Cybersecurity Trends

UK edition n.1 / 2021

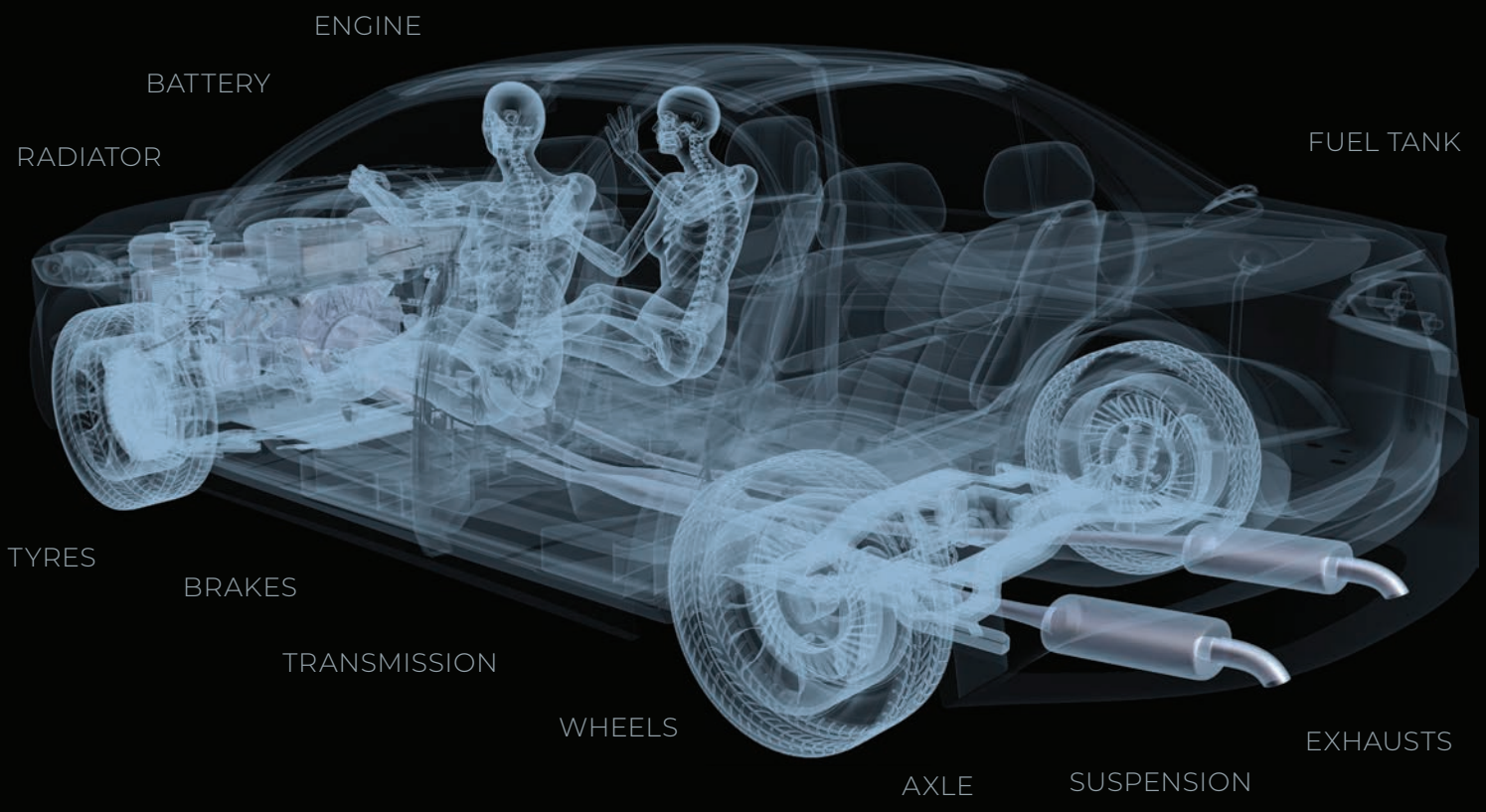
Nation-state Attacks, 3rd Party Attacks, APTs...

BLOCKAPT™

WHEN DEFENDERS BECOME PREYS: HOW TO BEEF UP YOUR RESILIENCE

BLOCKAPT™

You may have ‘best in class’ security, but are you moving forward?



We bring together essential components to power your security.

All driven by our MMAR* technology

*Find out more at www.blockapt.com

Contents



Authors : Raj Meghani, Marco Essomba, Laurent Chrzanovski

Security... still a long road ahead

In our last few editions, we highlighted a lot about the state of affairs when it comes to Small and Medium Enterprises (SMEs) particularly looking at security adoption across the board, educating the staff and dispelling some security myths when it comes to technology implementation.

In some ways, a lot of our industry peers recommended that SMEs take a page out of their larger counterpart's playbook and start thinking about advanced security, as we concluded that every organisation no matter their size or mode of operation remains a real target for cybercriminals.

But the second half of 2020 (and still ongoing!) has exposed new weaknesses in the security preparedness of enterprises, governments and entire nations themselves. The on-going COVID-19 pandemic has no doubt unearthed a lot of these and we can safely say that 2020 has certainly been a rough year for the enterprise security teams with some high profile nail-biting moments for CISOs and Security Heads.

One of the breaking news of this first quarter, which we explore in this edition, is the hack of Solarwinds as definitive proof that the playing field has changed. Dubbed as one of the "most sophisticated attacks" seen so far, we are looking at brave cybercriminals (and their sponsors) taking on the security giants in the industry and taking out critical infrastructure. And as we speak, security leaders are preparing for the growing number and sophistication of attacks in 2021 and beyond. But in our opinion, a lot more needs to be done.

We also look further into the exposure of risks and reputational damage as a result of cyberattacks not just to the organisations but also along their supply chain.

One thing to be said is that the security industry has certainly become provocative!

From movies, TV series (eg, Mr Robot) to gaming, security has seen the hype that has made the art of cybersecurity infamous. We also see new terminologies emerge monthly, new advanced point solutions, AI and machine learning engines that do it all for you...i.e. the next best security tool that you must have. But the perception of the general public, organisations and teams created by marketing or media is far from reality.

Yes, advances have been made but a deep look into 2020 and ongoing enterprise security posture reveals that teams are still:

- Struggling with a lack of visibility into threats (often alerted too late)
- Bombarded with alert-fatigue or data volume
- Dealing with access privilege issues even after concepts like Zero Trust have gone mainstream
- Tackling breaches arising from endpoints and email targeted attacks

It is estimated that a business will fall victim to a ransomware attack every 11 seconds in 2021. That's down from every 14 seconds in 2019. The total cost of ransomware will exceed $20 billion globally and that translates into more time to investigate and respond to breaches for security teams and more damages to digital assets for organisations.

A reactive approach and having a cyber incident response plan is no longer on a level playing field with the attackers. Technology and humans need to be better connected to stay steps ahead of the cyberattackers and adopt a preventative approach to cyber breaches. Neither people nor technology are infallible.

Perhaps, stripped away from the cyber-glitzy jargons and security-tastic attributes, we are not quite as advanced as advertised. The build-up has not lived up to the real-world challenges - as evident from the disruptive example we have already witnessed.

And thus we say it as it is with security..... there is still a long road ahead. ■

When the (threat) hunters become the prey. How scared should we be?

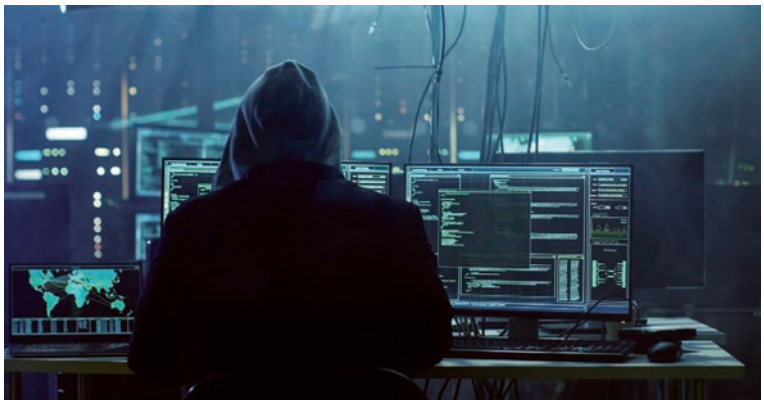
Author: Marco Essomba

Nation-state attacks vs. the IT industry

The last 18 months have shown that the cybersecurity industry needs a robust security response, particularly on a global scale and for the industry to become more cyber resilient.

Before the end of 2020, we witnessed various high profile and serious nation-state led cyberattacks - most notably the attacks on the U.S government institutions and critical infrastructures that are still having a global impact. While it is not uncommon to hear about the rise of nation sponsored attacks in this digital race era, we must recognise that the latest and most advanced attacks routes were channelled through security firms. This goes way beyond the 'espionage as usual' norm that we are used to seeing.

This illustrates that the cybersecurity landscape continues to evolve and become much more dangerous especially when the custodians of the security themselves become targeted with sophisticated offensive measures.



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

When we started seeing the sophisticated attacks in light

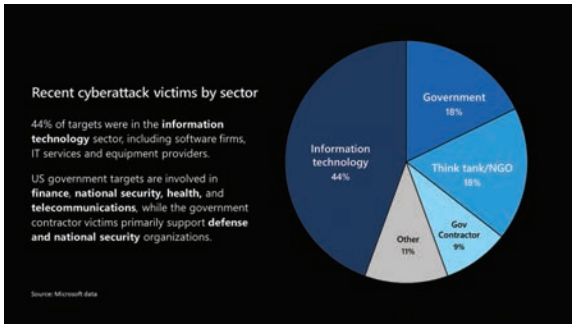
No account of details can be conveyed without mention of the dreaded "C" word, so let us get that out of the way. The COVID-19 pandemic has been a major contributor to the rise of advanced threats particularly when cyberattackers aimed their sights at hospitals and public health authorities, from local governments to the World Health Organisation (WHO).

Notably, in July 2020, the UK accused Russia of trying to steal vaccine-related information through cyber-espionage. The officials confirmed they had continued to see an "ongoing threat" of nation-states targeting the vaccine research-and-delivery programme.

Using the IT sector as the attack vector

A recent 'attack by sectors' report published by Microsoft stated that 44% of attacks were aimed at the technology sector, including IT and software providers. Next up were direct attacks on the Government sectors (18%), NGOs and Thinktank organisations (18%) followed by other sectors (11%) and Government contractors (9%).

Foreign-sponsored attacks have figured out that the most lucrative attacks are through the trusted supply-chain network, particularly the IT and security providers. If you are a foreign adversary looking to gain national intelligence, gain technological advancements and take down critical infrastructure, this makes total sense. Why play the long game when you can go straight to the source?

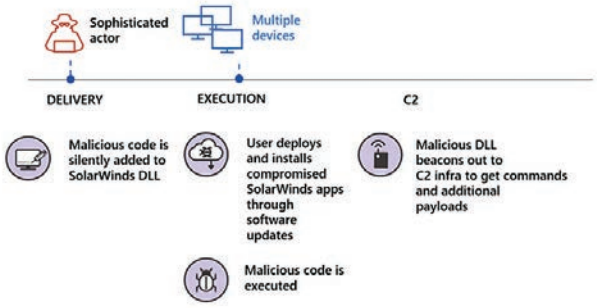


The notoriety of attacks that revealed all

For years, the renowned cybersecurity firm FireEye has been the first call for government agencies and companies around the world who have been hacked by the most sophisticated attackers, or fear they might be.

In December 2020, FireEye was in the spotlight when it revealed that its systems were penetrated by a nation with top-tier offensive capabilities. The company announced it had suffered an intrusion that resulted in the theft of some 300 proprietary red-teaming software tools the company provides to clients to help secure their IT operations. The hackers used novel techniques to make off with their tool kit, which could be useful in mounting new attacks around the world. Subsequently, the investigation led to the discovery of SolarWinds breach.

SolarWinds, another major US information technology firm, was also the subject of a cyberattack that spread to its clients and went undetected for months.



Solorigate supply chain attack diagram

Hackers secretly broke into SolarWinds' systems and added malicious code into the company's software system. The system, called "Orion," is widely used by companies to manage IT resources. SolarWinds has 33,000 customers that use Orion but alarmingly US agencies – including parts of the Pentagon, the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration, and the Treasury – were attacked by the nation-state (allegedly Russia).

No doubt that SolarWinds, with its lengthy list of government and large enterprise customers, is a desirable target for an adversary nation looking to profit from these exploits.

SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom	General Dynamics	Sabre
Ameritrade	Gillette Deutschland GmbH	Saks
AT&T	GTE	San Francisco Intl. Airport
Bellsouth Telecommunications	H&R Block	Siemens
Best Western Intl.	Harvard University	Smart City Networks
Blue Cross Blue Shield	Hertz Corporation	Smith Barney
Booz Allen Hamilton	ING Direct	Smithsonian Institute
Boston Consulting	IntelSat	Sparkasse Hagen
Cable & Wireless	J.D. Byrider	Sprint
Cablecom Media AG	Johns Hopkins University	St. John's University
Cablevision	Kennedy Space Center	Staples
CBS	Kodak	Subaru
Charter Communications	Korea Telecom	Supervalu
Cisco	Leggett and Platt	Swisscom AG
CitiFinancial	Level 3 Communications	Symantec
City of Nashville	Liz Claiborne	Telecom Italia
City of Tampa	Lockheed Martin	Telenor
Clemson University	Lucent	Texaco
Comcast Cable	MasterCard	The CDC
Credit Suisse	McDonald's Restaurants	The Economist
Dow Chemical	Microsoft	Time Warner Cable
EMC Corporation	National Park Service	U.S. Air Force
Ericsson	NCR	University of Alaska
Ernst and Young	NEC	University of Kansas
Faurecia	Nestle	University of Oklahoma
Federal Express	New York Power Authority	US Dept. Of Defense
Federal Reserve Bank	New York Times	US Postal Service

Similarly, there are also accounts of McAfee, Symantec and Trend Micro among the list of major security companies whose codes have been stolen by hackers.

Coming to terms with the subject

Security firms have become a frequent target for nation-states and hackers, in part because their tools maintain a deep level of access to corporate and government clients all over the world. By hacking into those tools and stealing source code, spies and hackers can gain a foothold to victims' systems.

It is no doubt that the aforementioned firms take security very seriously and have state-of-the-art tools. But these breaches are reminders that nobody is immune to the risk of being hacked. The reality is that every organisation or institution is subject to the same truth that compromise is inevitable.

Moreover, the very art of successfully penetrating security firms means that foreign states have vastly upskilled their tools, technologies and hacking skills. Regular businesses and organisations simply cannot compete with that level of cyber onslaught often backed by state-led investments and adversary talents recruited from the deep-web.

Building hope & extra cyber resilience for businesses

Now that we have acknowledged that attacks are inevitable and by the time you realise it, it will likely be too late. It is time to work towards readiness.

No single tool can be relied on to never fail and no single point solution can be expected to protect your business or organisation wholly.

For security leaders, this is a good time to reflect on their dependence and trust in technology solutions. They need to prepare for when their supply chain (MSSP, Security, IT or Application/Software Vendor) is compromised.

For organisations, a defence-in-depth approach is key. In other words

a deeply layered approach to security without relying solely upon single vendors or tools. This is the reason why large enterprises put monitoring solutions like SIEM (Security Information & Event Management) in place but also invest heavily in SOAR (Security Orchestration Automation & Response) to help with automated Incident Response and procure Managed Security Services to help with resourcing. These technologies and resources (if properly integrated) work hand-in-hand to alert, respond or trigger failsafe should there be a breach.

The cybersecurity industry should work in collaboration with businesses to address the challenges of disparate solutions by acknowledging the limitations of solutions and also providing freedom of choice to achieve security synergy.

On a national level, the Government has a responsibility to educate businesses to shift the perception to realise that state-sponsored or led attacks are the major threats. Transparent talks with businesses and better collaboration with the cyber industry on the state of security will dispel any false sense of security and go a long way towards preparedness. ■

Cybersecurity's role in enabling digital transformation and maintaining trust for the healthcare sector

Author: Saj Huq

The past 12 months has placed extreme, unrelenting stress on the healthcare sector. As organisations were focussed on saving lives, malicious actors spotted an opportunity to capitalise on their vulnerabilities, the critical reliance on healthcare services and the heightened emotions about the virus.

Threats have included attempts to steal intellection property from organisations developing vaccines, ransomware attacks and disinformation campaigns. Even as COVID-19 vaccines are being rolled out, criminals are sending fake text messages, purporting to be an NHS representative getting in touch about a vaccine appointment, to scam people into sharing their bank details. And, according to security firm Positive Technologies, half of all cyber attacks on healthcare involved ransomware from July-to-September 2020. These threats create an atmosphere of uncertainty and distrust and could affect the sector's ability to maintain services, but we can't allow this to undermine the digital transformation that healthcare is undergoing.

Before the pandemic, the sector was already evolving into a new era where AI, advanced analytics, connected devices and other technology unlocks opportunities to provide more personalised and efficient services. At a recent roundtable LORCA held with cyber innovators, policymakers and healthcare professionals, we heard about how the pandemic has also accelerated the adoption of telemedicine and increased the level of data sharing across new regions and infrastructures.

But attendees told us that for the public to benefit from these innovations, they need to trust healthcare organisations to store and use their data

BIO

Saj Huq is the director of LORCA: the government-funded London Office for Rapid Cybersecurity Advancement. LORCA recently held a roundtable with healthcare professionals, security experts and policymakers to explore the cyber challenges faced by the health sector and the innovation gaps that exist. Read the full report on LORCA's website: lorca.co.uk/lorca-needs-accelerator-healthcare

securely. Organisations need cybersecurity solutions that protect public data and they need to clearly explain the security measures they are taking to people. Past data sharing initiatives have suffered from public concerns about data, and when it comes to technology like AI it's more important than ever that people understand the complex algorithms and privacy controls that are being used.

In with the new, but the old is sticking around

Cyber innovators looking to help secure the health sector also need to take its current IT infrastructure into account. Although healthcare organisations are making giant leaps in many areas, attendees stressed to us that they are also grappling with many of the same IT challenges from ten years ago. They are balancing cloud-based infrastructure and new technology with legacy architecture. Protecting data shared across the ecosystem, securing legacy devices and defending against ransomware attacks are not new challenges.

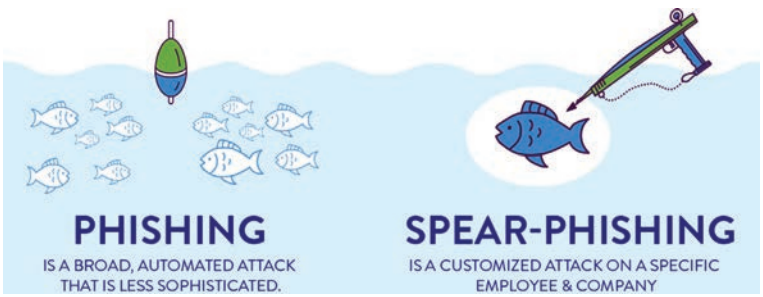
In some cases, the acceleration of digital transformation has made existing limitations more obvious. Attendees described examples of clinicians uploading information to medical forums to access a second opinion when they didn't have the tools to consult with colleagues remotely. This is a hard in-between stage to be in.

