

We can observe the same situation on the most crucial topics of this year:

- **Healthcare:** while *"a majority of Europeans support building a European Health Union to enhance cooperation in the field of public health"* (65%), the same interviewees *"are completely divided when we come to the issue of letting their governments share their health records with private companies"* (45% for, 47% against). Worse *"a majority of young Europeans under the age of 25 are willing to let their insurers collect personal health and exercise data through the use of health wearables"* (46%).

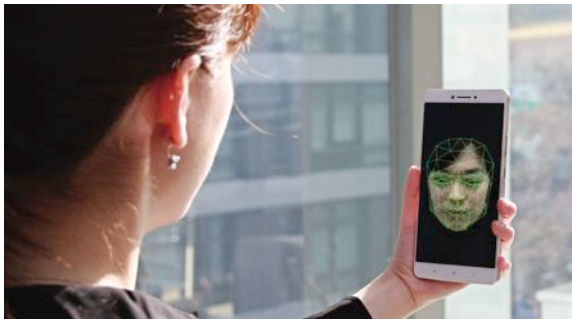


- **Social media censorship and fake news spreading:** *"The perception of Google, Amazon, Facebook and Apple has deteriorated notably over the last year: only Germany supported breaking them up last year. Today all European countries except Italy and Poland are in favour of limiting the power of Tech giants"* with the addition that *"Europeans are overwhelmingly against Facebook becoming a private messaging behemoth"* and that there is a *"wide consensus among Europeans that social networks have had a negative impact and increased political polarization"* (56%). But for the same citizens, *"fake news on social networks should be controlled by the platforms and not by governments"* (55% vs 27%).
- **Jobs:** *"an overwhelming majority of Europeans (61%) are willing to pay more taxes in exchange for raising the salaries of essential workers"; "a vast majority of Europeans wants laws and taxes to save human jobs against automated tasks"* and *"There is a strong and broad support for the introduction of a "tech tax" with 65% of citizens in favour and 15% against".* But at the same time, *"one-third of Europeans would prefer to have an AI rather than a civil*

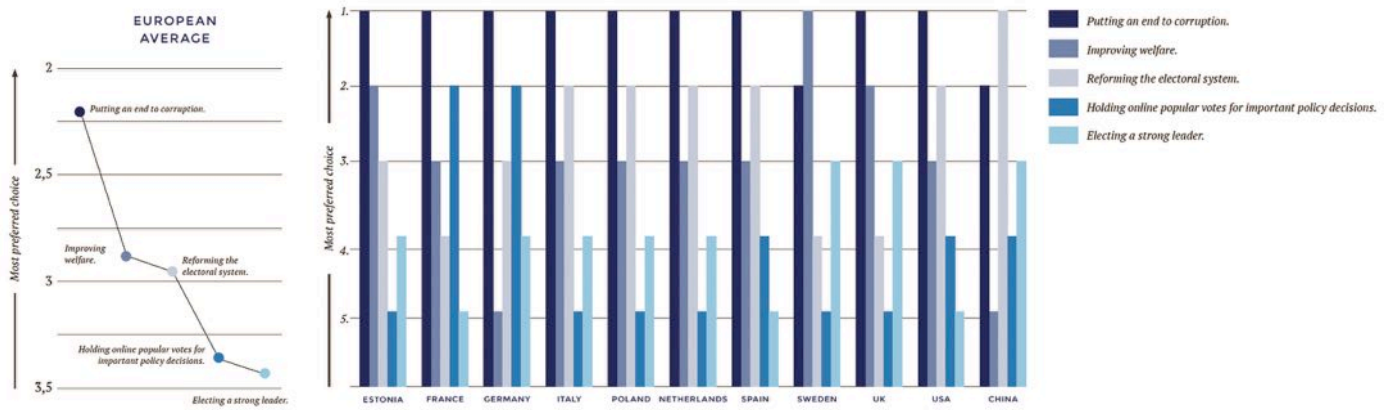
servant make a decision on their social welfare payments or approving their visa. One-quarter of Europeans also trust AI more than humans when it comes to negotiating and granting mortgage loans".

▸ **Online shopping:** The misunderstanding on what is desired reaches its apex with the Amazon case: *"a majority of Europeans (50%) believe Amazon is hurting small businesses and local shops"* but *"up to 64% of British respondents, 48% of Germans and 47% of Italians prefer to buy their books via their platform instead of going to a physical store".* In addition, *"more than a third of Europeans (35%) prefer to have a package delivered by a robot rather than a human"...*

▸ **Dangers of the online world:** *"the vast majority of Europeans (86%) believes digital addiction is a problem"* but *"a vast majority of Europeans want democracy to go digital: 72% would prefer to vote via their smartphones rather than physically, and only 17% are against"* and *"42% of Europeans support the use of facial technology in their daily lives if it makes them more convenient".*



To sum all that, there is a total lack of trust in the elected State, which is severely damaged by a wrong amalgam of all the State Institutions in charge of law and order, not to speak about the wide-spread phenomenon of total distrust in the "deep state". Incompetence, plethoric administrations and bureaucracy (public and private) are not a problem, even welfare comes after the fight against corruption – or better said what is perceived as being corrupt in each State –is the main problem to solve to restore trust in democracy (an opinion shared both by Europeans and Americans)...