Digital transformation

This is an exciting moment for healthcare. The sector is undergoing huge digital transformation, with the pandemic accelerating many of the plans that were already under way. The past 12 months have also demonstrated some of the benefits that digital innovation in the sector can bring, from vaccine development to greater healthcare monitoring. Much of this progress is dependent on sensitive data, which means secure by design and privacy by design principles need to be built into the operating fabric of the healthcare system if it's going reap the benefits of technology while mitigating the risks. The sector will rely on the cyber innovation community to help it embrace change in a secure way that maintains people's trust. ■

Taking the bait – Phishing can bite back and leave its mark

Author: Raj Meghani



Phishing is the malicious act of attempting to acquire sensitive and personal information such as usernames, passwords and credit card details by posing as a legitimate entity through digital communications.

Spear Phishing is where an attacker uses targeted information about employees and the company to make the phishing campaign more persuasive and realistic.

BIO

Raj Meghani is the Chief Marketing Officer at BlockAPT. A leading edge UK based innovative cybersecurity business empowering organisations with an advanced, intelligent cyber defence platform. Through its unique Monitor, Manage, Automate & Respond (MMAR) framework, BlockAPT protects SME's and Large Enterprise's digital assets against cyber threats by unifying operational technologies with advanced automated solutions on one platform through a single pane of glass view. Passionate about all things cybersecurity, technology and digital transformation, Raj has over 20 years of experience helping businesses across financial services, IT and professional services with their growth and retention strategies.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

Yes, most of us are familiar with those terms. But according to Verizon's 2020 Data Breach Investigations Report, 75% of organisations globally still experienced some kind phishing attack in 2020. The numbers suddenly start to add up - people at all levels are waking up to the fact that this is indeed one of the single largest cause of data breaches and is only heading upwards in one trajectory as it gains popularity among hackers.

So why is phishing still prevalent as a major cyberattack and what are the gaps here which so many millions of innocent people are falling prey to?

I believe it's more about education and training and not just ad hoc checks or policies in place – it's about enforcing those policies in a sustainable and regular manner. That means a mindset change, transforming the way your business and its biggest asset – your people - think and act to ensure the safe protection of sensitive information and data they have access to.

With 96% of phishing attacks arriving by email, we can see that just by enabling email security and educating employees on pitfalls and what to look out for will start to reduce the number of 'repeat offenders' who are persistently clicking on spoof emails containing malicious links.

Today, hackers have moved their focus from just gaining a pure financial motive through social engineering incidents. The vast majority of motivated targeted attacks now appears to be focused on gathering more detailed intelligence.

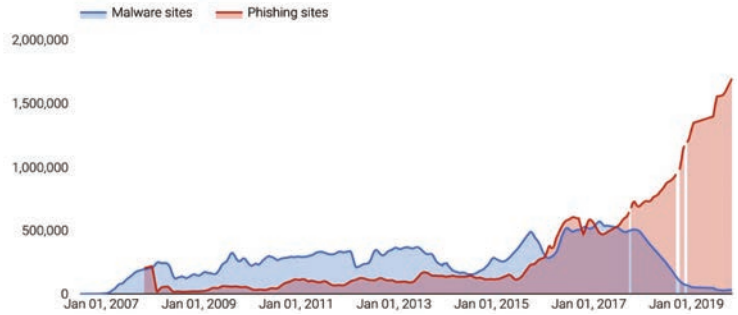
This means hackers are focused on the stealing of credentials through phishing attacks to gain access to systems, applications, accounts, etc. Whilst this doesn't diminish the impact of spear phishing as another key contagious factor, we can see the potential in terms of chaos and devastation this can cause in addition to reputational damage. The latter being further addressed by Maria Chanmugam in her thought provoking article – "Why are you risking your reputation?"

By using our own intelligence and analysis of the different types or groups of cyberattacks, their methodologies for targeted attacks, etc we can be both reactive in our actions taken and proactive about preventing future phishing attacks.

To do this, we can evaluate a vast range of data and statistical information already out there through different research studies, white papers, thought leadership forums or security experts' views, etc.

The ever increasing popularity and reliance on social media, with the necessitated fast tracking of remote working through the COVID-19 pandemic, has added to the rising number of phishing websites we see today. Social engineering attacks come in many forms, not just email. Attackers use social media, text messages and even voicemail to trick users through smishing, vishing and USB drops malicious attacks.

Google figures state as of 17 January 2021, they have seen 2,145,013 phishing sites registered. This in itself an increase of 1,690,000 from the year before.



Source: - shows the steep increase in the number of websites deemed unsafe between January 2016 and January 2021.

The impact of phishing attacks on an organisation – whether engineered through email, mobile, website or other social media platforms has a devastating impact on organisations.

Proofpoint's "2021 State of the Phish" report following a year long study is an interesting read to get a deep dive into the user's Awareness, Vulnerability and Resilience towards phishing attacks.

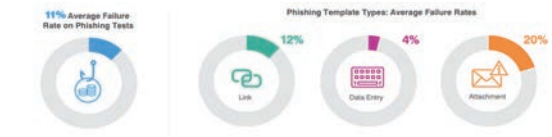
Their research involving security leaders globally revealed:

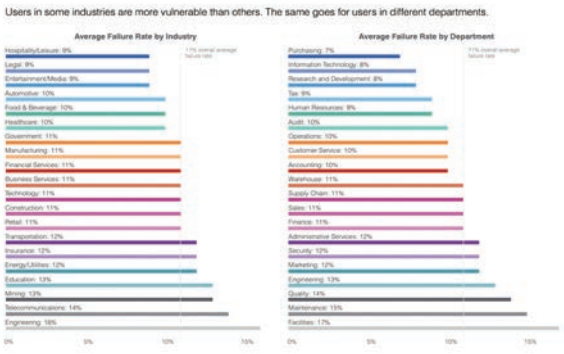
- 60% of organisations lost data
- 52% of organisations had credentials or accounts compromised
- 47% of organisations were infected with ransomware
- 29% of organisations were infected with malware
- 18% of organisations experienced financial losses

Everyone is at risk or vulnerable through some form of targeted phishing attack. But which industry sectors are top of the hackers' radar? And who is their preferred, favourite functional target to gain access to an organisation's sensitive data?

If we know which threats like phishing are growing exponentially, which industry sectors are repeatedly attacked, which departments and who within them are targeted, methodologies on how they are targeted, etc we can be better placed to put in place resilient, preventative measures to stay one step ahead.

Whether you are a small, medium or large organisation, the industry sectors most at risk appear to be Healthcare & Pharmaceuticals, Manufacturing,





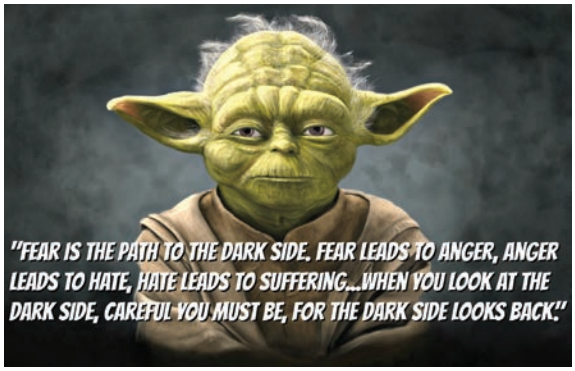
Construction, Education, Technology and Business Services respectively.

Artificial Intelligence, Threat intelligence and Behavioural Analysis is great, but we still need to mitigate these risks with stringent cybersecurity policies, security tools and technology. The company's responsibility is to provide the framework for cybersecurity, education and training. The individual's responsibility is to enforce and adhere to them. Every human has a role to play and not just those in the IT function. Key to this is education and training – not one offs but built into best practice and regularly tested.

Whilst this can pose as an overwhelming task, especially to those who are not experts in this area and believe it can't happen to them... until it invariably does..., technological advancement through automated platforms and managed security services have become more and more affordable and can take action to block against attacks like phishing, ransomware and malware on your behalf with very little if no intervention.

So the message for the rising threat of phishing is clear then. Either take the bait, get bitten and deal with the repercussions and scars. Or take simple steps to ensure your organisation has the right security ecosystem in place with people that are adequately educated and trained on how to spot and prevent phishing attacks.

As Yoda says... "When you look at the dark side, careful you must be. For the dark side looks back". ■

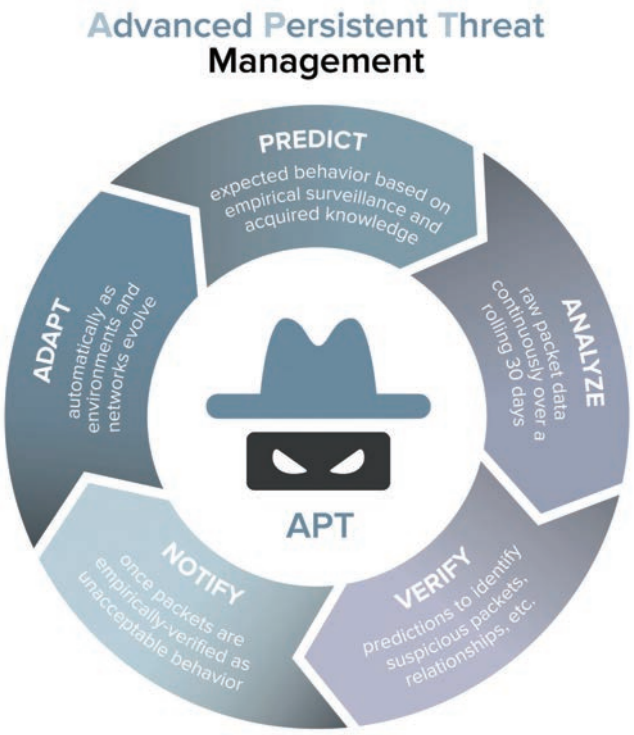


Why are Cybersecurity companies a target?

Author: Battista Cagnoni

In the last decade or so Cybersecurity has seen an exponential growth in several different ways. We have seen increased awareness about Advanced Persistent Threats (APTs) and Nation State cyber activities. We learned how Tactics, Techniques and Procedures (TTPs) initially used by extremely sophisticated threat actors have then been utilised by cyber criminals, typically less advanced but much more focused on quick monetisation. As a direct consequence, organisations started to put cyber into their equation of business risk. Something considered an annoying IT Security challenge has quickly shown its real dimension forcing organisation's boards to consider cyber threats as a primary business risk.

There is a first and big distinction that needs to be made between two different situations. Nations attacking other nations and nations attacking civilian organisations. While the first is much more an espionage type of activity, somehow tolerated since everybody tries to spy on others and typically not very visible, the latter is much more popular and hits the news every week. That's where I want to focus on and especially on the Information Technology and cybersecurity vertical.



If we look back, we have seen several very well-known situations where Information Technology and cybersecurity organisations have been targeted and compromised. It seems a very tough challenge to the most but for Nation State level attackers, it's only a matter of time and resources and even very sophisticated and mature organisations can get compromised. Beyond this superficial aspect, why has this specific type of organisation been under attack?

Back in 2011, RSA announced that they had been breached and their Secure-ID database was disclosed. Three months later, Lockheed Martin got attacked and part of the attacking methodology was leveraging authentication tokens generated from the seeds allegedly subtracted from RSA. This certainly is not an isolated case[1]: Floxif for example infected 2.2 million worldwide CCleaner customers with a backdoor. Attackers specifically targeted 18 companies and infected 40 computers to conduct espionage to gain access to Samsung, Sony, Asus, Intel, VMWare, O2, Singtel, Gauselmann, Dyn, Chunghwa and Fujitsu.

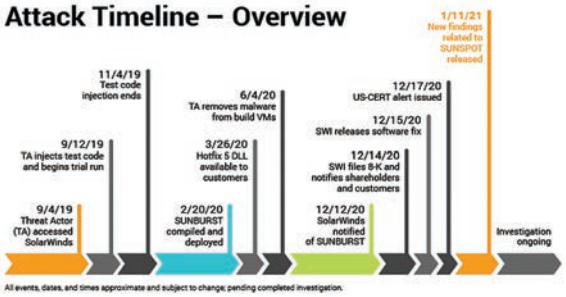
BIO

Battista is a Cyber Security Expert, CISSP GCFA GCIH. As Cyber Security professional with 20+ years of experience in different verticals, covering Security Engineer, Security Analyst and SOC manager roles, Battista is passionate about technical, social and cultural aspect associated to Cyber Threats and Incident Response methodologies..

In another attack on South Korea, hackers compromised a commercial anti-antivirus package to provide a path to breach and steal South Korean classified military data, including wartime contingency plans jointly developed by South Korea and the United States. But certainly, one of the most destructive attacks has been NotPetya leveraging the MeDoc software supply chain. A tweaked version of MeDoc was infected with a backdoor to permit the delivery of a destructive payload disguised as ransomware. This attack paralysed networks worldwide, shutting down or affecting operations of banks, companies, transportation and utilities. The cost of this attack to FedEx and Maersk was approximately $300 million each.

Fast forward to last month and how could I not mention Solarwinds, victim of a very brave and sophisticated attack that was probably destined to stay undetected for a very long time. The irony is that one of the Solarwinds customers using the compromised software was Mandiant, the company that performed thousands of major breaches investigation worldwide and exposed to the public the activity of one of China's cyber espionage units in the APT1 report back in 2011. Mandiant detected and responded promptly disclosing the breach and publishing a set of IOC associated with the Red Teaming tools that were leaked by the attackers.

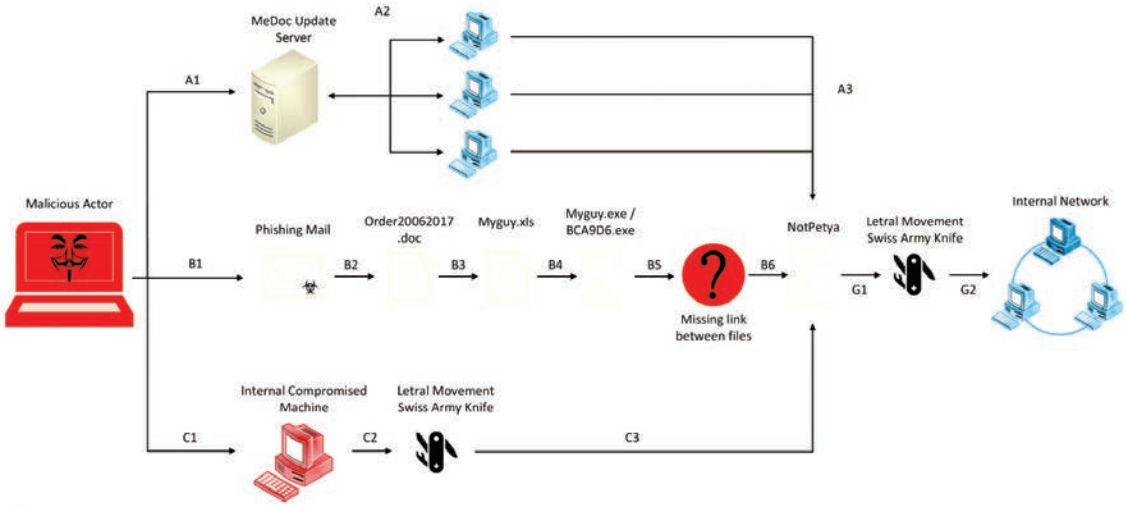
In all the cases just mentioned plus several others there are, in my opinion, two main clear reasons why the attacker targeted the supply chain compromising software and cybersecurity organisations. The first and straightforward is getting access to the final target network via the



software distribution channel, a very sneaky and clever way of getting parachuted into the target network via a backdoor. Nothing very different from the Trojan Horse. The second reason is the need for intellectual property like attacking methodologies and testing. The value those tools represent for the attackers could be the insights into which attacker techniques are used during Red Team customer engagements and then teaches those customers how to detect. The risk of the tools being made public at some point is that organisations who are not Mandiant customers might not have detection for them in place. That's why Mandiant decided to develop and release a set of IOCs, a contribution that the cybersecurity community worldwide warmly appreciated with open arms. ■

1 https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/ssca/2017-winter/NCSC_Placemat.pdf

NotPetya Intrusion Vector and Propagation



General process:
G1 – NotPetya uses lateral movement arsenal to spread.
G2 – NotPetya spreads in an internal network.

Proven method – spreading through MeDoc software update:
A1 – attacker hack update server of Ukrainian software company MeDoc. Attacker explores the server, crafts a malicious update and uploads it to server.
A2 – users worldwide pull and install the malicious update.
A3 – malicious update code downloads NotPetya.

Suggested process by Ukrainian CERT and others:
B1 – attackers sends Phishing mail containing malicious attachment.
B2 – victim opens the attachment Order 20062017.doc.
B3 – the file runs leverages RTF exploit CVE-2017-0199 to download file Myguy.xls
B4 – Myguy.xls runs script to download Myguy.exe/BCA9D6.exe
B5 – the EXE copies itself to disk using a naming randomization function and supposed to download NotPetya. This EXE is not a Ransomware.

Alternative process – spreading using compromised internal machines
C1 – attacker installs NotPetya on an accessible machine within an internal network (i.e. via Botnet or previously installed malware).
C2 – NotPetya uses lateral movement arsenal to spread.
C3 – NotPetya spreads in an internal network.

cybereason

BLOCKAPT™

Swift Response

Against attacks you least expect.

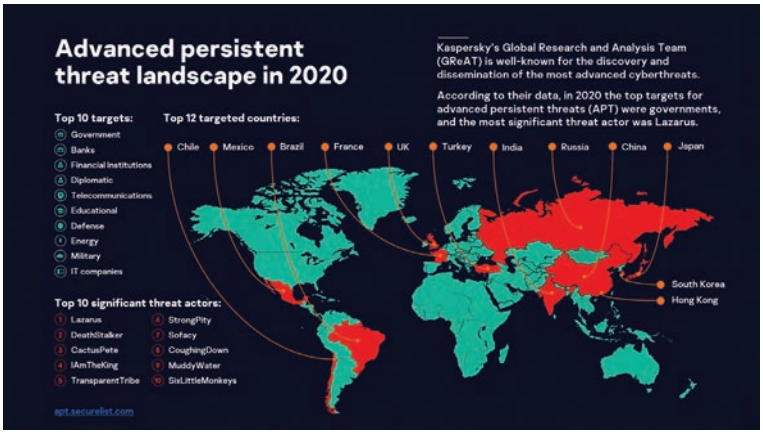
Leveraging AI to learn APT strategies

Author: Dr. Konstantinos Kyriakopoulos

APT Wars ...

Advanced Persistent Threats (APT) are cyber-attack operations executed in a series of steps following elaborate strategies similar to ones found in military operations. Recent incidents of APTs, include the breaches in SolarWinds and Fire Eye. One challenge in identifying APTs is that individual steps or phases may manifest either as benign traffic or malicious traffic targeting an organisation. Intrusion detection systems (IDSs), a mandatory line of defence in a network, may be unable to detect these attacks either due to lack of context or due to the time variation between attack stages which may span a long period of time.

Generally, APTs can be structured through a seven-stage cyber kill chain developed by the US Department of Defence and consecutively the stages comprise reconnaissance, weaponisation, delivery, exploitation, installation, command and control, and action on objectives. Alternatively, MITRE has developed the ATT&CK framework to assist network security operation centres to orientate themselves and launch potential mitigation actions or precautions to cyber threats.



Machine Learning to the rescue

There are two main categories of Machine Learning (ML) approaches; supervised and unsupervised. The former finds associations between features of input samples and an output label, usually given by a human supervisor (e.g. classifying given samples). The latter finds commonalities between features of input samples without requiring human intervention (e.g. clustering together given samples)

The research community has long depended on devising ML techniques, such as Hidden Markov Models (HMMs), to model APTs. This is achieved by : 1) collecting relevant data, e.g. alerts from an IDS like Snort, to identify alert observation transitions and 2) modelling the stages of an APT scenario based on HMM state transitions.

BIO

Dr. Konstantinos Kyriakopoulos' research focus is in advancing the current state-of-the-art of Machine Learning to address emerging challenges in cybersecurity. He has 16 years of experience in detecting network intrusions and Multi-stage Attacks, computer network performance management and cross-layer monitoring. His research focuses in Wireless, Wired and Virtual networks, developing Machine Learning and data fusion algorithms for anomaly-based Intrusion Detection Systems (IDS) and leveraging contextual information and the human factor to inform decision-making. He is currently leading the networks team within the Signal Processing and Networks group in the Wolfson School of Mechanical, Electrical and Manufacturing Engineering at Loughborough University (LU), UK. He has contributed to advancing IDSs in the defence sector by successfully engaging in licensing of research outcomes to the Industry through LU's Enterprise Office.

Challenges of modelling APT attacks

There are three main challenges in building supervised ML models for APT attacks:

1. Lack of available labelled data: There are limited labelled datasets available to leverage in order to create appropriate models for APTs. Part of the reason is that companies and organisations have their own data silo, and it is challenging to share cyber-attack data especially due to commercial sensitivity, public esteem, GDPR and privacy reasons. Perhaps, the research community along with industry could devise approaches for sharing such data and benefit all stakeholders, while preserving privacy or commercial value.

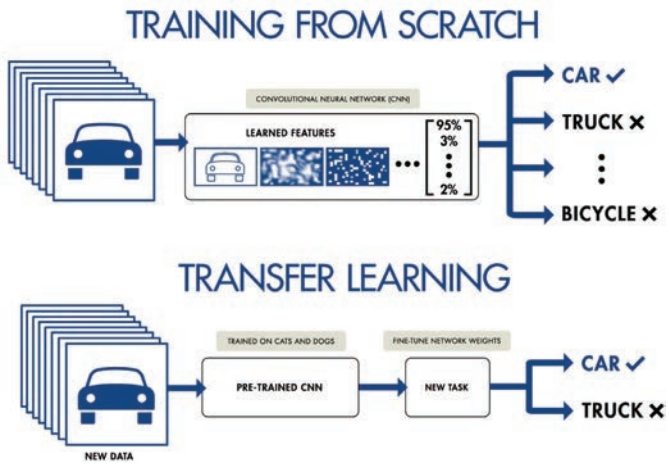
2. Model parameter optimisation: Even when successfully creating a mathematical framework to model specific APTs, say gather the alerts observations and state transitions based on HMM, parameters (notated in the figure as λ) are difficult to optimise due to the unavailability of labelled datasets. Datasets may not exist, be insufficient, outdated or require a high number of computation resources to compute the optimum parameters.

3. Adaptation of models to new environments: There is also the need for adjusting already built models (built in a source environment) to the traffic dynamics of other operational environments, which may exhibit different patterns of 'normal' background traffic. Model adaptation is also necessary to address concept drift, i.e. the phenomenon that the underlying normal traffic characteristics gradually drift with time. To compensate, ML models needs to periodically account for such changes.

What is Transfer Learning and how can it help?

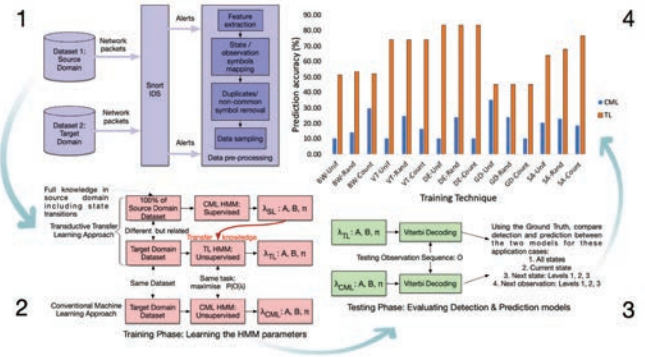
Transfer Learning (TL) is also referred to as learning to learn, life-long learning and knowledge transfer, among other terms. TL is a tool allowing models to continue learning in new domains or new tasks, leveraging prior learned knowledge.

TL addresses the above challenges by reusing prior knowledge, acquired from a source domain, and assists in the development of a model in a target domain. Source domain is the domain where we may have the full information on a specific APT. Target domain is the domain where we do not have all information, e.g. we may only have observed IDS alerts but no knowledge of the APT stage. However, if there is some commonality to the source domain, e.g. a similar attack is present, we may be able to leverage prior knowledge obtained in the source domain to identify a similar attack in the target domain (this is known as transductive TL).



Specifically, by having full knowledge of the source domain, i.e. knowledge of both the alert observations and APT states, we may generate a model that optimally represents the source domain using a supervised conventional HMM approach. Then, we may transfer this knowledge (i.e. model λ) from the source domain to the target domain, where further learning is achieved by adapting the parameters to the target domain using unsupervised HMM approaches, i.e. having only the alert observations from the network traffic and no knowledge of the APT state.

In our research team, we have conducted work on this topic and you may find more detailed information on the publicly accessible article, 'Learning to Learn Sequential Network Attacks using Hidden Markov Models', accessed through IEEE Xplore website. You may also find relevant code in the Code Ocean platform, by searching the same title.



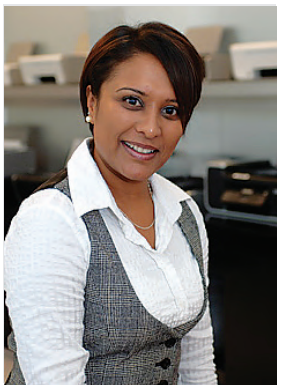
1: Methodology to collect and pre-process alerts from the source and target domains using Snort IDS.

2: Training phase: Transfer learning (TL) scheme compared to conventional machine learning (CML) approach. Note that there is full knowledge in the source domain, hence Supervised Learning (SL) CML is used. The derived model is transferred to the TL framework and then adapted to the Target domain using Unsupervised Learning (UL) approach.

3: Testing phase: The performance evaluation for both CML and TL is based on the same test sequence of observation alerts (O).

4: The results highlight the supreme improvement in predicting the next phase of an APT when deploying transfer learning (orange bar) against when using conventional approaches (blue bar). ■

Getting to know the ins and the APTs



Author: Raj Meghani

Ok, that was a bad pun I get that; but what is worse is the knowledge of the existence of cyber adversaries who are relentless in their criminal motive and continually watching, waiting and targeting their victims be it organisations, businesses or individuals.

I am talking about the stuff of nightmares that keep security professionals awake at night!

For me, having collaborated with CISO's and industry security experts, things have certainly been interesting as I've been watching daily new threats emerging on the horizon. However these last few years, there has been a significant shift from unvarying, mostly obvious and mass attacks to extremely clandestine and uber targeted approaches. Enter...

Advanced Persistent Threat (APT)

As the word "advanced" implies, an Advanced Persistent Threat (APT) attack makes use of perpetual, deep, and complex hacking methods to gain access to a system and remain inside for a prolonged period (months and years), with disruptive outcomes.
APTs simply prevail because the old ways of adversaries were accustomed to deploying a gradual increase in the refinement of attacks in a linear

progression way of advancement as opposed to exponential attack methodology. Therefore, the advantage of an organisation being able to better evolve and prepare against a threat's sophistication no longer applies when dealing with APTs.

Look, this is not to say do not focus on the basics of your cybersecurity organisational blueprint first. If businesses do not have their core security programmes in place, they will still see the breaches across their data and intellectual property. The emphasis comes after the security has been put in place as most stop here and move to focus on putting out new fires.

For example, top marks to organisations that implemented robust endpoint security at the right time and recognising these are a weak link. But in today's cyber landscape, that is simply not enough. A realisation to the course-correction method of operation is simply not scalable and a whole new perspective is needed to combat APTs.

Throwback to World Cup 2014, where Germany scored 7 goals against Brazil. Germany was relentless in scoring (even after a big lead gap) and Brazil could have had everyone playing in defence but the opponents would have likely scored. And that is the APT conundrum when it is not understood properly.

For organisations, it's the need to forget about possible perceived threats and instead accept that compromise is inevitable and work with this in mind.

The slow burn effect of APT

Another key realisation should be that APTs are necessarily only aimed towards Government infrastructures and organisations. Commercial and private large organisations should very well be prepared for APT based targeting. Vulnerabilities are still a weak point that is exploited to gain entry but unlike the traditional hackers, the motive is not quick just a quick financial gain. Data will more be intelligently sought and gathered in most cases.

Once the attacker gains an entry point, they remain stealthy on the organisation's network, device or application, extracting valuable information and trying to remain undetected as long as possible. It's a game of hide and seek with dangerous repercussions. The return on investment on such a covert attack is very fruitful and frankly a nightmare from an organisational point of view.

In the case of APT, the organisation is simply not seeing the damage real time. The attacker once embedded will evolve with the organisation. Their mode of operation:

- Gain entry - onto the network using vulnerabilities such as malware injections
- Establish a foothold - use backdoors and tunnels with malicious codes to go in and out when desired
- Embed themselves deeper - exploit passwords to get admininstration access for deeper controls to systems, applications and accounts.
- Move laterally - jump across servers and networks to spread thin and expand the reach
- Listen, watch and stay out of sight - understand security protocols, prepare counter-measures and work towards goals (for as long as possible) until they decide to come out of hiding and carry out a full blown attack.

Have you heard about Deep Panda?

An APT attack against the US Government's Office of Personnel Management, probably originating from China. A prominent attack in 2015 was code-named Deep Panda and compromised over 4 million US personnel records, which may have included details about secret service staff.

Protective measures

Since APTs are like Medusa's head with many snakes with many heads which can cripple at a single point, defences too should be deeply layered including (but not limited to):

- User and entity behaviour analysis to locate and identify stages of an attack
- Advanced endpoint detection and response to react to any endpoint compromises
- Deeply evolved email filtering to stop phishing and malicious link attempts
- Strong access control measures deeply routed with Zero Trust Principles in mind

In the end, it is important to understand that APT means the target will always be on the cross-hairs of their attackers. The best line of defence is proactively understanding threats, adversaries and minimising the impact surface to be as small as possible.

Sometimes, it is as simple as being cautious about what teams are revealing on social media platforms or the website. But it is also being mindful of all avenues of potential risk exposure and mitigating them in advance.
I will end my article in a darker tone than my beginning.
Late at night, you receive a text. Out of curiosity you look at your phone and notice it is an unknown number. You read the text and it goes -

"Hi, I am following you... BUT not on Twitter"

APT is more than just serious. Stop. Think. Act. And act again. ■

The song of the black swan

Author: Nicola Sotira

These days we are witnessing the show of the container ship "Ever Given" which with its bulk is obstructing the Suez Canal, a fundamental channel for the trade and transport of raw materials. Although it may seem trivial, we must know that about 12% of the world market passes through this channel; if we then analyse the numbers on the Italian market, we will see that it affects about 40% of our market. The canal represents a crucial junction from Asia toward Europe where about 30% of the containers transit, which translated into the number of ships is about 19,000. The impact worldwide is heavy, and it is estimated to be around $9.6 billion per day. A sandstorm, we could say, with global effects. In this new year, many of us have read and learned through the media and from the tweets of the founder of OVH, Octave Klaba. The announcement of the disastrous fire in the Strasbourg datacenter caused a rude awakening to all those who thought that the data in the Cloud is safe and always available, in a sort of digital eternity. So many small companies have seen their data go to ashes. Still, companies operating in the security and publishing sector have remained off-line, and together with them, the chess enthusiasts for the interruption of the service due to the data center's burning.

Globalisation and widespread connectivity are making supply chains more efficient and amplifying any problem's impact, not to mention the continuous drive to improve efficiency and reduce operating costs.

Being in the clouds isn't always bad

In March, Microsoft announced vulnerabilities in the Exchange Server mail and calendar suite, 10-year-old vulnerabilities exploited by Chinese hackers. The American company believes that the Chinese Hafnium group carried out the attack activities.

The news puts IT departments around the world on red alert. The goal is to apply patches and secure their servers; unfortunately, the operation takes time; the Netcraft company clearly illustrates this aspect. A few days ago, it still records that more than 90,000 servers online

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).

do not have patches installed. The vulnerabilities, when exploited, would have allowed access to the Exchange server, then allowing what is called a web shell to control the compromised server.

At the moment, there seems to be no connection with the SolarWinds case, however, one cannot help but notice that the whole thing takes place less than three months after the discovery of malicious content in the software Orion of the company SolarWinds.

A question of trust

Another attack that has severely tested our resilience is the one suffered by the SolarWinds company. This software is a network management solution with a wide range of tools in its portfolio for managing complex networks, one of which is the Orion application.

The main point that should make us think, is that the hackers managed to introduce malicious code into Orion. At the same time it was being compiled, it was injected into the program to look like legitimate code with a lot of authorisation backed by a security certificate, thus deceiving the whole chain of trust. At this point, the compiled solution looks like a legitimate SolarWinds product. Because the Orion suite is a network management tool, it requires root access to all your servers, workstations, and network devices so that it can implement the changes.

Therefore, it is evident that whoever controls the malware has full root access to every device managed by SolarWinds using Orion.

The rest is history. SolarWinds claimed that of its 300,000+ customers, approximately 18,000 entities downloaded the Orion update during March-June 2020. The malware operated stealthily by allegedly exfiltrating valuable intellectual property, confidential and proprietary data, emails, and other critical information from victims' systems.

According to FireEye, once installed on a system, the malware remained silent for about two weeks and then disguised itself as the *Orion Improvement Program* protocol, storing data of its internal activities in SolarWinds files making detection difficult. Former Secretary of State Mike Pompeo attributed, in an interview, the cyber-attack on Russia.

The grand finale

Another problem that has affected many organisations was that relating to the accident of Qualys, one of the leading companies in the provision of vulnerability management solutions using the "Software as a Service" (SaaS) model.

The data leak would be attributed to Clop ransomware; the data was posted on a Tor page and included orders, invoices, quotes, and some scan reports.

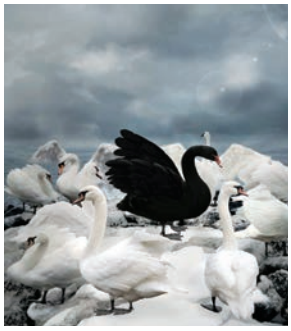
In a world that now sees software as the main actor, software supply chains, from development to production, to updates must enter the perimeter of security controls. Adversaries can inject malicious code via automatic updates, poison a network with clandestine malware via a backdoor, or use multiple ways to break into an organisation. If the infrastructure used to deliver the software or the software itself is breached, the damage is done.

At the end

In this pandemic year of closures and contagions that have also affected production capacity, all companies have realised that improving business resilience is essential. It's essential to remain competitive, to be able to maintain market confidence, and, last but not least, to support financial stability.

A vision of resilience is more oriented to critical services than oriented to individual systems and/or applications, considering the interconnections with other market players. On this issue, it is necessary to implement the concept of end-to-end, that is, to map the critical resources between people, processes, data, structures, and the internal ecosystem. It is necessary to understand and include critical third parties.

In this context, it is therefore not surprising that those "black swan" events seem almost regular today. This evidence does not automatically mean an increase in frequency, but it does highlight how, in a globally interconnected environment, problems that once remained isolated today have large-scale repercussions.



Organisations must grapple with this new challenge that they must review the concept of risk on the supply chain by including the cyber component and managing its exposure to protect the value of their business and their reputation. ■

Why are you risking your reputation?

Author: Maria Chanmugam

Risk to reputation has always existed. But it is far greater today because of our reliance on data and technology. Data is the core of the digitized economy. Just as the opportunities for innovation around it are significant the risk of an attack or breach is immense.

Today organisations are judged not simply on the quality of a product or service, but how they are led and governed, how they respond to a crisis, their financial performance, and their ethical and social commitments. Even issues that are considered very minor can affect reputation; like companies whose websites come up as being "not secure". That means simply that they do not have an SSL certificate for their websites.

A key part of safeguarding reputation is the crucial control off the ever-present threat of cyberattack on your business. This means a data breach. Just as data is increasingly valuable to businesses – especially data related to customers and payments, it is also valuable to criminals. Smaller businesses often mistakenly believe that they are too small to be a target and do not prepare. That lack of preparation creates vulnerabilities for criminals to exploit. Today it has never been easier to lose your reputation.

Why is Reputation Important?

A positive reputation is the largest intangible assets an organisation has. Irrespective of whether they are large or small it impacts on how successfully a business competes, and its ability to attract and retain customers - basically how successful it is.

What is reputation? Why should we care about it? Reputation is essentially the beliefs or opinions that are held about an organisation or an individual. Our opinions or beliefs result from:

- Expectations
- Experiences – of how an organisation has behaved
- The messages people are exposed to and the conversations they participate in or observe with colleagues, friends, and family, in mainstream or social media.

BIO

Maria Chanmugam is one of the founding directors of Clevercoms. A management consultancy specialising in the Telecoms and Technology sector. Clevercoms works with Boards, CEOs, and Management Teams as a "Transformation Catalyst" to create strategic and operational growth opportunities. Maria is a member of the Chartered Institute of Public Relations (CIPR) with Accredited Practitioner status. She works with businesses to develop and implement integrated marketing plans, increase awareness, manage reputation, and achieve their business goals. She specialises in business-to-business marketing and communication.
LinkedIn: https://www.linkedin.com/in/mariachanmugam/
Company website: https://www.clevercoms.com/

Aon's 2019 Global Risk Management Survey – a survey of thousands of risk managers across 60 countries and 33 industries – ranked reputational damage first and cyber-attacks third as risks for UK businesses. This is unsurprising as reputation is inextricably linked to how businesses manage and mitigate cyber risk. (Brexit anxiety naturally was second.)