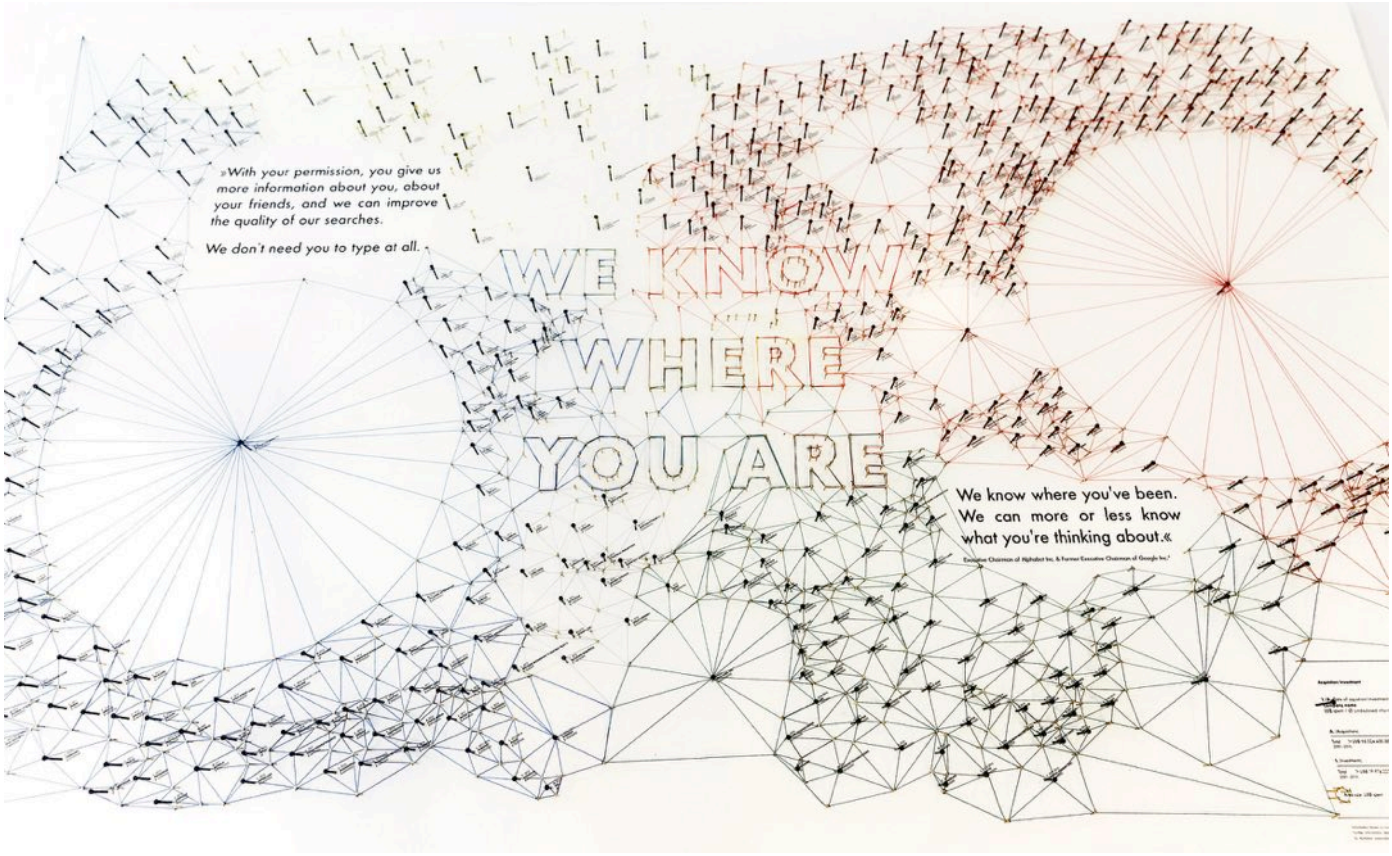
Meanwhile, academic and specialised authorities are waving red flags daily. We selected three topics within the last and more important of them among the enormous panopticon of security and cultural challenges we face.

The first is certainly the live facial recognition one. British readers know better than all what we will write, as it made the headlines of all mainstream news. On June 18th, the UK Information Commissioner, Elizabeth Denham, published on her institution's blog a general public article resuming her deep concern on the urgent limitation needs to face Giant Tech-run live facial recognition (LFR)[1] and, at the same time, to allow law enforcement forces to use this technology at its best[2].

We reproduce here the most impressive phrase of her text, in our opinion: *"We should be able to take our children to a leisure complex, visit a shopping centre or tour a city to see the sights without having our biometric data collected and analysed with every step we take".*

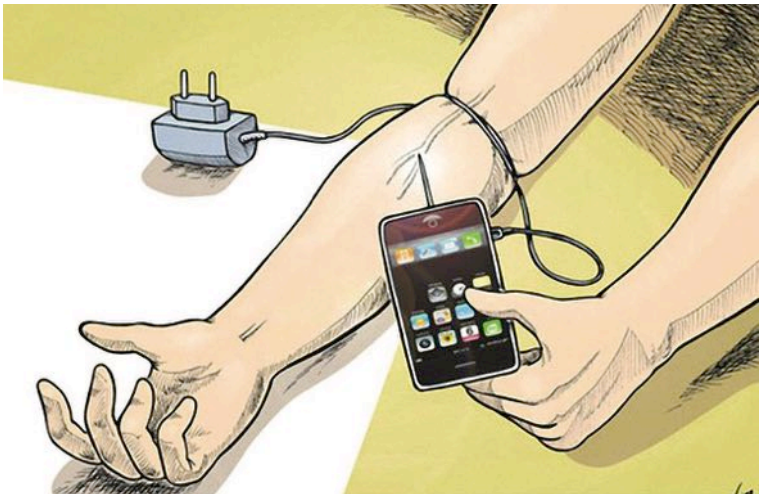
It is useless to say if this phrase is in line with the public opinion we just analysed, the use of LFR by law enforcement institutions and, worse, by intelligence services is totally rejected by the same poll we quoted. For a sensation of comfort, citizens prefer to be followed step by step by the apps they use, against their own personal intimacy, than to let the State do one of its primordial duties with healthcare and education: ensuring the citizens' security.

The second is that no more digital hygiene or cyber awareness-raising will be accepted if it will be considered against each one's comfort. And as



Alphabet City, artwork by Tactical Tech et La Loma, made with openly available GAFAM data.

the majority wants the smartphone to be used all the time, for work, private life, banking, and now even... voting, the gates of hell are deeply opened as there is nothing less secure than a smartphone. Worse, in the enhanced edition of his fundamental "The Shallows: What the Internet Is Doing to Our Brains", Nicholas Carr points out a phenomenon studied in-depth by many scientists in the occasion of the post-lockdown traumatisms: abuse of smartphones, besides contaminating easily the cloud with all possible viruses, is reducing dramatically the external membrane of our brain, the sensitive part which rule is exactly to allow information to enter our memory. The earlier – children, but also adults – start smartphone use excesses, the worse their memory capacities will be, as this membrane regenerates very slowly and stops regenerating after 50 years old (see Tanil, Yong 2020 & Liebherr et al. 2020).