Trust can be destroyed by a cyberattack and how an organisation responds to it. The failure to prevent a data breach is one issue; the failure to manage the aftermath effectively can create an even greater level of mistrust, which, in turn, negatively affects customer and market views and behaviour.

As more companies migrate their infrastructure to cloud-based systems, the threat of a cybersecurity incident grows. This is particularly so for SMEs. Advancements in cloud technologies and software as a service over the last few years has been a significant benefit for small businesses, enabling them to deliver sophisticated services and customer experiences that mean even a one-person business can operate on a global scale.

The cost of cyber attacks

Global cybercrime costs are forecast to grow by 15% per year over the next five years, reaching $10.5 trillion USD annually by 2025. If it were measured as a country, then cybercrime — which is predicted to inflict damages totalling $6 trillion USD globally in 2021 — would be the world's third-largest economy after the U.S. and China. (Source: Cybersecurity Ventures, 2021 REPORT: CYBERWARFARE IN THE C-SUITE)

In the UK almost half of businesses (46%) and a quarter of charities (26%) report having cybersecurity breaches or attacks in the last 12 months. 32% of these organisations were experiencing these issues at least once a week in 2020. (Source: Cyber Security Breaches Survey 2020 Department of Culture Media and Sport UK)

Lost business costs accounts for nearly 40% of the average total cost of a data breach: $1.52 million in 2020. This includes increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation. (Source IBM/ Ponemon Institute, Cost of Data a Breach Report 2020)

The impact on reputation

More than half of all cyberattacks are committed against small to medium sized businesses (SMEs), and 60 percent of them go out of business within six months of falling victim to a data breach or hack. KPMG research found that 89% of small businesses who had experienced a breach said it impacted their reputation resulting in brand damage, loss of clients and ability to win new business. Quality of service is also a risk. 96% of SMEs who had experienced a cyber breach found it impacted on their ability to operate. (Source: Cyber Streetwise and KPMG).

These staggering figures suggest that many small businesses are unprepared and unconcerned when it comes to cyber breaches; but customers are increasingly concerned about the security of their personal data. A PwC study which examined consumer sentiment around cybersecurity and privacy risk reported that 92% of consumers agree that companies must be proactive about protecting their data. 85% of consumers said that they will not do business with a company if they had concerns about their security practices. (Source: PWC Consumer Intelligence Series: Protect.me)

Quite simply reputation is an organisation's most precious asset and that applies across the board irrespective of size. This means that managing cyber security risk is critical. A proactive approach is needed to mitigate the impact that a cyber breach could have on reputation. Small businesses are putting themselves at huge risk by underestimating the enormous impact a cyberattack can have on their reputation.

Safeguarding reputation

Every organisation faces cybersecurity threats and therefore risk to reputation. Running a small business requires the ability to understand, anticipate and guard against risk. Understanding risk requires a clear view of the consequences of a cyberattack or data breach and this means education and preparation. With Cybersecurity and reputation clearly linked it is easy to put overreliance on the robustness of internal IT systems and for management to be confident in their IT teams.

It is bigger than that though. Ownership of reputation is with the Board/Senior Management who also have responsibility for managing risk. Guardianship is with PR/ communications/marketing teams. The key questions

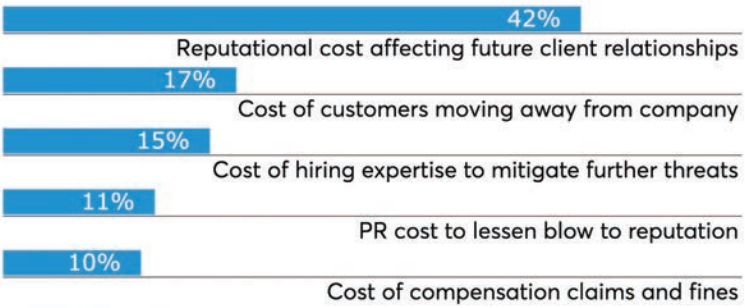
business owners need to consider when preventing or managing a data breach is, what are the relevant types of expertise needed to effectively manage cybersecurity? To adequately prepare for or manage the aftermath of a cyber breach requires expertise from those individuals who regularly manage communication and relationships and have responsibility for developing the brand and reputation.

So, what do businesses, in particular SMEs need to do?

- Reputation can not to be viewed or managed in isolation, it must be part of a continuous cycle of assessment of risks, issues, and potential crises.
- Understand that everyone in an organisation, from the board through to the delivery resource, IT, the people who answer the phones have an impact on reputation. So, cyber security training and education is essential.
- Keep in mind that you do not need a crisis to damage reputation. Carelessness, apparently unimportant actions, or inaction can impact reputation e.g. disabling a firewall or not carrying out a security update. Stolen or compromised credentials were the most expensive cause of malicious data breaches. According to IBM research one in five companies (19%) that had suffered a malicious data breach was infiltrated due to stolen or compromised credentials. Once again education is the key to prevention.
- Ensure that you have adequate security and appropriate processes in place to manage risk. Test the robustness of your systems and processes. Testing for security is vastly different to testing for working functionality and cannot just be done once. This is even more critical as people, more and more, work from home and use their own devices to access company information.
- Cyber security is not hard. It is just another business issue. Do not focus on the technology that enables attacks to happen. Think about it in operational and commercial terms. It is an investment not a cost and is an ongoing process.
- Reputation management is not about control – it is about influence. It is about how and what people think of a brand or organisation. So, we can influence how our organisation is perceived, but we cannot have full management control of the process.
- Ensure that there is a culture which respects organisational reputation.
- Have a crisis communications plan in place. Or if the worst happens, at the very least, get professional support with the communications process.
- For reputation management to work there must be effective oversight, the board must lead, with support from those with appropriate operational expertise. If you do not have full time resources, ensure that you access external support.

What'll it cost you?

The top costs of a company data breach, according to industry accountants.



Source: BlackLine

The impact of a cyber breach can be huge and long lasting. The potential for reputation damage is real and as we have seen can take many forms, from loss of brand confidence to impact on revenue and closer scrutiny from regulators. But there is also opportunity to benefit from how these events are handled, both to mitigate the immediate effect and to gain long-term insight to better respond to or even prevent future events. Securing trust is critical for firms looking to sustain long-term value in their business, products, and services.

The loss of trust and diminished reputation that cyber breaches cause can be measured directly on your bottom line. Businesses can and do recover from the consequences but only if they are prepared. A lack of proactive planning may mean that communication is at best uncoordinated and at worst delayed, and this will have an impact on trust and reputation and ultimately your bottom line. ■

Sarb Sembhi – In the spotlight

Author: Raj Meghani

RM: What made you interested in cybersecurity and how did you pursue that dream?

SS: Like many things in my life, things happened by chance because I was interested in something. I made some good decisions back with regards to coding. Basically, a developer put in some hidden fields which I spotted, and he argued saying we could store information, and nobody would know or will look at it. For me it was not right, he ***thought*** no one would use it, I ***knew*** it could be used. That was a good security decision but at the time I didn't realise the full impact of my decision.

I accidently fell into security – it was a smaller part of what I was doing until I started to look at risks in my projects. For example, CCTV cameras sat on the network, but no one was interested in them or paying much attention to the risk exposure here. Other security risks sitting on the network sparked my interest. I wanted to be an expert in a field which I found interesting, but no one was looking into. There may not have been great money to be made here, I look at things because I'm genuinely interested in them – which just happened to be things which impact security in a big or small way. I did the same thing with mobile phones security when BYOD came in, Cyber Insurance, etc. Converged security in terms of technology, risk management and instant response, Convergence has been a key theme in my time in security.

RM: What do you see as the biggest cybersecurity threats facing businesses now?

SS: Threats that are out there and will always be around because technology companies & vendors abandon updates for their technology products too soon. It's good for them as they don't have to worry about support but we need to go back to when things lasted over 10 years. Infact, I just heard about this on the radio, where previous washing machines, kitchen fridges, etc lasted a long time. But those operating systems are no longer supported so legacy systems are big threats.

People are next - we are not infallible and can fall prey unintentionally or intentionally to threats such as phishing, insider threats, etc. In the current climate and where economic conditions globally are poor, the scammers are just looking at ways to make money in their country.

Lastly, a lack of knowledge and understanding. Ignorance - where people are reluctant to accept key facts such as fake news, misinformation, etc across small and big businesses can affect them in big ways.

RM: How do you think we can plug the skills shortages and lack of diversity in this industry?

SS: There is a misconception that security requires a lot of technical background. Unless you are technical you can't get in. Some existing people

BIO

Sarb speaks, writes and contributes to global security events and publications. He was the Workstream Lead for Thought Leadership of the UK Cyber Security Council Formation Project and is the Co-Vice Chair of the Smart Buildings Working Group 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.

give that impression to protect their positions and I think that is wrong. We need to promote people who understand risk, and to, convey it in a way everyone can understand. Many of these people are not technologists but understand impacts of risk, etc. Security is a people business and it is people who use technology – not the other way around! So the skill we really need is how we communicate with people, and how they view and manage their risks.

The Cybersecurity Council Formation project through the Government Digital, Culture, Media and Sport (DCMS) department is one I've been involved in where discussions around skills have resulted in a good approach targeting younger generations before they decide, when they decide, apprenticeships, etc. The Working Group is looking at diversity and inclusion to draw in professionals from a wider range of skills – to enhance how we respond as a profession in order to be more effective.

RM: We have AI today – how do you see this evolving in the future?

SS: Many analysts have talked about where we are on the curve of adoption, magic quadrants, etc. We are with AI where we were with the internet 20 years ago. Even though there is very well developed content on

the internet, be it movie streaming to social media sites, it is being used in a very sophisticated way. However, 98% of websites today use new technologies slightly different from how they used them 20 years ago. AI is in its very early days, even 20 years from now AI will be way ahead but 98% of businesses using AI won't be using it in too different to the way in which they are using it today. There is a lag between technological development, usage by the leaders and widespread adoption. This means it is difficult to predict with confidence.

RM: You wear the hat of Co-Chair of the IOT Security Foundation, but you are also involved in some of the top UK initiatives around smart buildings/ smart cities for the future. What's the biggest challenge you see there?

SS: It's related to Manufacturers and Customers. The former by producing cheap products which are not secure and the latter who buy those products on price which are not secure. This gives vendors a bad name. If legislation could control or limit the sale of insecure devices, that would make a big difference. Online marketplaces such as Amazon, etc also need to be governed better adhere to higher standards.

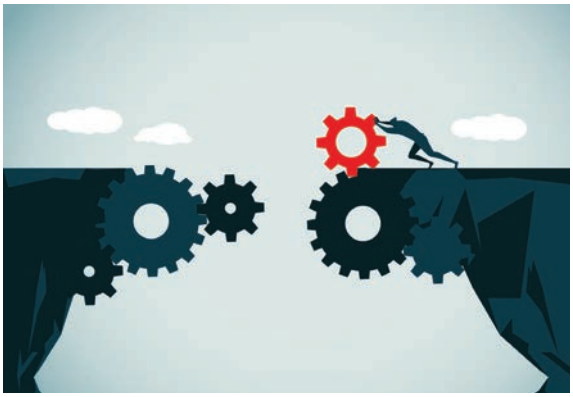
RM: What are your top 10 predictions for 2021 on the cybersecurity front?

SS: 10's too many – not sure I could come up with 10 just now…! If you look at private individuals, consumers investing in IoT for smart homes, etc it's easy to buy a cheap product online without truly understanding the risks. This increased last year with remote working and the trend will continue.

Commercially, whether you look at the vendor, installer or whoever, there's no excuse not to buy secure products or change passwords from the default set up. This is where the cyberattacks have taken advantage and are winning.

Phishing attacks are more targeted as Governments announce financial aid, etc. Opportunistic attackers taking advantage of the current economic climate.

Ransomware is another one. I was involved in an Infosec webinar just yesterday. This attack works because the attacker will infiltrate data on your machine, understand the value of the data to price it at the right level and decide how much they want you to pay. This will carry on and hurt businesses by reputational damage, etc.



Finally, there is a wide knowledge gap for businesses to understand risks and responsibilities – especially SMEs as they are the weak link in the supply chain dealing with large enterprises. Cybersecurity should be more than just a hygiene factor.

RM: What's your view on Zero Trust?

SS: Something that's developed over a period of time - acknowledgement of the old castle model of security which was wrong, then we had the de-privatisation approach which led to the onion layer which led to Zero Trust. It's an evolution where in the industry we are in, it's getting harder and harder to secure organisations and protect their assets. Approaches and concepts are very important to describe evolution better, I don't know what the next big thing is going to be called or how it will be described.

RM: What are the main security industry buzzwords which annoy you and why?

SS: I don't really have any particular gripes on any buzzwords, but I do have gripes about attitudes of the security industry. Where they use language which excludes others – using every-day terms and not just technical terminology is key to plugging that skills shortage.

There is a need for these buzzwords and terms because they describe the past and the maturity aspect but there is also a place for using them with the right people.

But at a push, I'd say the use and abuse of the term "Smart", which in consumers minds implies that it is secure, when it actually isn't.

RM: If you could pass on one piece of advice to someone looking to build their career in cybersecurity – what would it be?

SS: The cybersecurity industry is absolutely massive even though it's in its infancy but it will grow and get wider. The principles remain the same but there are more things involved than there used to be – because knowledge is moving on, technology is staying stagnant or static, etc.

It's the impact of technology and the way people react to it. I would advise there are some things which stay the same, and some things will be wildly different. You could end up in niche careers within cybersecurity roles that don't exist today. It's very exciting, especially as the people in cybersecurity are some of the most supportive and helpful people I know. But don't pretend you know more than you know and be out of your depth because that's when they'll be unforgiving. It's ok to make mistakes – we are all human.

RM: Who or what has been your biggest influence in the cybersecurity space?

SS: Those people who have stood out quietly because they've done the right things. In early days, the thinkers of de-parameterisation, people who were pioneers in their fields. Even in cyber threat intelligence, there are a couple of people I know who are extremely knowledgeable leaders. They are spending their time laying the foundations of what good is, to help the profession overall and promote cybersecurity awareness.

Some of the real heroes out there cover all aspects of cybersecurity from CISOs, publishers, journalists, event organisers, OWASP, etc – not purely because of their cybersecurity background but spreading the message in the right ways. There are too many to mention but they know who they are! ■

Security as a shared value

A conversation with Arturo Di Corinto.

Author: Massimiliano Cannata

In this interview, Arturo di Corinto addresses a particular aspect of security: that linked to the relationship between the supply chain and the complex chain of customers and suppliers that constitutes the ecosystem of reference for all companies operating in complex markets.

Security and the supply chain. Professor, how do you interpret this relationship, which is increasingly at the centre of management attention?

This is a complex issue. Managing security risk for the supply chain is crucial for companies and institutions that provide services or make products that integrate third-party components into their solutions. If this type of service is the company's core business, the importance for management is immediately apparent. However, since it is a type of risk that arises from relationships with their suppliers, both direct and indirect, its mismanagement can have consequences on both a national and international scale. This was demonstrated by the attack on the SolarWinds supply chain, which resulted in the exposure of data, information and systems worldwide, including in sensitive sectors such as the nuclear industry in the US. But the issue is also of great concern to all companies which, under the European NIS (Network and Information Security) Directive, are Essential Service Operators or Digital Service Providers.

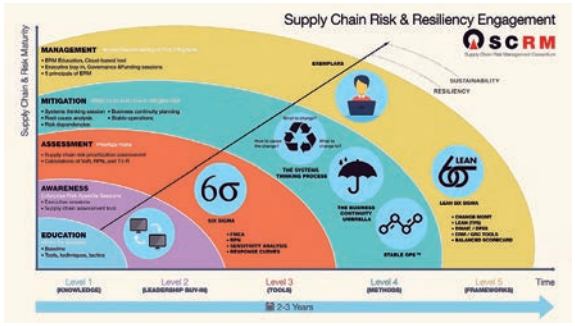
Can a chain of suppliers that is careless about business protection and data privacy become a weak point for the security of the company?

Every product and service supply relationship between companies - design, research, implementation, verification, distribution, maintenance, testing - depends on the ICT infrastructure, both for services provided to the

BIO

Arturo Di Corinto is a researcher and lecturer in cognitive and communication psychology. He is a university professor of journalism techniques, digital media and creative writing. He is currently a researcher at the Center for Cybersecurity and International Relations Studies at the University of Florence. A former lecturer at Stanford University, La Sapienza in Rome and the Academy of Fine Arts in Carrara, he was director of the Master in Public and Institutional Communication at Link Campus University in Rome. He directed the Open Source laboratory - Logos - at Sapienza University in Rome. He was Director of Communication at the National Cybersecurity Laboratory, and has served in various positions at the Presidency of the Council of Ministers as an expert in public communication, at Cnipa, now Agid, and at the Department for the Digitalization and Innovation of PA (DDI). An expert consultant and journalist, he has worked for RAI TV, EU, UN, ISFOL, CGIL, Il Sole24Ore, Wired and L'Espresso. He currently writes for Il Manifesto and La Repubblica and has published over 40 books on the digital world. Author and correspondent for the Rai Uno television programme "Codice. Tutta la vita è digitale".

end user and, more generally, for production processes. Attacking the ICT infrastructure means in fact driving the *supply chain* for illegal or criminal purposes.



What types of risks are associated with so-called 'third parties'?