Coming back to Matrix, the thought of Morpheus fits perfectly our times: *"Throughout human history, we have been dependent on machines to survive. Fate, it seems, is not without a sense of irony."*

And to conclude with irony, "Oxford English" could well be the ultimate tool to prevent us from any GAFAM censorship: with colleagues and the agreement of the one mentioned in our text, we paraphrase a description known to us thanks to the milestone for scholars of ancient lighting devices: late Donald Michael Bailey's four volumes of *A Catalogue of the Lamps in the British Museum* (London, 1975-2004).

We used Twitter, Linkedin, Messenger, Facebook and posted: "*our colleague XXX is known to be in congress with selected students*" attaching a picture of him with his PhD students, 99% being women. Our text was not censored while writing nor after posting it on each abovementioned media! Of course, we erased all posts immediately as well as the fake accounts created for this exercise...

Bibliography :

- Nicholas Carr, *The Shallows: What the Internet Is Doing to Our Brains* (updated ed.), Atlantic Books, London 2020
- Cal Newport, *Digital Minimalism: Choosing a Focused Life in a Noisy World*, Penguin Business, London 2019
- Clarissa Theodora Tanil, Min Hooi Yong, *Mobile phones: The effect of its presence on learning and memory*, PLoS ONE 15(8): e0219233. (https://doi. org/10.1371/journal.pone.0219233)
- Magnus Liebherr, Patric Schubert, Stephanie Antons, Christian Montag, Matthias Brand, *Smartphones and attention, curse or blessing? - A review on the effects of smartphone usage on attention, inhibition, and working memory,* Computers in Human Behavior Reports 1, 2020 (https://doi.org/10.1016/j.chbr.2020.100005)
- Gretchen McCulloch, Because Internet: *Understanding the New Rules of Language*, Randomhouse, London 2019 ■

1 https://ico.org.uk/media/for-organisations/documents/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf
2 https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf

Securing your customers - How, Why & What?

Author: Sarb Sembhi

When being asked a "How" question, my first response is usually Why? Why, future-proof security for your customers, and this is a legitimate question for those providing a security service as well as those who would normally be consuming security services from vendors. If you understand the why and it is important enough, we can figure out the how later, but if the why is not big or important enough, the how becomes irrelevant over time.

The simplest way to approach this 'why' question is to think about awareness training you have for staff.

BIO

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

The hope is that the more they learn, the more they will understand and perhaps want to learn as well as make better decisions. Equally, the reason for future-proofing customers is that the more you are able to help them get closer to the end goal, the more they will want to do the right things themselves to achieve the goal. And in reality, it is not just customers you are probably trying to future-proof when it comes to security, it is suppliers as well; but the reasoning and approach isn't vastly different.

However, if you look at the 'why' question from the pros and cons for not future-proofing your customers, then the main reasons for not future-proofing them would include, expending resources on an activity which may be wasted (from an enterprise perspective) and one that could lead to a reduction in revenue (from a vendor perspective). This is a slightly narrow-minded approach, but as in every facet of life, we can see that the more any individual understands any activity, they begin to understand what they don't know and what they need to do to improve to a point where they start to invest more of their own not less. This is true of every hobby, knowledge expanding pastime, or amateur activity, be it knitting, performing magic tricks, playing golf, running, exercising or mindfulness. Or from a business perspective, the better the organisation understands marketing, sales, customer analysis, etc. the more they benefit to a point they will understand

where they need to spend and how they need to organise those activities better.

Let's assume that either as an end user enterprise or a vendor that you buy into the idea that future-proofing your customer's security will benefit you and other stakeholders. The next question is what does future-proofing security for customers actually mean, and what does it include?

To keep this short, what we don't want to do is to give them fish, we want to start them off by teaching them how to fish – to use the universally accepted analogy. Relating this to security, what we want to do is to build capabilities in developing security resilience.

One of the best ways of developing security resilience capabilities in your customers is to get really good at it within your own organisation. If you are not good at it within your own organisation, you have little chance in achieving it anywhere else. So, once you have future-proofed security in your organisation, you will be able to start looking at what that means for your customers.

To this end, if you are able to understand what the blockers are to getting started and can figure out tactics and strategies on how to overcome the challenges in your own organisation, you will be better able to figure out how to get started in this with your customers. And, if you ask the "what" question several times over, to consider what is required in such a programme, you will probably conclude that the most efficient way to achieve the objective, is not to do all the work, but to enable the creation of successful initiatives within each of your customers. The more successful you are at embedding these in, the more successful you will become in achieving the overall objective.

To be successful what you will have to get good at isn't actually future-proofing, but to get good at breaking down every major barrier to successfully getting started in building and embedding risk management and resilience capabilities into an organisation so that the programme is sustainable for the long term.

In keeping with the approach of not having to fish for your customers continuously and teaching them how to get started and improve over time, to make this sustainable, involves encouraging them to share their successes and how they overcome their challenges, and contributing to that process. If you act as if you are the fountain of all knowledge you will only set yourself up to fail, the knowledge and the learning must come from a wide range of different experiences shared across all participants so that there is better relatability across them; your organisation's experiences may not be the best example for everyone.

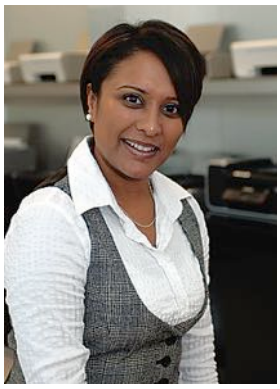
Finally, any successes in any customer future-proofing their security are their success story not yours, promote them and refer anyone interested to them, let them help others to futureproof their customers.

I appreciate that this is a very simplistic approach, but my view is that we don't need to over complicate things.

As members of the industry we all have a role to play in future-proofing the security for our customers,

suppliers, board members, the wider community and other stakeholders. I have been working on this for several years with many others. I would encourage every organisation to consider initiatives which raise security for all, as I would like to see the low hanging fruit to no longer be low hanging for attackers. We cannot assume that others will do something when we don't show our own commitment to the future. Good luck, let me know how you get on – you can find me on LinkedIn. ■

Future-proofing customer security: The magic bullet.