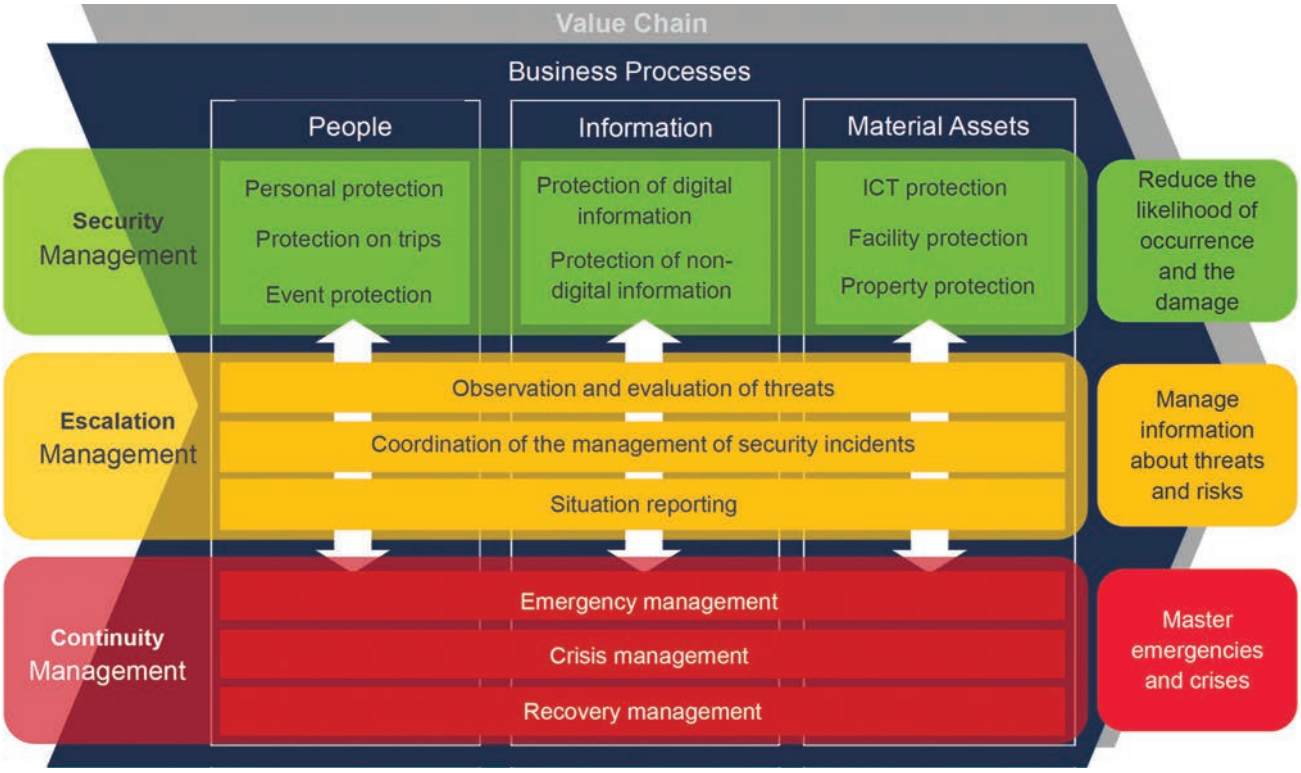
The risk is directly proportional to the complexity of the *supply chain*, the target and the operational capacity of the attackers. In order to combat the *cyber risk* associated with the supply chain, it is necessary to identify and contextualise the "attack models" (Threat model), also following an action of cyber threat intelligence. To make it clear: when we talk about *supply chain* attacks, we are talking about counterfeiting of equipment and data exfiltration, a condition that must impose a decisive increase in the level of attention together with a strengthening of monitoring tools.

What does the monitoring activity consist of?

Various protection options are mentioned in the literature and monitoring is only one of them. The ideal sequence proceeds from Identity Management to recovery actions. An organisation can be defined as resilient by its ability to implement proper 'Identity Management' through these steps: personnel are identified, their credentials authenticated, and finally they are authorised to access production and distribution resources, according to their role and tasks. Then there are the Staff Training and Awareness Programmes that serve to increase awareness and the ability to prevent and react to security incidents. Very important is the definition of security policies, i.e. the processes *and procedures* for protecting production and distribution processes *(Information Protection, Processes and Procedures)*.

Can we briefly explain why?

Because maintenance procedures depend on these, which are of enormous importance and which must be planned and controlled in accordance with *security policies*. In fact, it is necessary to apply those technical solutions necessary to protect communications between suppliers and customers in order to arrive at *Response Planning,* the response plan to actual computer incidents. Only later can monitoring intervene with an activity known as *Security Continuous Monitoring*, which takes place when the ICT infrastructure and company assets are actively monitored to detect any current or past security incidents. In the case of a successful attack, recovery activities must be carried out in a coordinated manner with internal and external stakeholders.



Shared responsibility and reputational risk

Should reputational risk be treated with the same tools that are used to protect the safety of services and products?

It must be considered that the reputational risk is always very high, but honest and transparent communication makes the difference. We all know by now that there is no such thing as zero risk in cyberspace, so the reliability of a company cannot be based on the presumptuous assumption that characterises the position of those who are convinced they will not be attacked or in denial of an incident, but rather on the ability to manage the incident correctly and to involve *stakeholders* in their role as stakeholders in the incident itself.

Enterprise Governance Risk and Compliance is a discipline that is gaining momentum. Are the standards, those relating to certification but not only, adequate to guarantee the security of the supply chain in all its development and articulation?

They are not enough, but they help. I would rather ask myself why so few realities are certified and why they are only certified in certain contexts. Here too, I hope that the new rules will bring about a profound cultural change, which is what we need most. ■

There is a particular risk in doing business with the country system you are dealing with. When dealing with organisations operating across borders, how do you define the scope of responsibilities?

Judging by the recent history of cyber attacks, companies are not all sufficiently equipped in this sensitive area. Today, with the NIS and the National Cyber Security Perimeter Act, things are changing. The *Golden Power* itself helps us to define the concept of responsibility, but error is just around the corner and the problems caused by reliance on *legacy* systems penalises companies that are less aware.

Is it your job to improve your supplier's security?

Author: Steve Stobo

We have all seen the recent press about third party attacks within our supply chains, we may feel that with all the recent attacks (and coverage) that this is a relatively new phenomenon. Maybe the hackers are looking for the "weakest link" within the ecosystems of their targets and looking to capitalise on their perceived lack of security.

But if you look at just a few of the recent attacks like **SolarWinds** and **SITA,** both those attacks happened to companies who no doubt have invested massively in cybersecurity over the years and who could never be described as the "weakest link", nonetheless they were still attacked and those attacks had a huge consequence for the companies that used their services.

BIO

Steve Stobo is Director and founder of Cyber Consultancy Services (CCS) Limited
Steve has operated in software and solution enterprise business development for 30 years with a focus on Cybersecurity for over 15 years. He has helped many global customers and SME businesses identify, quantify and remediate their cybersecurity and compliance risks, both for themselves and their 3rd party suppliers. An author of white papers, blogs, etc and a regular speaker at information security events, Steve shares a passion to help businesses reduce their risk exposure and improve their security posture.

Look at some of the other attacks such as the **Tesla, Space X, Boeing** and **Lockheed** who had data exposed by a 3rd party, **GE** who suffered a breach from what most would consider a mundane low-risk supplier with

their human resources document management system where 200,000 Personal Identifiable Information (PII) records of both previous and current employees were exposed.

Even **Microsoft**, who had an unnamed partner that handles licensing for their Azure customers got breached. The list could go on and on.....

And again, you would not consider that all of the suppliers to these companies that were attacked, would have poor cybersecurity or be in any way a risk to the businesses using their services or products.

What they did have in common was that they were all part of the company's extended ecosystem. In today's world, businesses share data, networks, infrastructure, intellectual property and many forms of information with many third parties to help improve the way they work, to reduce costs and improve the overall service they provide to their customers. However, with this connected ecosystem the risks to them increase significantly.

It's also not just the larger companies that are attacked, it is all businesses that face the onslaught from hackers. Therefore, it's all of your suppliers that are under attack and could pose a threat to your business!

But you already know this, so you will already risk assess your suppliers as part of a Third Party Risk Management (#TPRM) or Supply Chain Management (#SCM) strategy.

You could already be using a variety of tools or internal applications and systems to try and understand, and ultimately reduce your risks. Or maybe you are using static, point-in-time questionnaires or a spreadsheet-based approach. (But beware - that has no way of validating the information you have collected is accurate and will also be out of date the minute you have collected it, ultimately giving you a false sense of security.)

Either way, the problem you now have is that you have lots of information on the cybersecurity and compliance risks associated with the suppliers you assessed, but what do you do with it?

You could contact them and ask them to improve their security, but you would need to be specific about what the issues are, what they need to do, and what the expected outcome should be. It would be hard doing that internally in your own business, let alone dealing with a 3rd party supplier and expecting to get the improvement in security, reduction in your risks and the required results you want in a timely manner.

"Is it your job to improve your suppliers security?"-

Steve Stobo

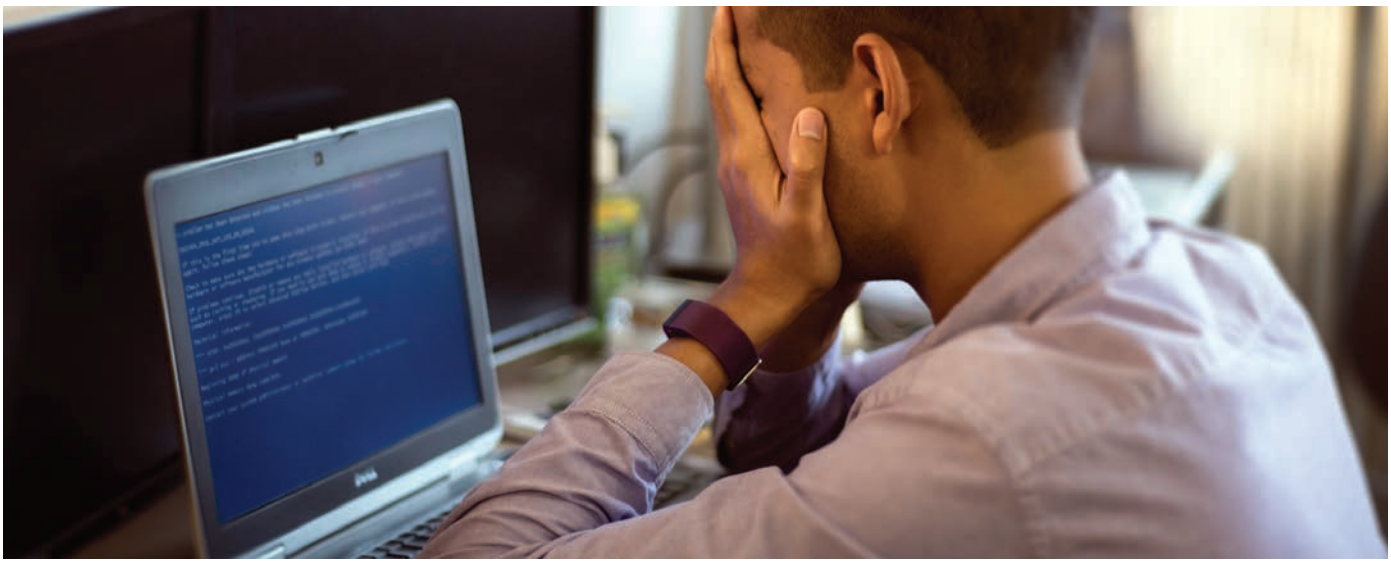
No, it should not be your responsibility to tell your supplier how to improve their security. Yes, you can point out the areas you are not happy with, the areas where the risk outweighs your risk appetite or does not meet governance or regulatory requirements, but ultimately it is up to the supplier to sort their own security out.

So whilst there are solutions and systems out there in the form of risk assessment platforms, etc, it is often hard to evaluate which one is best for you to examine the domain and infrastructure landscape of a 3rd party supplier 'passively.

Some intelligently integrate into a business' TPRM or SCM without the need for any programming or installing agents. Visibility of the technical risks, compliance risk and probable financial impact to you if they are breached is seamlessly displayed through a single dashboard.

It's the remediation feedback here which is key to mitigate against future cyberattacks and improve their security posture, improving the supplier's security and compliance, and reducing the risk they could pose to you!

If you can get your head around the fact that the buck may ultimately stop with your supplier's but it's a supply chain you are dependent on and your reputation is at stake, it's a no brainer to prevent rather than react in a crisis mode when the incident has already occurred. ■



COVID-19 has opened the "e-pandora's" box

Author: Luca Tenzi

Thanks to a worldwide panic and forecast of the "scenario of the worse", hackers can now aim for the highest targets.

Amid an acceleration in the use of digital automation over the last five years, the risk of a major cyber-event is looming. It is important to understand that the pandemic has brought forward catastrophic cyber scenarios in the mind of many experts, a cyber blackout being the next pandemic[1].

While the technical digging in how the recent hacking of the cybersecurity software has been conducted is being studied, by most if not all cybersecurity and cyberwarfare experts, the reason why hackers are now going after the cybersecurity solution is not being openly discussed. Nevertheless, attacking the cybersecurity company is a strong statement by

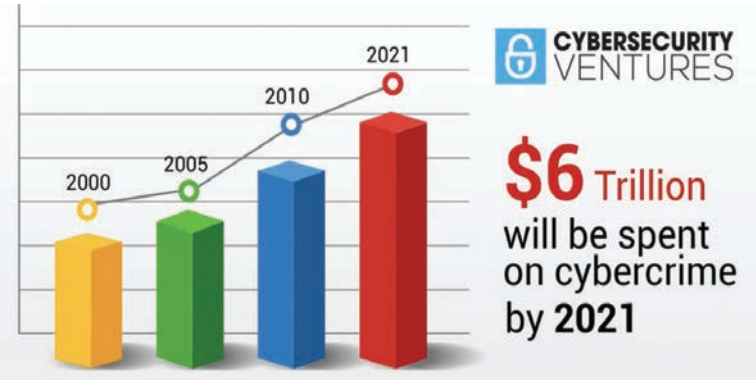
BIO

Luca is an expert in corporate security with 15 years of experience in Fortune 500 companies. He led security operations in diverse environments. His experience covers several sectors, including manufacturing, IT&C and fi nancial institutions. Luca worked and lived in Europe, Africa, the Near East and Latin America, specializing in country-level risk assessments and management in high-risk areas such as Venezuela, Iraq and Libya. Luca is an innovative strategic thinker and has a rich history of collaborations with a wide variety of business and security stakeholders around the world. Passionate team man and mentor, empathetic cultural and with diplomatic skills, has led the implementation and management of global security strategies, risk reduction programs and loss prevention. He acted as delegated security director, responsible for operations security and crisis management. Today, he's a strategic consultant at the IAEA (International Atomic Energy Agency, Un-Vienna).

the aggressor. Those cyberattacks do weaken the overall trust in the cyber world and most likely the government's abilities to defend its own presence in the cybersphere.

One must recognise that COVID-19 has been the springboard for the quantum leap onto the 4.0 society. An unprepared, and in some cases unwilling, fast forward to the ICT society that got us exposed to a cyber criminality quantum leap. Cybercriminals have taken the pandemic as the greatest opportunity of all time. The quantum leap in a more than ever connected society, substantiates the ransomware attacks roaring come back in 2020, the best opportunity ransomware groups may have ever see given the constant use of company laptops for business, pleasure, gaming, shopping, the Internet of Things (IOT) and Industrial Internet of Things (IIOT).

We know that Ransomware-as-a-Service (RaaS) is now much more common than direct attacks from specific groups. Making phishing and spam attacks much simpler and available to anyone. Ransomware attackers also commonly scan public-facing applications for known and unpatched vulnerabilities, which with the new way of doing business have multiplied. Most phishing is still done by email, with targeting techniques used to make it look like it is coming from a trusted party, a vendor, or a shopping platform.



Nevertheless, in 2020 we have seen some sophisticated attacks against the cybersecurity vendors, and this was unexpected or less expected. It is widely accepted that the next war will be a hybrid war seeing businesses and governments targeted by cyber-attacks. Cyber-attacks to respond to missile strikes[2] or missile strikes to respond to cyber-attacks[3]. We can add that bilateral and multilateral diplomacy too will be influenced by cyber-attacks. Cybersphere and next generation network influence and markets are at stake[4].

A modern Von Clausevitz would say cyberwar is the continuation of cyber-politics/diplomacy by other means. Maybe for this simple reason the cybersecurity community was quick in pointing to the usual suspects, Russia, China, Iran, North Korea with a new entry like Vietnam. Too quick, too soon, too easy? The experts indicate that the cyber traces left behind are clear indicators of the aggressor's easy way out.

One would wonder why state-actors or proxies that can pull a sophisticated attack would leave behind enough evidence to confirm the attacker's origin, in a matter of days one should add. A *"Veni, Vidi, Vici"* cyber message? We came, we did and now you know. This knowledge that hacking strings together, Chinese, North Korean or Russian imprints, are readily available on the darkweb, easily allowing copycat hacking. Recent attacks appear to develop into a free-for-all, with criminal groups taking advantage of the attack in some sort of coordination or 'follow the lead' approach.

Some indicate that we're now living in the era of the mega-hack. Where software flaws are being seized on by sophisticated hackers to compromise the computer systems of thousands of organisations, all at once. We know that AI is helping in finding those flaws. But cybersecurity software flaws don't just affect one company, it puts thousands or even tens of thousands at risk as hacking groups break into as many systems as possible before a fix is found and applied.

Attacking the heart of the cyber defences is a change in the scheme of cyberwar, it shows the fragility of modern networks and sophistication of alleged state-sponsored hackers to identify hard-to-find vulnerabilities. From cybercriminal to cyberespionage to ransomware attacks to by-pass UN or US financial sanctions are the cyber "justifications".

A fragility in a *fragilis* post-pandemic economy, gathered around a 4.0 society that would not survive if the defences should fall. ■

1 https://www.metacompliance.com/blog/the-next-global-crisis-a-cyber-security-pandemic/
2 https://eu.usatoday.com/story/tech/2020/01/07/iran-cyberattack-risk-up-missile-strike-iraq/2838442001/
3 https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/
4 Https://globalnews.ca/news/6151260/huawei-founder-canada-us-pressure/

Self-defending networks: reality or fiction?

Author: Marco Essomba

The concept of a self-defending network is not new. In the early 2000s, leading network and security vendors such as IBM and Cisco used the term to describe a network-as-a-platform. A collection of network and security devices working together as one unit to defend against cyberattacks by adapting continuously to stay one step ahead of cyber threats.

10 years ago, the technology and tools required to bring together multiple vendors to create a self-defending network was very limited. Moreover, the cost of building such as a system was prohibitive, and the market as a whole was not ready. Most security vendors had closed systems with no ability to integrate them with other third-party systems. Self-defending networking was more fiction than reality since organisations did not have a mature enough network and security ecosystem to implement it.

Things have changed. Today, the technology glue to bring different devices in a homogeneous framework is ripe, and the market is active. The advances in data analytics, Robotic Process Automation (RPA), Machine Learning, Artificial Intelligence, and Application Programming Interfaces (APIs), means that all the ingredients necessary to create self-defending networks are in place.

Self-defending networks: why does it matter?

Enterprises worldwide are facing increasing challenges to protect their digital assets against the growing number of cyber-attacks. The global skills shortage in cybersecurity is not making it easier. Cybercrime is growing exponentially amplified by the remote working triggered by the COVID-19 pandemic.

The global cost is estimated to reach $10.5 trillion annually by 2025 (Source: Cyber-warfare in the C-Suite, Cybersecurity Ventures, Nov 2020). Enterprises are continuously looking for ways to stay one step ahead of cybercriminals by ensuring that their network and security infrastructure can detect and act quickly against active cyberattacks before any damage is done. Doing this in an efficient and cost-effective manner remains a challenging task for all organisations globally.

There is no lack of technology to defend against cyberattacks. What is lacking is an integration layer that can ensure that people, processes, and technology are working better together in a synchronised manner to defeat even the most persistent and well-resourced attacker.

Of course, technology alone is not the solution to stop cyberattacks. The glue between people, technology, and processes must be in place. A self-defending network can help achieve that.