Author: Raj Meghani

Future-proofing. Now there's an interesting word in the context of security. Future-proofing security. Is that even possible in today's world? If so, why aren't more organisations doing it?

In the world we live in today, it's no longer just about defending your technical infrastructure, your data, your employees. It's also about protecting your customers.

The customer journey has evolved rapidly as a result of the pandemic which means that with remote working, etc. comes a new set of challenges and an increasing need to increase secure, remote working and cybersecurity resiliency. The level of complexity for customers has increased as cyberattacks get more sophisticated and there continues to be a plethora of additional security products and applications entering the market.

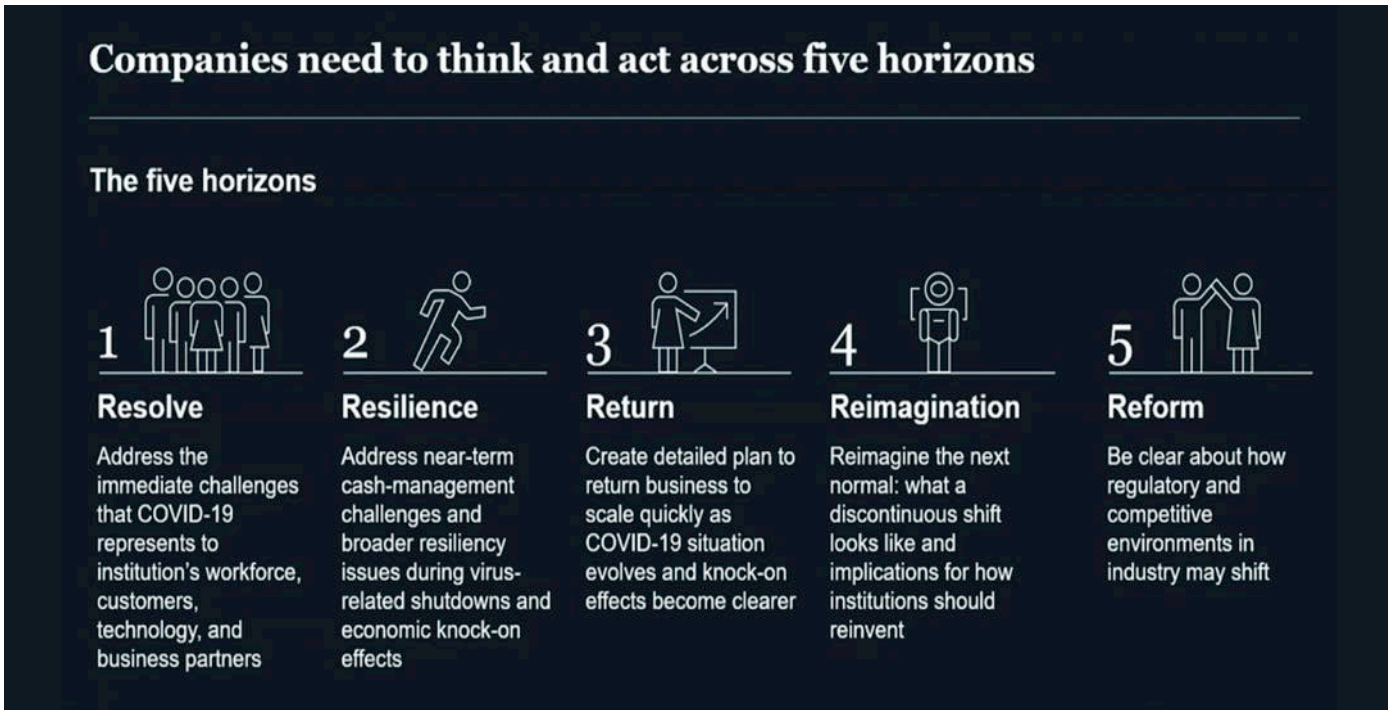
The rapid growth of digital outlets and transitioning to the cloud has also provided new opportunities and infiltration avenues for cyberhackers. It's not just your customers' data that is at risk, it's their supply chain and contacts too.

McKinsey's views on the path to the next normal in a post-pandemic world for businesses – the '5 Rs' - make an interesting read.

- Resolve
- Resilience
- Return
- Reimagination
- Reform

BIO

Raj Meghani is the Chief Marketing Officer and Executive Director at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with an advanced, intelligent cyber defence platform through its unique Monitor, Manage, Automate & Respond (MMAR) framework and single pane of glass view.Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 20 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com



Source: McKinsey, "5 Rs on the path to the next normal"

They talk about businesses, in general, being in the 'Return' phase.

If I put on my cybersecurity hat and apply the 5 'Rs', I'd be more inclined to say businesses are still in the 'Resolve' stage given the rapid increase and sophistication in cyberthreats we are seeing on a daily basis.

Most businesses have some form of security deployed – no matter how basic e.g. a firewall, email security, etc. But with these disparate technologies not talking with each other, exposing vulnerabilities via a wider attack surface, how can businesses be confident they can manage and secure their customers and supply chain's sensitive information when they themselves are often firefighting in a reactive mode?

Businesses who aim to become more security resilient will require security expertise and intelligent toolkits which can automate and collaborate across entire infrastructures through a single view. They will require a 'built-in, not a bolt on' approach. A preventative approach to block advanced persistent threats through real-time visibility across their entire security ecosystem helps them stay ahead of their attackers and provides peace of mind to their customers.

Returning to the norm will require a shift in mindset across the business – not just IT. Cyber attackers are getting savvier, ransomware is on the rampage and businesses need to look at how they can better utilise and enhance their existing security ecosystems to protect themselves, their customers and their supply chain.

Reimagine the attack surface for cyberattackers during and post COVID-19 and fast forward to what that looks like tomorrow in light of the increasing cyberattacks. Safe today but what are the repercussions if your business is breached? Fines. Reputational damage. Customer attrition. Legal proceedings. Protect the security of your customers today – you don't need to reinvent the wheel, you just need to plug any vulnerabilities that expose risks to your business, its employees and that of your customers.

I predict more stringent regulation and data privacy laws ahead which will inadvertently protect your customers.

I predict more businesses will be under the cybersecurity spotlight when trying to win new business and clients.

I predict reform in that protecting customer's security will be more strictly enforced – it won't be an option.

I've said it before, and I'll continue to say it. Future-proofing your security is a mindset and cultural change – not just a technological one. Doing everything within your power to stay steps ahead of the hackers and thinking about the safety of your business and that of your customers is paramount – and it goes a long way towards supporting customer retention in the process. ■

Can we Automate IT?

Author: Marco Essomba

The network and security industry has been talking about automation for quite some time now.

In fact, the uptake of automation (an increase of 12% in 2020 over 2019 reported - World Economic Forum) across various industries is on the rise and it has been changing the way these businesses operate, particularly the industrial, aerospace and manufacturing to name a few.

BIO

Marco Essomba is the Founder & CTO of BlockAPT. A leading edge UK based cybersecurity firm empowering organisations with an advanced, intelligent cyber defence platform. The BlockAPT platform allows organisations to Monitor, Manage, Automate & Respond (MMAR) to cyber threats – 24/7. Marco's passion, expertise and knowledge over 15 years of providing cybersecurity solutions has culminated in the design of our unique BlockAPT platform. Developed over time as a toolkit to help small and large enterprises business security issues, BlockAPT's platform brings together threat intelligence, vulnerability management, device management and proactive incident response management to help fight the war against cyber attackers.

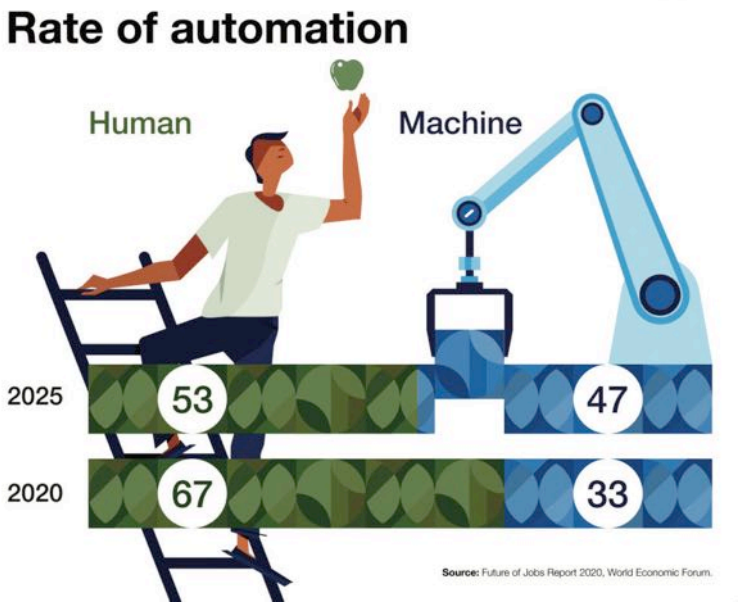
LinkedIn - https://www.linkedin.com/in/marcoessomba/

Twitter: https://twitter.com/marcoessomba

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

Security & Automation

Notably, SpaceX was a large step for automation, allowing astronauts to dock successfully into the International Space Station with minimal effort. A small step for spaceflight, but a giant leap for automation!



There is however a misconception that automation (i.e. implementation of automation technologies) is here to take away human jobs. But that is not the case. Robots are not coming for your job (yet). Yes, in essence the whole deal about automation is reducing human intervention but that doesn't necessarily mean taking away but more so addressing a pain point. Take monitoring for example, we have talked about alert fatigue being a major issue in the security environment globally. The application of automation will help cut through the noise and find the real threat that can otherwise be left unaddressed for a while. And insecurity that time is enough to leave a mark.

In addition, automation is driven by application technologies and this can add value to areas like threat intelligence as it compliments machine learning and ultimately can fuel Artificial Intelligence (AI) too. The reason being automation is multi-faceted and collects/organises data at a large scale to draw hypotheses. This is useful for insights and resource utilisation. And thus, so far we have built a soft case for automation in network security.

A strong(er) case for automation in Security

I may be biased towards automation since at BlockAPT our fundamentals are deeply tied to this. There are some barriers to automation caused by:

▸ **Complexities** - A lot of organisations have acquired/invested/created tools or software which may be custom or now legacy. Such organisations find it hard to adopt automation as this means a complete overhaul of technology and possibly a full-blown transformation project extending beyond security. This may be a tough pill to swallow but that is ultimately the fix. As companies scale up and grow they need to address the complexity before it becomes a challenge. Realisation and working towards implementing automation as soon as possible should be on top of their strategy with buy-in from the board level.

▸ **Resources** - As with any investment, automation requires that security professionals be trained to adopt and utilise this to streamline security operations. However, as mentioned talent is hard to come by and it is getting even harder to retain professionals. These can act as a barrier to automation implementation as organisations need a dedicated team to make this work.

▸ **Costs** - I saved the most obvious one for the end. As with any digital transformation project starting from the outset, an organisation will need a combination of technology, people and processes to ensure its successful adoption. Tools can be expensive and usually, one size does not fit all as organisations come in all shapes and sizes (i.e. technologies and tools used).

But fortunately, we have already witnessed a dramatic shift towards the use of automation in 2020. Organisations are investing in adopting automation tools to supplement their integration of existing capabilities as opposed to integrating existing tools through in-house integration projects. Marketing automation is an example of this as organisations are more and more tuned to digital. This means more channels, analytics and platforms to monitor, manage and work on for marketeers. It is very similar across security too but with the added skills shortage of security personnel.

When it comes to security automation, some of the key benefits are:

▸ **Cost-effectiveness:** For security operations, automation allows faster data sifting, collaboration and workflows making responsibilities like incident response extremely efficient and without manual intervention. By eliminating resource-draining repeatable and menial tasks, security professionals can concentrate on important tasks. For organisations in the long run, the ROI on manpower and efficiency will be extremely rewarding.

▸ **Better resources utilisation:** Automation takes away the 'alert fatigue' from analysts and this means resources are more effective and confident in their tasks. Organisations will also find it easier to retain, train and onboard new talent as the processes/workloads can be divided in a much better manner. Having the technology to aid in monitoring, threat hunting, alerting or responding makes a security professional's job better without a doubt.