The key business objectives of a network-as-a-platform include: (1) ensuring that security practises and policies are aligned to business needs; (2) ensuring that the cost of security operations is manageable; (3) reducing complexity and simplifying the overall network and security infrastructure to maximise effectiveness; and (4) detecting and responding to cyber threats faster, ultimately improving the Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR).

Self-defending networks: what is it?

As a whole, self-defending networks comprise technology, processes and people.

From a technology point of view, the ability to manage, monitor, orchestrate, automate and respond to cyberattacks faster and in a cost-effective manner is at the centre. All the components of a self-defending network are available today - a set of tools and automation processes that provide the glue to all the network and security layers.

An effective layered defence approach also referred to as defence-in-depth ensures that all the components are working as one. Devices providing anti-virus, proxy, firewalling, VPN, endpoint detection, IDS/IPS, vulnerability assessment, patch management, SIEM, SOAR, policy compliance, routing and switching should be fully integrated.

The days of siloed technologies working independently are gone. Integration is the way forward.

In multi-vendor security infrastructures, the ability to integrate different technologies from different vendors is key. A best of breed approach adopted by many medium and large organisations means that a self-defending network must provide a communication layer between all the systems involved in a highly secure and seamless manner. The ability to manage and integrate several vendors in order to automate and orchestrate processes is also key. Ultimately, a vendor and industry agnostic approach is required to ensure that an organisation's security ecosystem is protected to meet current and future cyber threats.

It's a collaborative approach which is required – no point solution can truly achieve this goal by working on their own.

Self-defending networks: how does it work?

The core components of a self-defending network can be grouped into 5 key categories: central management, monitoring, automation, orchestration and response.

1. Central management and deep integration:

In order to enforce an organisation's policy, a central management system is required to bring all the different components into a unified ecosystem. Policies and processes should be able to be managed from a single pane of glass. A central management engine should enforce the organisation's security policy at a global level – benefitting all functions not just IT including Legal, Risk & Governance, Operations, Finance, Marketing, etc

2. Continuous monitoring:

Monitoring is key in order to ensure visibility across the entire ecosystem. With increasing and more sophisticated tools to hand, using Big Data and security analytics, events correlation can be used to give the overall self-defending network more intelligence. Anomalies should be detected faster responses to cyberattacks should be faster using known patterns, heuristics and machine learning models. The data collected overtime across the network should provide greater threat intelligence. As the self-defending network matures, it can 'learn' faster overtime by self-tuning, reducing false positives, maximising its effectiveness, and helping reduce the organisation's overall cost in security operations.

3. Automation and orchestration:

Automation can include the use of playbooks and rules which provide an abstraction layer required to formulate response plans. Using various tools and technology such as RPA, automation is allowing processes to be systematised allowing security teams to focus on critical incidents.

4. Responding faster to attacks:

The end result of any effective self-defending network is the ability to respond faster than current systems can. With all these components working together in a coherent and consistent manner, security teams should be able to reduce operational cost and reduce complexity dramatically.

If you want to be better prepared for the next generation of cyberwarfare, you will need to ensure your organisation is invested in a self-defending ecosystem. It's not a case of whether you should – it's more a question of why you already haven't? ■

“Who does not want to listen, must feel”

How deep ignorance and savage global capitalism are leading the West to a complete disaster in all fields of security.

Author: Laurent Chrzanovski

It is clear, for any open-minded global observer, the aim of attacking companies globally, including the cybersecurity ones is evident: the hackers gain control not only on data belonging to a lot of huge companies, customers of the attacked ones, but also and mostly on State data. A sort of birthday pie for the criminals.

This problem would not be ours if every single European nation did not mimic in the worst possible way the US internal and external politics and policies as far as defence is concerned.

As history has proven since 1929, the USA has an extraordinary capacity to take swift decisions and recover quickly from the worst disasters, while when facing similar catastrophes, Europe copes with their consequences for decades. Hence, according to a sad tradition inaugurated with the Great Famine of 1845, Europe will crash while the USA will mitigate the consequences at its best.

Fast forward to today and the relentless attempts to hack security companies. There are 3 main reasons for the common western failure to cope with this fast-growing trend.

1. The endless reign of King Ignorant

The first, and by far the most dangerous reason of failures has always been ignorance. Techies are techies, decision-makers are decision-makers, customers and suppliers are what they are, each with a typical niche education type having the most minimal interest in what is happening globally today.

How else could we explain that a company publishing e-books titled *"Help Protect Your Company From a Data Breach"* (SolarWinds, 2019) giving interesting lessons to its customers, was itself compromised at such an unprecedented level?

How could we understand the 8 month passivity of its CISO, of its CSO and of all their collaborators denounced by the highest US State level?: *"Known vulnerable versions of the platform were released in spring 2020 and were still vulnerable through mid-December 2020."* (SolarWinds Attack—No Easy Fix; Congressional Research Service (IN11559), January 21, 2021).

Worse, in my personal view, how could a company – specialising in supply chain management tools – branding itself for having more advanced security than any of its competitors offer us the most shameful example of disaster cybersecurity management?

As a matter of fact, SolarWinds has been the very source of the hack, performed, in addition, through the company's most popular product, Orion (its Network Management System). This "worse practice example" has been emphasised in all reports: *"what makes the SolarWinds hack so remarkable is that SolarWinds itself was the vector of compromise for its customers"* (Carina Mendola, Brett Creasy, Lessons Learned from the SolarWinds Hack: What Went Wrong & How Can Lawyers Help Mitigate the Risk of Cyberattacks, bit-x-bit report, March 2021)

Does it bring to mind the cyberwar waged between Iran and Israel last year? A last-minute ace-team action prevented Israel's water system from delivering toxic water (an overdose of chlorine) as a consequence of a hacked water plant system. As specialists in the supply chain (here network chain), Israel responded with sea & earth immobilisation of the vital Shahid Rajaee container hub, shutting down all technological infrastructures compromised by the hack.

We can all live and learn from the misfortunes that have befallen other states. But if we choose to ignore through sheer arrogance then the consequences can be devastating.

2. The planned suicide of fundamental research in the Western world

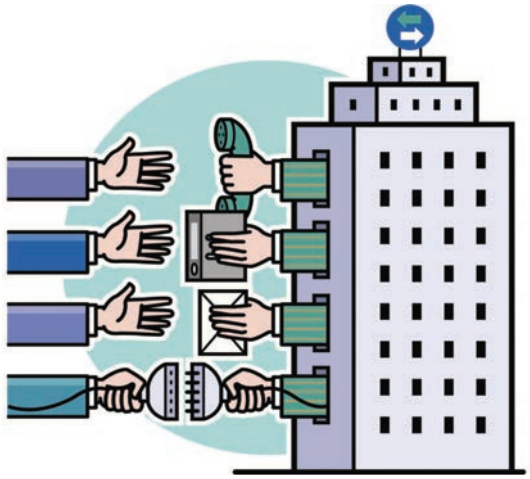
Mimicking the USA, Europe started, since the end of the cold war, to undermine the budgets of fundamental research, reaching its almost total destruction. Nevertheless, the USA is still the homeland of most of the top-20 research universities and its research agencies can still perform fundamental research at a decent level. Europe does not have a single university in the top-20. The only four *"old world"* universities of this hyper-select club being in the UK (2) and in Switzerland (2).

The consequence is that no innovative products to combat cybersecurity will truly ever be state owned, private R&D commissioned by the super power organisations still sits at odds with the State's fundamental research.

When one performs R&D, the target and the timeframe are clear and whatever does not fit into the final objective is disregarded.

In State fundamental research, if small groups gather the elements and the human skills necessary to build the final R&D phase, most of the scientists work on an open timeless field where no single discovery is ever wasted : several times, a useless invention for the army can be adapted and delivers immense potential for medical purposes, a spatial research can be converted into a new top component in transport airplanes building, etc.

When looking at this core sector for a State supremacy – the spatial one –, we realise that the same situation is valid for cybersecurity, another State top priority. There are no more comparisons to be made between Europe and countries where State fundamental research is considered as a national priority, like Israel, India, China and Russia.



BIO

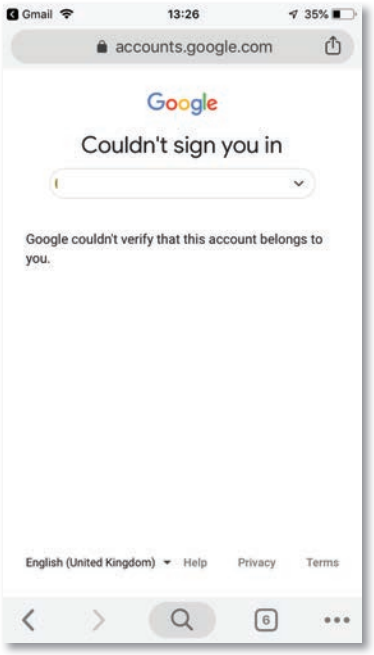
With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu 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.

3. The madness of outsourcing State data and critical infrastructure defence

Looking now into the security breaches in a historical aspect, the Solarwinds case is the last case within a very long list of critical/classified State data hacked through State contractors.

Google, Apple, Facebook, Amazon and Microsoft (GAFAM), have crystal clear programmes for nationwide education systems, e-health systems, smart cities and also... mass surveillance. In a world, whatever a State should do or plans to do, they can do it, now. The range of their activities and projects ready to be sold is so broad that, sometimes, we find the most unexpected of the GAFAM selling a new product type not belonging to their «core activity», like Amazon's next-gen facial recognition system that recently won the US Customs bid.

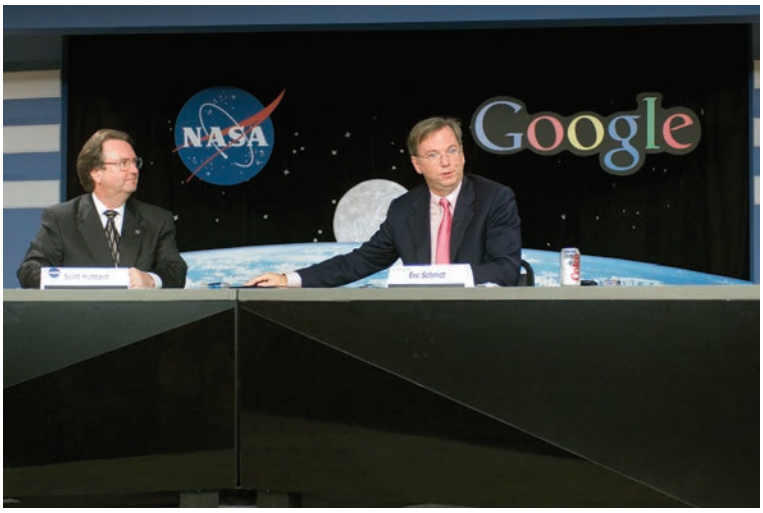
And in times of high turbulence like nowadays, the only sure survivors and winners of the COVID pandemics



times are by far the GAFAM and some niche-specific cybersecurity companies, with a reputation of excellency proven during the last years, most of them having also unsurprisingly holding huge contracts with the US government.

To explain it better through my own activities, as a University Professor, I work thanks to the taxes paid by the citizens, in the three universities of three different EU nations, I'm trying my best to give and share as much knowledge as possible to my students, even after PhD level, and to boost my institution's rank by publishing in A category journals.

In all three cases, I am now impeached for using the old intranet



system, unplugged, and am forced to use a Google account given by the respective University, where I am obliged to have all the mails exchanged with staff and students and I am kindly invited to store my research - something which I will never do.

In all the above mentioned institutions, the Google system is "secured" by the respective University IT departments – while the contract each of us signs with Google is a "standard" one, giving the tech giant the right to access all our data. As the IT departments were never designed nor trained to handle such external modules, crashes are common: in two of my three workplaces, all accounts were hacked and their whole content completely deleted. My case in point is made from my own personal experience of cyberattacks.

Yet for the Western world, the 2020 series of Cybersecurity companies compromised and the recent SolarWinds hack mark the last moment to change our thinking and actions radically. Ignorance is no longer an option. The old German saying "Who does not want to listen must feel", is now in it's second phase - with disastrous and dire consequences to follow. ■

Third Party Cyber Risks - how to manage them

Author: Lisa Ventura

Every day, without exception, many companies suffer cybersecurity attacks that can be costly and destructive. These attacks can also seriously damage their reputation, affect profits, corporate image and consumer confidence. They can result in lost customers, lost sales and reduced profits. Data protection and privacy laws require organisations to manage the security of all personal data they hold, both of their staff and their customers. If this data is deliberately or accidentally compromised, organisations may be subject to regulatory sanctions and heavy fines.

On top of all this, when we talk about vast data ecosystems, there is another, even more critical problem that many large companies face: managing privacy and cyber risks related to the information we provide to third parties and beyond. This is known as third-party cyber risk.

According to a study by the Ponemon Institute, third-party organisations accounted for 42 per cent of all data breach cases in 2020, down only slightly from 44 per cent of cases in 2008. Third-party data breaches are still the most costly form of breach due to additional consultancy fees to investigate them.

Companies often share data with service providers and their subcontractors to improve service delivery and reduce costs. In this process, data changes ownership multiple times as documentation, often containing information that directly identifies their business and customers, travels through the data ecosystem. Third parties are often custodians of the

original information, so it is critical to know what cyber security measures they are taking to safeguard this information further down the value chain.

If a third party you are dealing with were to be hacked, it could force your organisation to respond to incidents that are completely out of your control or that originate from an indirect source. Unfortunately, the knock-on effect on your organisation could be just as great as if your organisation suffered a cyber attack directly. You may not be held accountable under current data breach regulations, but your organisation could still suffer high reputational damage as a result of the incident. In addition, your customers may also be more likely to be targeted by cybercriminals looking to exploit a data breach regardless of how or where the original incident started.

Regardless of your industry, from healthcare to hospitality, you need to consider the risks of your documentation travelling through big data ecosystems. How can you manage data protection risks when a large amount of data from your organisation travels out of your control and into the hands of third parties? As the number of connected third parties

and cyber attack techniques and risk vectors increase, Third Party Risk Management (TPRM) best practices are evolving rapidly. Here are some ways you can manage third-party cyber risk within your organisation:

Classifying suppliers into specific categories according to their risk

To do this successfully, you should follow these steps:

▸ Building a framework for third-party categorisation

This should help to identify which partners require a more in-depth assessment based on their role in the organisation's activities and the size and criticality of the business relationship.

▸ Developing a workflow to examine the intersection between criticality and risk

If you work from the categorisation framework, risk managers will be able to use cybersecurity risk quantification tools to create third-party portfolios, so that cyber risk and business impact/criticality can be considered simultaneously.

▸ Establish a strict cadence for frequently addressing high-impact suppliers

This should be done through an analytical approach that combines business criticality and risk.

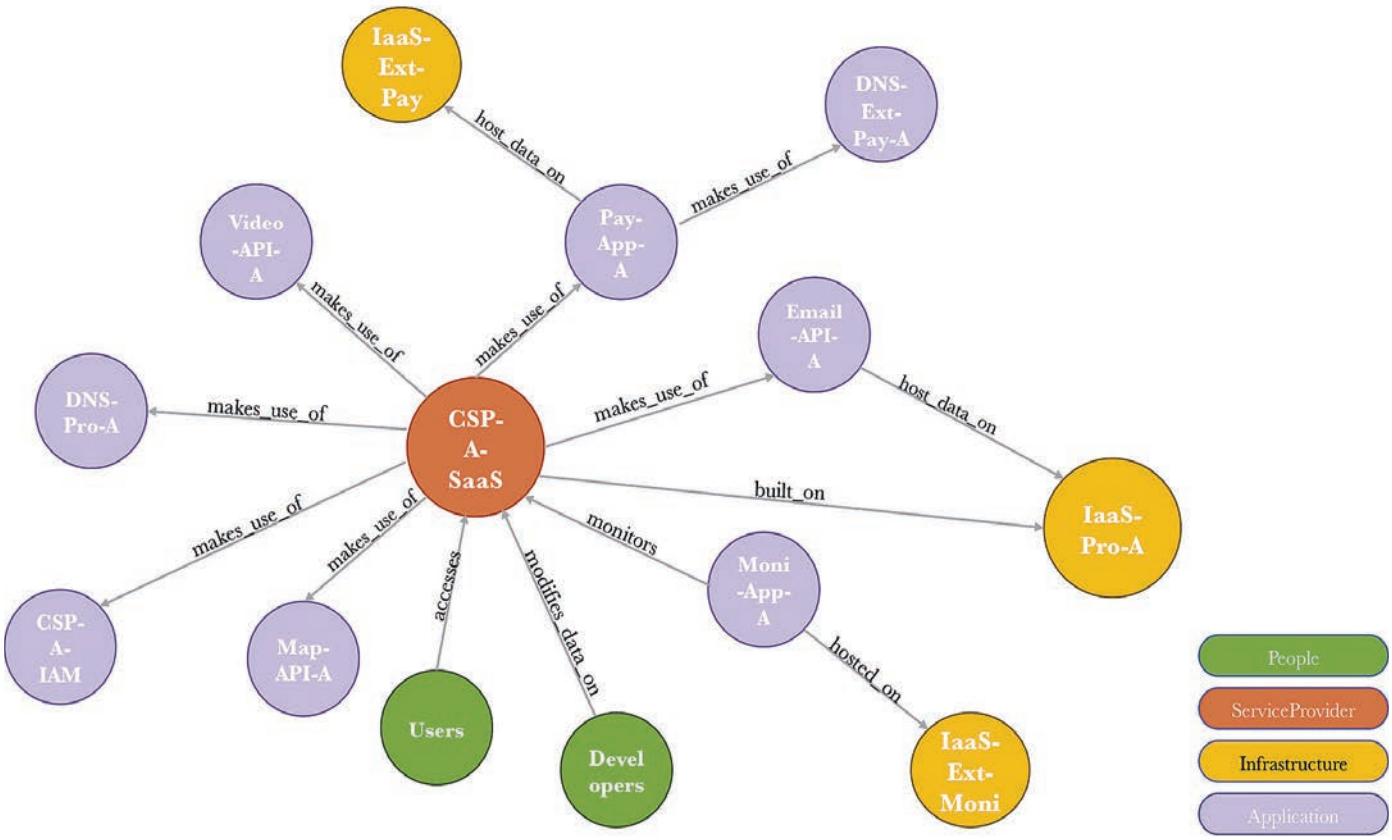
▸ Ensuring appropriate risk when transferring data

Such a simple approach takes into account the intersection of risk and supplier criticality and often requires suppliers to have insurance with supplementary protection.

Organisations can also use these four solutions for third-party risk management:

▸ Properly map the data flow

Maintaining data records throughout the lifecycle will help prioritise data governance and implement strong mechanisms to easily track or trace data between providers. Such discipline should be enforced by assigning



data ownership and accountability by implementing a control system, identifying data custodians and enforcing security policies.