▸ **Reducing complexity:** Automation (when intelligently adopted) will no doubt reduce complex

processes by breaking them down, taking out the repeatable/time-consuming tasks and enabling collaboration. It has been reported in the past that on average a security analyst of a large firm has to manage 10 different tools, making reporting a nightmare (NIST on Alert Fatigue). Automation technology can make tools that otherwise do not work well together, collaborate, complete actions with custom workflows and ultimately bring everything into a single view for better management.

As you can see I simply re-used the previously mentioned 'barriers' and flipped them as positives. And that is precisely what automation does to organisations. There are two sides to everything!

But of course, there are more benefits to mention that will outweigh any initial hurdle for an organisation. One of the key ones is a reduction in a margin of errors as progressive automation brings AI, and that increases analytics capabilities. Ultimately, decision making will benefit also (i.e. guided by concrete data) whether it is from security operations or a leadership point of view.

So, should you Automate IT?

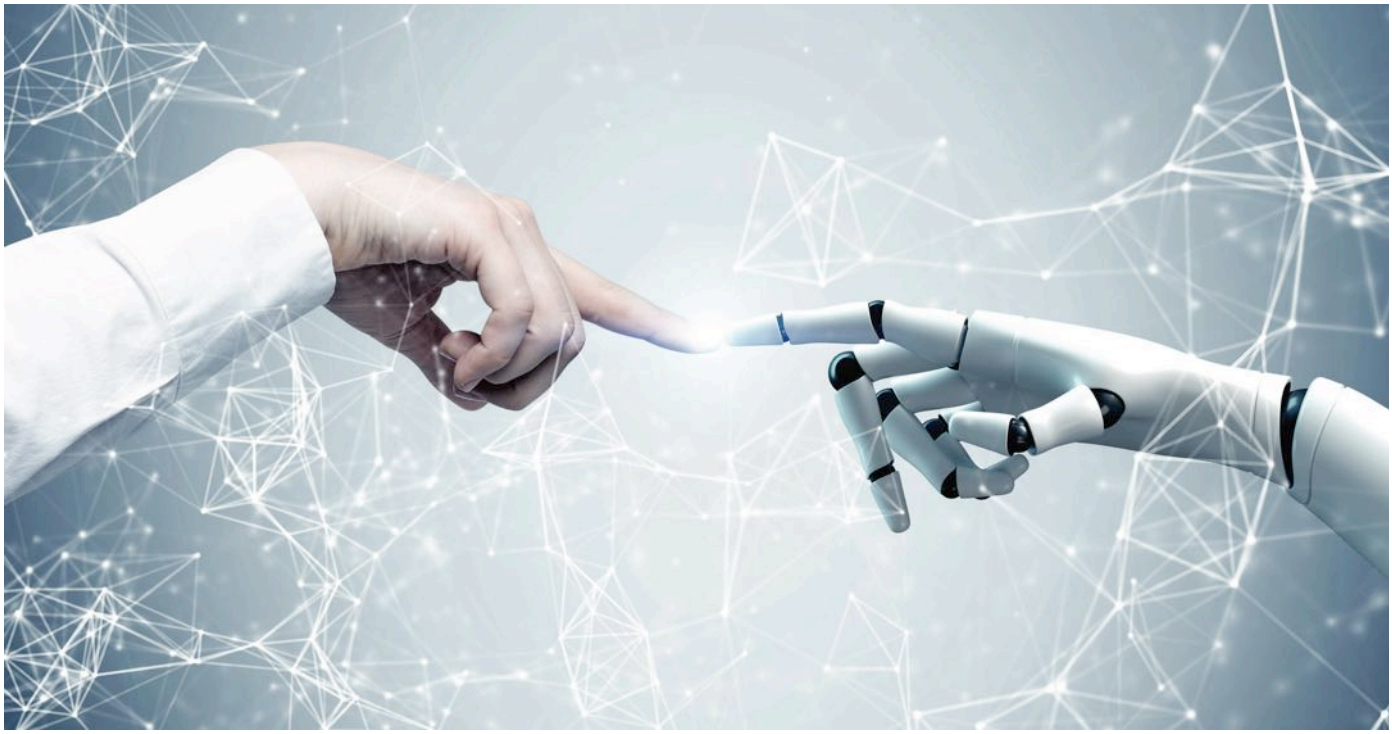
Well, the answer is yes and no.

No, if you're doing it as a tick box exercise or vanity project.

But a massive YES, if it is to improve end-to-end security operations throughout the organisation. Remember, threats are growing at an alarming rate and getting more sophisticated. To better understand, investigate and remediate these, security leaders and operations teams need to be able to rely on technology automation to take care of repeatable workflows so that they can focus on problem-solving.

One thing is clear, automation is vital to future-proof your organisation's security and protecting your digital assets from advanced threats.

It may seem like an immense challenge for our industry, but one organisation can surely overcome it. If automation can send humans to a space station just imagine what it can do in network and security. ■



The UK Response to cyber risk in SME and supply chain for post pandemic recovery.

Detective Superintendent **Paul Lopez**

In the East of England, a new not for profit company has been recognised as a critical factor for economic recovery and societal resilience by protecting rapid post pandemic national business growth and in the much-needed development of national work-ready cyber capability.

The Eastern Cyber Resilience Centre (ECRC) is a police-led, not-for-profit company, working in partnership with Academia and CyberSecurity experts with the aim of increasing cyber resilience amongst Small and Medium businesses, government agencies and the third sector.

BIO

Detective Superintendent Paul Lopez joined Essex Police in 1993. Over the past 5 years Paul has worked across number of diverse disciplines including Serious and Organised Crime, Intelligence and most recently headed up the Regional Cyber Crime Unit. Paul has recently been appointed as Director of the Eastern Cyber Resilience Centre and is keen to use his experience to support businesses within the region tackle the growing threat of cyber-crime and improve their levels of cyber security by providing affordable cyber resilience solutions.

THE EASTERN CYBER RESILIENCE CENTRE

The ECRC is one of a new network of nine such Centres across England and Wales. A National Cyber Resilience Centre is due to launch imminently. This will support regional centres by engaging with national stakeholders including large businesses and National/Regional Government. The business community has demonstrated enthusiasm, as this solution escalates problem solving for the cyber skills talent shortage in business and policing, as well as the growing risk to smaller businesses from cyber-attacks. Many of our SME businesses are critical links in the UK's supply chain and do not have the skills or knowledge to realise and mitigate risk alone. In an interconnected world, this of course affects us all, and the generous and forthcoming investment from the private sector to develop the Centres is true partnership in action in a digital age.