▸ Assessing how third parties protect your data

Evaluate third parties based on risk attributes such as transaction volume, type of data sensitivity and regulated data and consider the impact of evolving privacy and data regulations where data is processed. Conduct assessments and evaluations of these entities and the security controls they have implemented to protect the organisation's information.

▸ Use the best industry standards and best practices

Create risk profiles through the use of third-party cybersecurity assessments. Cyber threat intelligence reports provide comparative data between third parties against industry best practices and this information could be the basis for creating risk profiles.

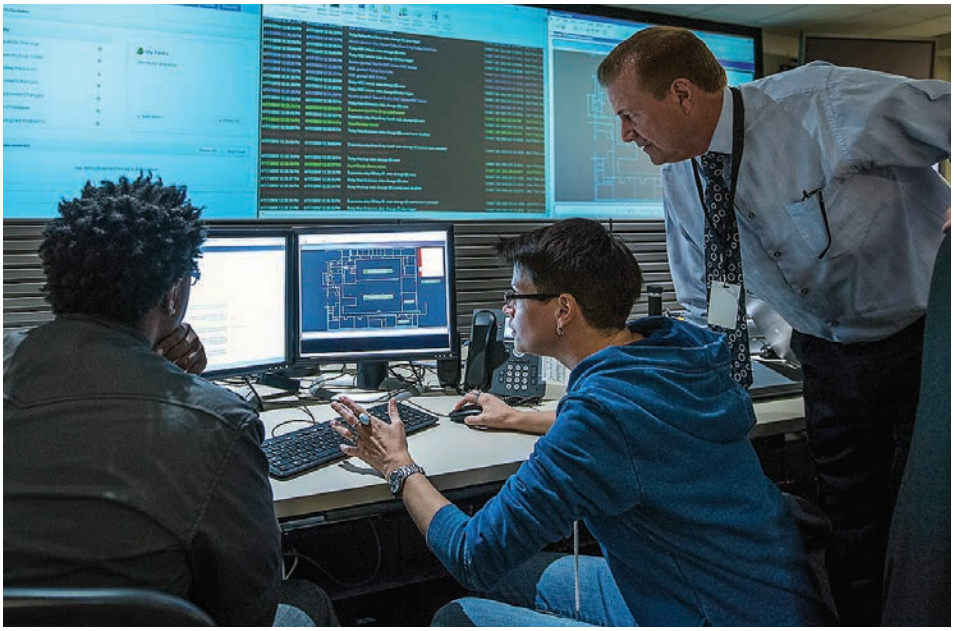
▸ Creating a playbook of computer incidents and subjecting it to stress tests

Ensure that the cyber incident response plan is consistent with other plans established to address key threats to your business operations. Components should include training all members of the organisation and conducting a threat planning test, as well as assigning responsibility for communicating with stakeholders and the media in the event of a data breach. The incident playbook should be stress-tested with realistic scenarios and include an interactive customer portal for sharing information and a specific hotline to answer questions from the public.

In the event of a data breach involving a third party, these steps will help to quickly answer fundamental questions: How is our data? Where is the data stored? Who did we sell the data to? You cannot prevent all breaches involving your customers' data, but you can provide clarity, reassurance and transparency in the event of a data breach. ■

BIO

Lisa Ventura, CEO & Founder of the UK Cyber Security Association, is an award-winning cyber security consultant, and is CEO and founder of the UK Cyber Security Association (UKCSA), an association dedicated to individuals and companies actively working in the cyber security sector in the UK. Lisa is passionate about raising awareness for cyber security, making others more cyber aware in business and helping to prevent cyber attacks and cyber fraud. She is a thought leader, a speaker at various cyber security, technology and IT conferences and events and author of various publications globally.
Lisa is on the Advisory Group for the new West Midlands Cyber Resilience Centre, the board of Think Digital Partners and Cyber Security Valley UK. She is also a strong advocate for women in cyber security, the cyber skills gap and neurodiversity. In 2020 she was named Infosec Superwoman of the Year by CISO Magazine and has won numerous other awards for her work, including SC Magazine's Outstanding Contribution to Cyber Security award.
More information about Lisa can be found at www.lisaventura.com.
Contact details:
@cybergeekgirl and @ukcybersecassoc
https://www.linkedin.com/in/lisasventura/
https://www.facebook.com/lisaventurauk/



Cyber Incidents – are you prepared for disruption?

Author: Raj Meghani

Let's face it – no one wants to be the victim of a cyberattack and face significant disruption in business from a financial, corporate and reputational damage stance. Yet how many businesses are truly prepared for the increasing number of cyber incidents we are hearing companies of all sizes fall victim to.

Too many times I see a **reactive** mode in companies when it comes to a cyberattack or incident breach. By then, the potential damage is already done, whether it is reputational damage, data gathering for ransomware or stealing sensitive data for financial gain.

With the growing trend in both types and numbers of sophisticated cyberattacks increasing, businesses need to be better prepared to prevent these types of attacks from happening in the first place.

We hear about Business Continuity and Disaster Recovery (BCDR) and Incident Response – sometimes used interchangeably – but are there any actual differences? I like these definitions to help differentiate between the three terms:

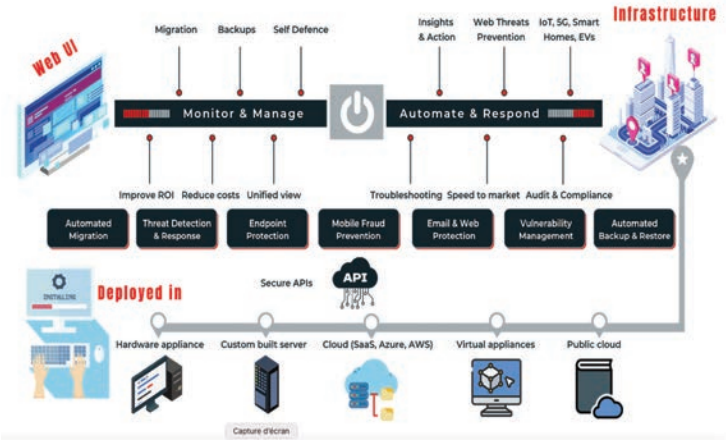
Business Continuity (BC) plans are deployed to keep the business operating whilst it can't operate the way in which it would normally do. It's more of a blanket response plan as it covers aspects of DR & IR including other processes, communication plans and continuity of operations.

Disaster Recovery (DR) plans are used after a disaster, natural or man-made. It outlines the response and recovery from the disaster. In simple terms, it's what the business needs to do to return to normal operations.

Incident Response (IR) plans are used during an incident (eg security) to detect, react, document, recover and prevent future incidents when trouble occurs – eg cyberattacks. In short, it's what businesses need to do when something unexpected and/or malicious happens.

It is the **Incident Response Blueprint (IRB)** which is the main focus here as this is heavily predisposed by information security, cybersecurity including forensic investigations.

To establish a clear plan of action and the steps required, businesses must first understand the root cause of the cyberattack across their entire infrastructure. What type of cyberattack is it? Where's it originated from and how? Who is the target? Unless the expertise is in-house with a security team, a lot of the time, finding answers to this in a quick and effective way is a challenge in itself. Add to that panic, consequences and media spotlights and it's easy to understand why having an IRB is paramount.



The ICO's position is very clear. If a data breach presents a risk to people's rights or freedoms, then it has to be reported to the ICO within 72 hours of an organisation becoming aware of it. Even if that step isn't thought necessary due to the individual circumstance of a breach, that decision has to be documented along with the facts relating to the breach itself.

So what are the key steps an organisation can take to create a cyber IRB? There is a lot of guidance out there, but the official UK NCC Group summarises this into 10 key steps.

1. Prepare to respond

- Review and rehearse cyber incident response procedures including technical and business roles and responsibilities, escalation to major incident management where necessary.
- Review recent cyber incidents and the outputs.
- Review threat intelligence for threats to the organisation, brands and the sector, as well as common patterns and newly developing risks and vulnerabilities.
- Define Threat and Risk Indicators and Alerting patterns within the organisation's Security Information and Event Management (SIEM) solution.

2. Inform employees

- Conduct regular awareness campaigns to highlight information security risks faced by employees, including:
  - Phishing attacks and malicious emails
  - Ransomware
  - Reporting a suspected cyber incident.
- Ensure regular security training is mandated for those employees managing personal, confidential or high-risk data and systems.

3. Detect and report the incident

- Monitor detection channels, both automatic and manual, customer and staff channels and social media for indications of a data breach or compromise. These can include but are not limited to:
  - Spoofed emails
  - Emails with links to external and unknown URLs
  - Emails that are non-returnable or non-deliverable
  - Notifications by internal users of suspicious emails
  - Notifications by external users of customers of suspicious activity
  - Notifications from Mimecast
  - Notifications from 3rd parties, law enforcement or ISP of suspicious activity
- Report the cyber incident via the Service Desk. If a ticket does not exist already, raise a ticket containing minimum information.
- Consider whether data loss or data breach has occurred
- Check escalation procedures and escalate as appropriate.
- Where appropriate consider reporting requirements to the Information Commissioner's Office (ICO), relevant regulator and or National Cyber Security Centre (NCSC).

4. Initial investigation of the incident

- Identify spoofed email
- Collate initial incident data including as a minimum the following:
  - Type of cyber incident
  - How was the cyber incident reported?
  - How many users have received the Phishing email?
  - What has caused the cyber incident?
  - Location of detection(s), both physical and logical
  - The number of affected assets across the organisation (initial), is this increasing?
  - Additional reporting relating to affected assets, including AV logs, system event logs, and network monitoring logs
  - Preliminary business impact
  - Any current action being undertaken

5. Incident reporting

- Report the cyber incident in accordance with the organisation's IRB.
- Where appropriate consider reporting requirements to the Information Commissioner's Office (ICO), relevant regulator and or National Cyber Security Centre (NCSC).
- Establish the requirement for a full forensic investigation - Activities may include but are not limited to:
  - Consider conducting a full forensic investigation on the advice of legal counsel.
  - All evidence handling should be done in line with the Association of Chief Police Officers (ACPO).

6. Analyse the extent of the incident

- Identify and research whether:
  - Personal data is at risk (internal or external to the organisation)
  - Other SENSITIVE data is at risk
  - Public or personal safety is affected
  - Services are affected and what they are
  - You are able to control/record and measure critical systems
  - There is any evidence of who is behind the attack
  - There is internal knowledge behind the incident
  - The act could be exploited by criminals
- Review affected infrastructure for indicators of compromise derived from the Phishing analysis to identify any additional compromised system(s).
- Examine threat intelligence feeds to determine if the Phishing attack is bespoke and targeted at specific individuals/senior stakeholders.
- Verify all infected assets are in the process of being recalled and quarantined.

7. Identify and report potentially compromised data

- Identify any data or systems that have been affected.
- Identify user credentials compromised or at risk.

- Identify IT services being impacted.
- Identify business impacts of the attack
- Identify how widespread the attack is across the organisation.
- Identify the tools used to detect the attack.
- Update senior stakeholders on any suspected or confirmed data breach including unauthorised access to personal data and/or sensitive organisational data.
- Report any suspected or confirmed data breach including any personal data breach to the appropriate parties

8. Develop a remediation plan

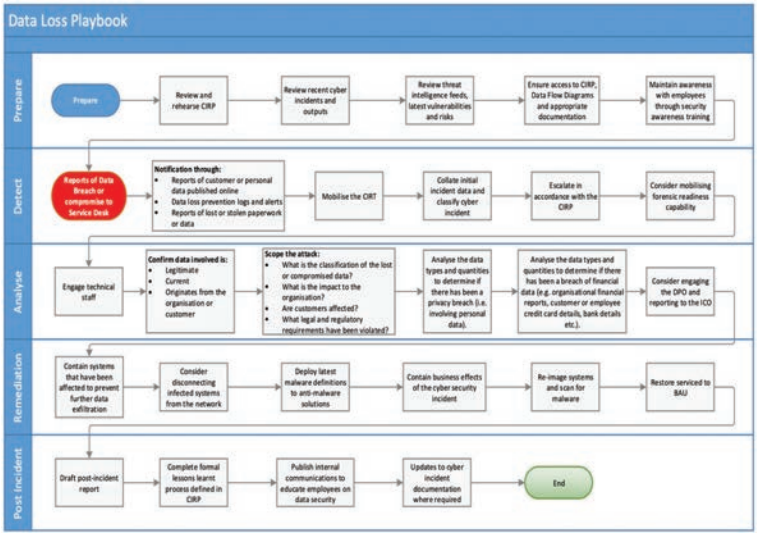
- Incorporate technical and business analysis to develop a prioritised remediation plan.
- Implement a communications strategy in line with the remediation plan.
  - Containment
  - Eradication
  - Recover to BAU

9. Incident reporting

- Draft a post-incident report that includes the following details as a minimum:
  - Details of the cyber incident identified and remediated across the network to include timings, type and location of the incident as well as the effect on users
  - Activities that were undertaken by relevant resolver groups, service providers and business stakeholders that enabled normal business operations to be resumed
  - Recommendations, where any aspects of people, process or technology could be improved across the organisation to help with, prevent a similar cyber incident from reoccurring, as part of a formalised lessons identified process.

10. Lessons Identified & Problem Management

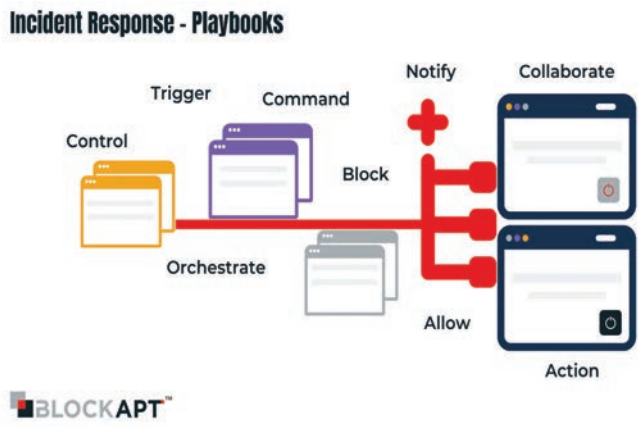
- Complete the formal lessons identified process to feedback into future preparation activities.
- Consider sharing lessons identified with the wider stakeholders
- Conduct root cause analysis to identify and remediate underlying vulnerabilities.
- Publish internal communications in line with the communications strategy to inform and educate employees on Phishing attacks and security awareness.
- Publish external communications, if appropriate, in line with the communications strategy to provide advice to customers, engage with the market, and inform the press of the cyber incident. These communications should provide key information of the cyber incident without leaving the organisation vulnerable or inciting further Phishing style attacks.



Source: Phishing playbook (Source: NCC Group – Official)

All of this can be cumbersome to manage with specialist skilled resource, time, and expertise constraints – especially compounded by the COVID-19 pandemic remote working transition.

There are cybersecurity solutions like automated playbooks or workflows with advanced AI tracking, detecting and responding to incidents in a real-time manner to help manage the businesses' IRB such as below:



"Humans are not infallible. So businesses need to invest in technology or a managed security service to support and protect their biggest asset – people – to stay steps ahead of the sophisticated cyber attackers we see today."

Raj Meghani.

The challenge is really embracing change behaviour – moving from a siloed piecemeal approach to doing things within an integrated future where predictive and preventative analysis of data feeds and response actions are truly integrated across the whole organisation outside of just the IT departments. ■

7 reasons why organisations get hacked

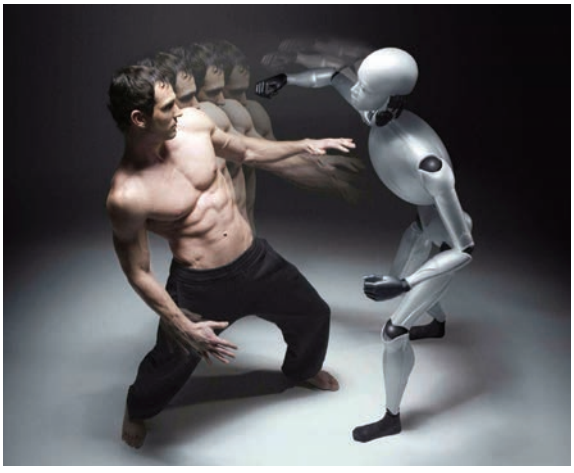
Author: Marco Essomba

As a security consultant, solutions architect and a virtual CISO helping clients globally designing and implementing security solutions to protect critical network infrastructures, I often ask myself, why do companies get hacked?

The question may seem trivial but deeply rooted in the answer is the fact that we as humans are often the weakest link in complex cybersecurity systems.

The fact of the matter is simple - it's not **IF** a company will get hacked but **WHEN**. Strong security planning and on-going reviews, audits and mitigations are the ultimate protection against cyberattacks.

I cover 7 reasons why companies get hacked (not an exhaustive list by any means) based on my experience working with clients in several sectors including banking, healthcare, insurance, oil & gas, to name but a few.



1. Humans are the weakest link

Humans are programmed to make mistakes. That's how we learn. That's how we have evolved biologically. Look at SpaceX, they made lots of mistakes and eventually mastered advanced rockets and spacecraft technologies. Even with a team of experts they still managed to crash a lot of rockets before docking successfully to the ISS.

The same applies to cybersecurity. Mistakes will be made, not if, but when. When that happens an attack window opens up. A hacker may strike within that gap. Even in the most tightly controlled networks humans make mistakes. This is inevitable so the best defence is to implement robust security measures, but also plan and prepare for fast remediation.

2. Cybersecurity technology is very strong but expertise is weak

With all the stories we hear in the news about several small and large firms being hacked a naive question may be asked as to why organisations cannot just buy the most secure and advanced solution and be done with security. Things are not that simple!

For one, security systems are designed, implemented, and managed by humans. As long as that remains the case, a flaw may always appear in the

chain. Moreover, cybersecurity technology is extremely strong and we are not short of amazing technologies.

One only has to look at firms like F5 Networks, Clearswift, Splunk, Forcepoint, and IBM - just to name a few. They are all providing advanced cybersecurity solutions that deliver end-to-end defences in many unique

ways. Yet the expertise to configure these sophisticated security products for their most optimum performance remains scarce and very niche. Hackers know about this expertise gap and are exploiting it to their advantage. I often notice a lack of ongoing security training and development of personnels which further adds to risk exposure.

3. Hackers have the edge

Hackers do what they do for fun, profit, government, espionage or political reasons. They only have to find ONE flaw in a system whereby security administrators must patch and protect against ALL flaws - whether technological or sociological. This is far from a fair fight!

With enough patience and will, even the most secure systems will be compromised by dedicated hackers with the expertise and patience.

What really matters is how fast a company can react to security flaws, patch vulnerabilities, respond, train, and continue to strengthen security measures and on-going processes against cyberattacks.

4. Cybercrime pays more

Cyber criminals are moving to the 'digital battlefield'. It makes sense since cybercrime appears to be transparent, less risky, and the chance of being caught seems remote.