The need to engage smaller businesses within supply chains and provide them with affordable solutions and practical help they can apply, has become a global challenge for post pandemic economic recovery.

International law enforcement and the World Economic Forum have expressed interest in this transformational UK Cyber Resilience Centre Programme.

The solution:

The framework that the UK's National CRC Programme has used is transformative, yet highly adaptive to ensure it can adopt and implement the national country requirements.

The programme governance structure also benefits from engagement and funding from global brands as well as strategic regional organisations. It has proven attractive to highly innovative, entrepreneurial companies and welcomed by global technology companies.

Strategically informed and tracked engagement enables threat intelligence to drive educational and preventative guidance at speed, improving resilience across the right organisations at the right time.

The model has exceptional potential to swiftly support Overseas Territories and Crown Dependencies. It is efficient, smart, agile, and responsive.

Conclusions:

1 A regional and national focus on protecting and improving cyber resilience throughout the supply chain to support post COVID-19 pandemic recovery and societal resilience. Supporting business growth through increased IP and operational protection is critical.

2 Interpreting and implementing national and international threat intelligence for SMEs, vulnerable organisations and third sector charities through affordable baseline cyber resilience solutions is required.

3 Cyber resilience solutions delivered by a nation's own developing cyber and academic resources, using tight and transparent service governance, a controlled and protected central service platform and internationally recognised skills and knowledge is a viable option.

4 Rapid dissemination of guidance and support to counter emerging national and international cyber threat intelligence and to provide the nation's security services with a complete and live picture of cybercrime and the security stance of SMEs, vulnerable organisations and third sector is advantageous.

5 The CRC model solves the engagement challenge of smaller and/or vulnerable organisations that believe they have no need or are afraid to engage cyber resilience support but who need help to manage cyber risk to their own businesses.

6 The UK model provides effective solutions for SMEs to choose and engage suppliers with knowledge, confidence and trust, solving problems in the short term and building legacy trust in quality provision within this emerging unregulated sector for the future.

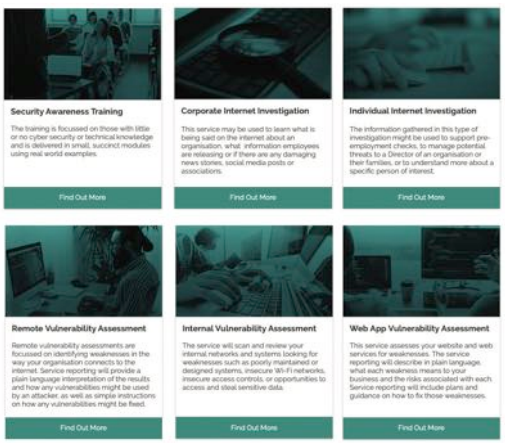
7 The internationally recognised skills and knowledge delivered through the programme ensure a high quality, escalated, workplace-ready, talent pipeline solution to accelerate talent supply into law enforcement, defence and Critical National Infrastructure (CNI) as well as the private sector.

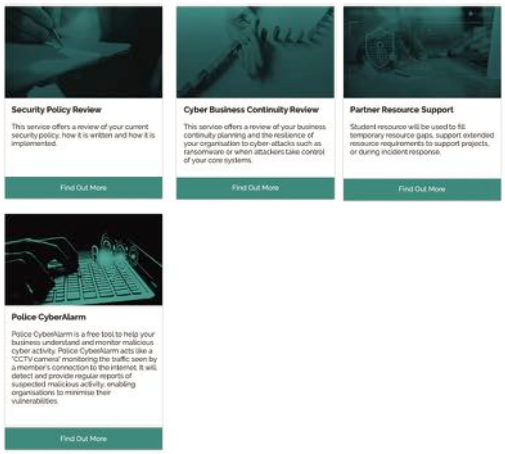
8 Investment and support from large entrepreneurial and tech focused companies who want to be associated with economic recovery programmes and national academic and talent development is forthcoming.

9 Programme implementation has proven resilient throughout the pandemic and can be deployed remotely, providing high return on investment from public seed funding.

10 This innovative transformational model is adaptive to be designed and implemented to align with key stakeholders, threat intelligence imperatives, technology and development strategies and key academic and skills development initiatives.

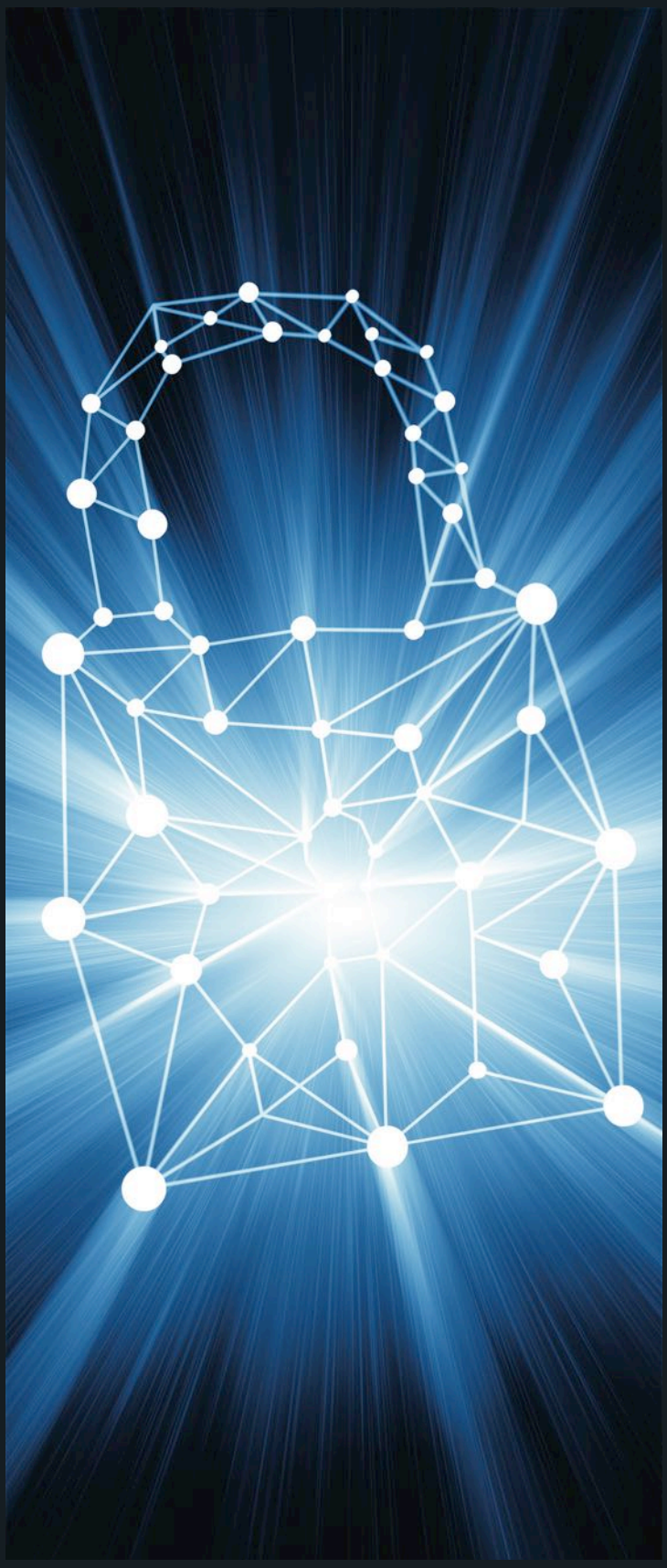
11 It is tried, tested, and trusted by the UK Government. Early-stage progress is being monitored for additional impact specifically with the supply chain to CNI. ■





For more information, please visit The Eastern Cyber Resilience Centre https://www.ecrcentre.co.uk/ or the network of Centres across England and Wales https://www.brimcentre.com/network.

Cybersecurity Trends



A publication

web for your business
swiss webacademy

edited by:

BLOCKAPT™

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

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

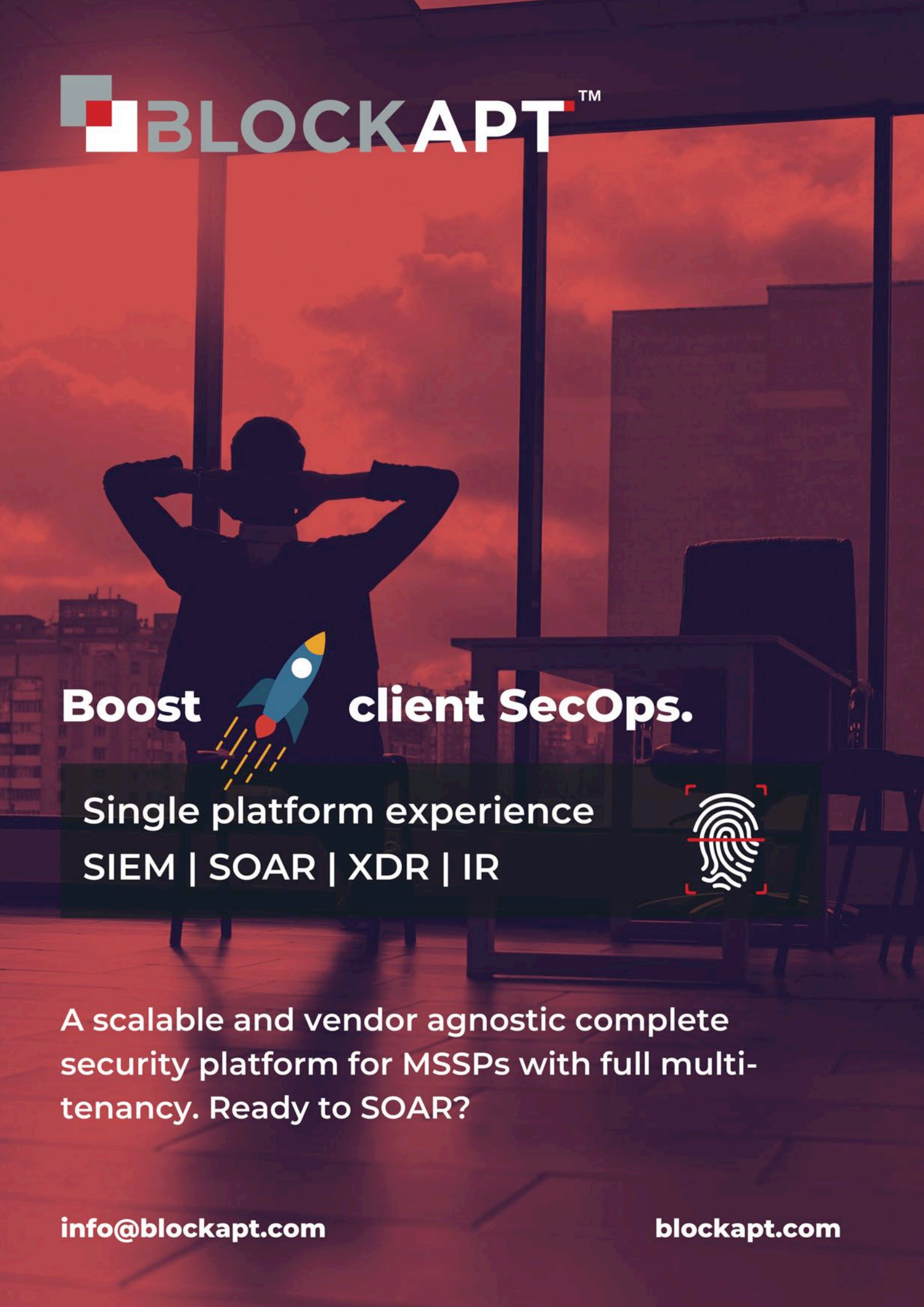
ISSN 2559 - 6136
ISSN-L 2559 - 6136

Addresses:
Swiss Webacademy - Str. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

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

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

BLOCKAPT™



Boost client SecOps.

Single platform experience
SIEM | SOAR | XDR | IR

A scalable and vendor agnostic complete security platform for MSSPs with full multi-tenancy. Ready to SOAR?

info@blockapt.com

blockapt.com