I can recall the cyberattacks at several banks that exploited the Swift banking system with several millions of dollars at risk in what appeared to be the greatest cyber theft attempt ever. Online crime is seamless, it's cyber, and it's often untraceable. No wonder it is becoming more and more a safer alternative for traditional criminals to operate digitally.

5. Humans do fall asleep on the security battlefield

Due to alert-fatigue, data overload or fire-fighting; security teams can fall asleep on the 'cyber battlefield'.

When this happens hackers will seize the opportunity to strike. Unless processes are put in place to constantly monitor and audit security systems, improve solutions, learn from failures, and keep administrators and staff trained, the cybersecurity defences in any organisation will stand no chance against Advanced Persistent Threats (APTs).

6. Technology as a whole moves very fast. The pace is relentless.

With technology moving at lighting speed it is not surprising that humans can't keep up with cyberattacks. Perhaps we should let the 'machines' with AI take over cyber security administration and let them enforce security and take humans out of the equation (I am only half serious!)....

A bit extreme of course, but not unrealistic. For one, machines can follow rules flawlessly and keep up with the pace of cyberattacks as well as adapt much more quickly than humans can. They won't fall asleep on the cyber battlefield and may prove to be less 'sloppy' than humans at maintaining security standards and processes. But that is still a long way before a 'Skynet' type of authority can automatically defend organisations against hackers without any human intervention. And frankly, no one wants that. Thinking and performing logically like a machine is what I am getting at.

7. In cyberspace you only know what you know

The challenge of cyber is the ghost-like transactions that happen faster than humans can cope with. What is really happening in your network may be a mystery. But with security analytics, **knowing what you should know is good. Knowing what you don't know is even better!**

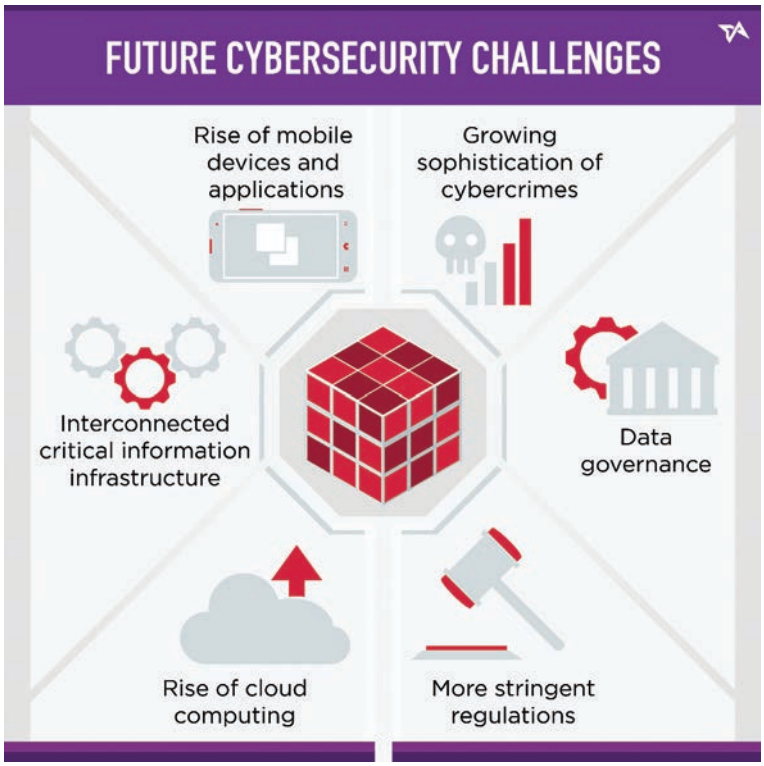
I will give you a moment to read and digest that last line again. ■

Cybersecurity Challenges for Boards

Author: Sarb Sembhi,
CISM, CTO & CISO, Virtually Informed

Businesses around the world face many challenges related to cybersecurity, not least because of the impacts of the pandemic. Business boards must remember that cybersecurity risks and challenges are like other challenges in that until the board learns more about them and begin to understand them, they will continue to seem daunting or mystical. Current cybersecurity challenges may include the following:

- **Who on the board will be responsible for cyber security?** – although many boards may have a single person responsible for cybersecurity risks, this is not true for all boards. That person would be the link for keeping the board updated on the cybersecurity strategy with the wider security team – even if it is just one person.



- **Having a single view of all security** – this is as opposed to just cyber security. The division between physical and cybersecurity has been eroded over the last few years and this trend is set to continue. Often called "Converged", "Integrated", "Holistic" or Enterprise Security Risk Management (ESRM), the approach is based on the advantages of having a single view of all aspects of security rather than to consider them as being siloed.
- **Quantifying what needs to be done and the return on investment** – although CISO's will try and help with this, it cannot be assumed that they are able to convey it in the language the board understands; nods and agreements to budgets or strategy does not equal to actual understanding.
- **Incorporating cyber into all activities** – in the same way that financial controls awareness and project management must be pervasive across the whole organisation, cybersecurity too needs to be just as pervasive. Boards need to take a strategic approach and provide security governance and how it will be implemented in project management, product development, procurement, etc.

BIO

Sarb speaks, writes and contributes to global security events and publications. He was the Workstream Lead for Thought Leadership of the UK Cyber Security Council Formation Project and is the Co-Vice Chair of the Smart Buildings Working Group 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.

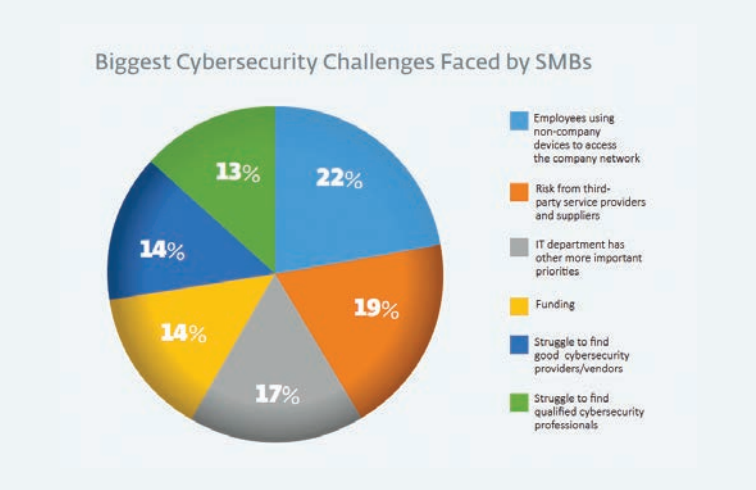
▸ **Budgets** – with new approaches to deal with the impact of the pandemic. Before the pandemic most businesses focused all their security spending on on-site / office-based controls, where a majority of solutions were geared up for such approaches. A change in thinking will require further investment to meet the new challenges of Work From Home (WFH).

▸ **Myths** – even today, there are many misunderstanding and misconceptions about cybersecurity which may appear to be a challenge because they are nothing more than a myth. Examples of this include that businesses won't get compromised if they invest in expensive solutions, or that a single layer of security controls will be enough to protect some assets.

▸ **Current threats** – the pandemic has illustrated these don't just change over months, but that they may change from week to week. Attackers and keeping up with the ones that may in particular affect their business, sector, industry, country, business model, technology, targeted ransomware or malware, etc. may be a challenging task where they don't know where they can keep up with the latest threats.

- Human Error - Response or preparation in response to the current threats – it is one thing to keep up with the latest threats and another thing to make the appropriate response.
- The interplay of IoT, Smart Homes and WFH on corporate devices and security – the lack of security in the home environment compared to the corporate office environment. The acceptance of this type of "Shadow IT" would not be accepted in the office.
- Dealing with insider threats - current external threats is one thing, but many small businesses due to the way they work and grow, have a tendency to trust all their employees with access to most systems and data. However, the fact is that insiders are able to cause much more damage to any business than most external attackers are, in most cases. The fact that most small businesses are unaware of this, may in itself make it a bigger challenge.

▸ **Cause and effect** – a recent study (https://www.canalys.com/newsroom/cybersecurity-investment-2020) has shown that despite increased spending on cybersecurity, breaches have increased. Some have said that this steady trend is due to notification responsibilities of data protection legislation. But that still doesn't explain everything, how the board interpret cause and effect within their own enterprise is important and very challenging.



There are many challenges business boards may experience depending on their background and experiences. These may even include the mistaken belief that cybersecurity is too technical for them to understand, this challenge is one of perception, or even misconception of the truth. Others similar to this include that they won't understand the risks adequately, or that even if they do, not much can be done about the risk, or they think that they don't have the necessary resources or that they won't be targeted as a business, or that they won't be targeted as directors.

Most of these are misconceptions or myths and they need to be dealt with head on by the person responsible for cybersecurity risks in the business, whether it is a director or an employee. The related challenge is that anyone with such misunderstanding may not be willing to be open about it and acknowledge it in a way to respond to it.

Challenges for businesses are not going to go away, nor are cybersecurity challenges, but the sooner some boards get to grips with how board members view cybersecurity, and its role in the realising and protecting business current and future opportunities the better. ■

Our top 10 cybersecurity predictions for 2021

Authors: **Raj Meghani & Marco Essomba**

I recall back in December 2020, when the conversation of 2021 cybersecurity outlook came up at a conversation, Raj and I could not help but smirk.

According to Raj, it seemed that with everything that has happened in 2020 (such as the Fireeye, Solarwinds breach leading to high-profile hacks), how could we really top this? Is the element of shock or surprise gone?

Nevertheless, we put our heads together, listened to our customers, partners & industry associates and deeply analysed the trends captured by our security engine to understand emerging threats.

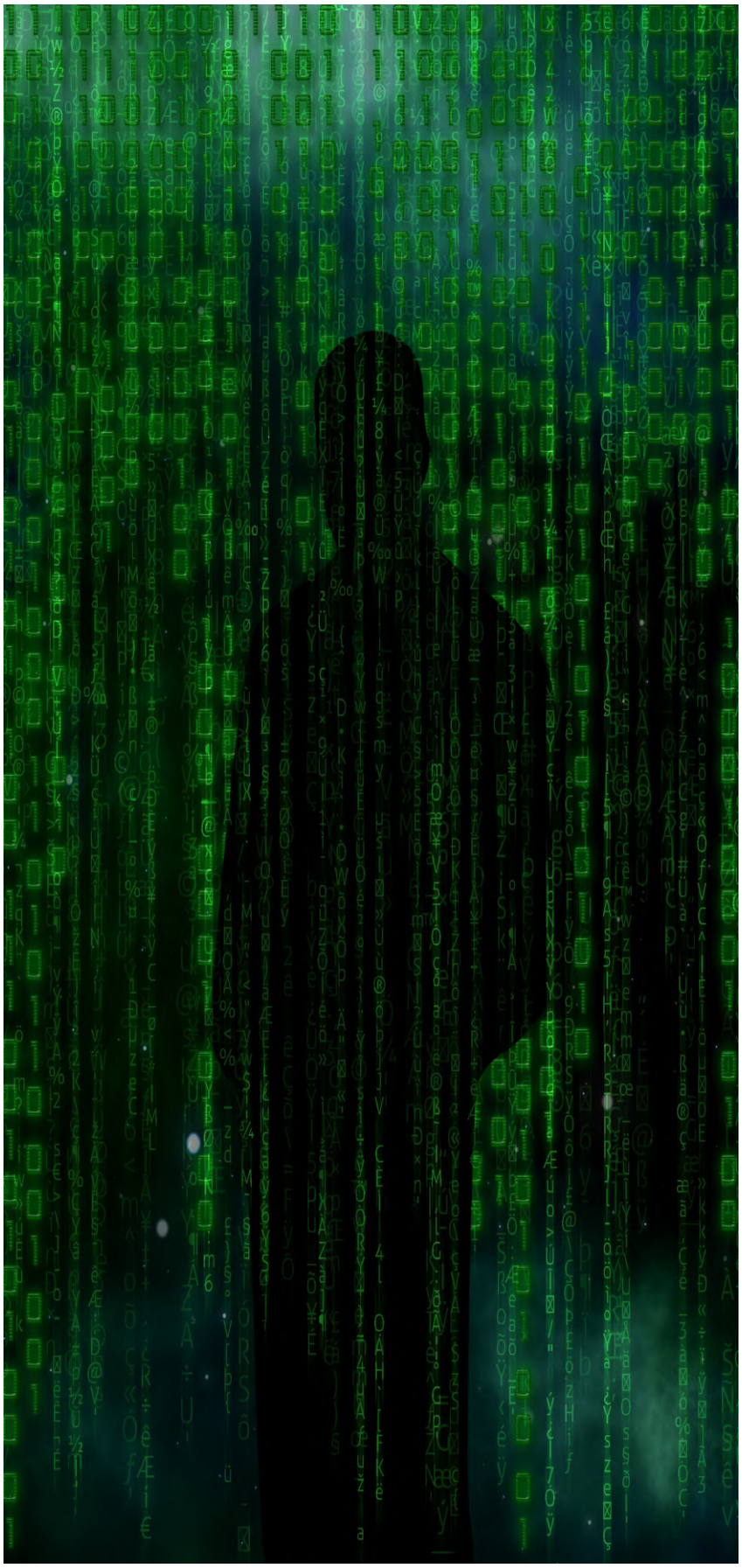
Lastly, as a bonus entry we also predict that a business will fall victim to a ransomware attack every 11 seconds in 2021. That's down from every 14 seconds in 2019! This means we could very well see the total cost of ransomware exceeding $20 billion globally.

The important takeaway from all this is that the threat landscape is accelerating at an alarming pace; so making security protection is one of your top business priorities for 2021.

Getting your business infrastructure, including security protection, does not just minimise your exposure to the rising threats and risks highlighted above but also safeguards your customers, partners and your supply chain. ■

The reality is despite the advanced state of cybersecurity trends and high profile breaches seen in 2020, we will continue to see more from the world of security and it will definitely remain a hot topic throughout 2021 and beyond. And thus, we unveil our top 10 cybersecurity predictions for 2021:

1 State-sponsored attacks and threat actors will be deemed as one of the biggest security threats in 2021
2 We will see a rise in Security Automation, particularly SOAR technology adoption across organisations as the cost of average time to identify and contain a breach rises significantly
3 EVs will be actively targeted by hackers by tampering with Smart Chargers and plug-in stations
4 As remote-working rises, attackers will swarm private VPNs and RDPs to get access to corporate data
5 We will witness more high profile attacks aimed at High-Net-Worth Individuals (HNWI)
6 Health care industry attacks will likely triple in 2021 leading to the industry moving to a more robust security strategy framework
7 Remote working will pose a bigger threat in 2021 as organisations balance flexibility and speed in being able to monitor, manage and respond to cyberattacks
8 Financial services, healthcare, critical infrastructure and legal sectors should be on top alert as their risk exposure increases with more sophisticated phishing and ransomware attacks
9 The explosion of new technology such as 5G and IoT will continue to transform and bring benefits but introduce a whole new level of additional complexities
10 Weak supply chain will become a loophole exploited by cyber attackers and pose an even bigger headache for organisations



A publication

web for business
swiss webacademy

edited by:

BLOCKAPT™

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

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

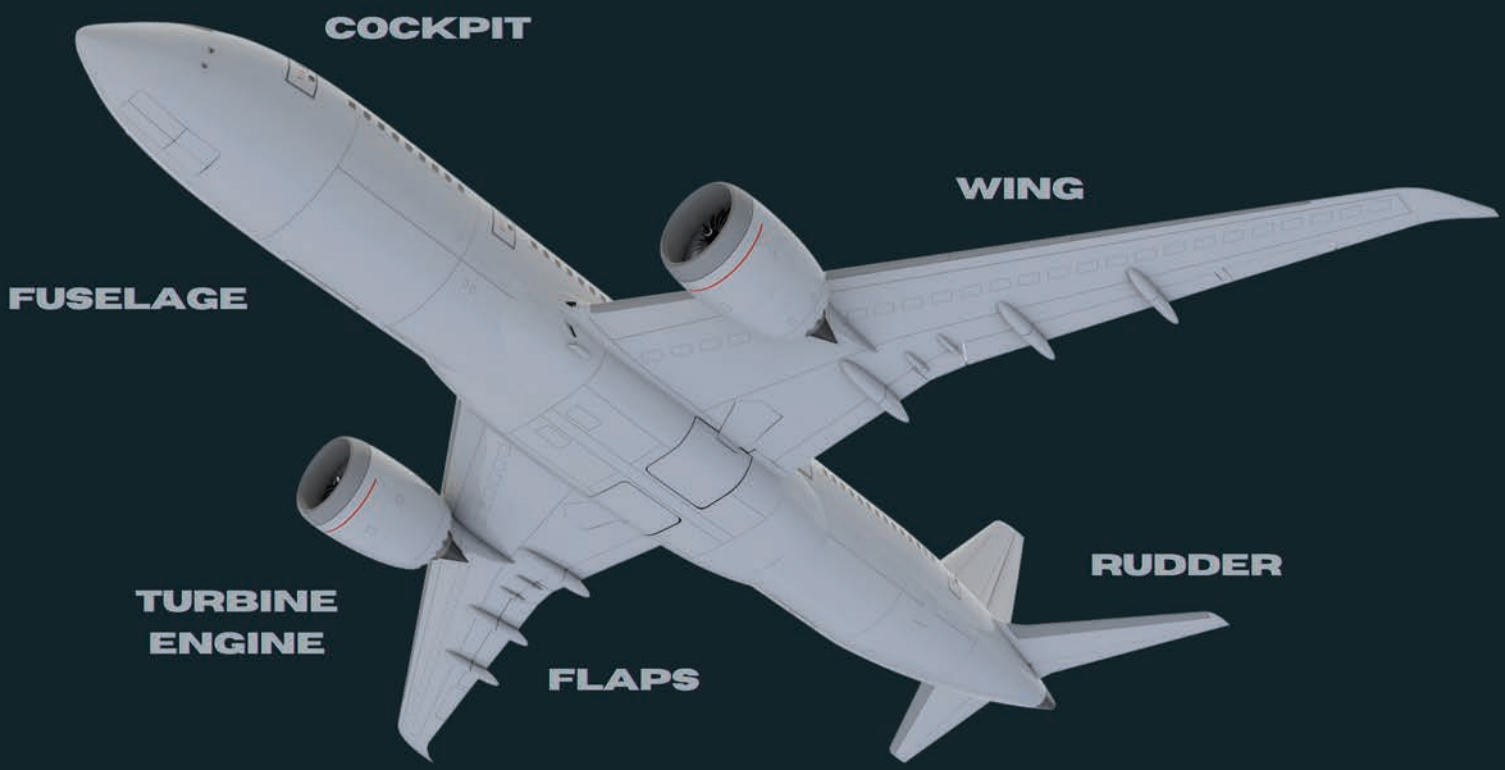
Addresses:
Swiss Webacademy - Str. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

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™

You may have the 'best in class' security, but are you really flying?



We bring together essential engineering to make your security SOAR.

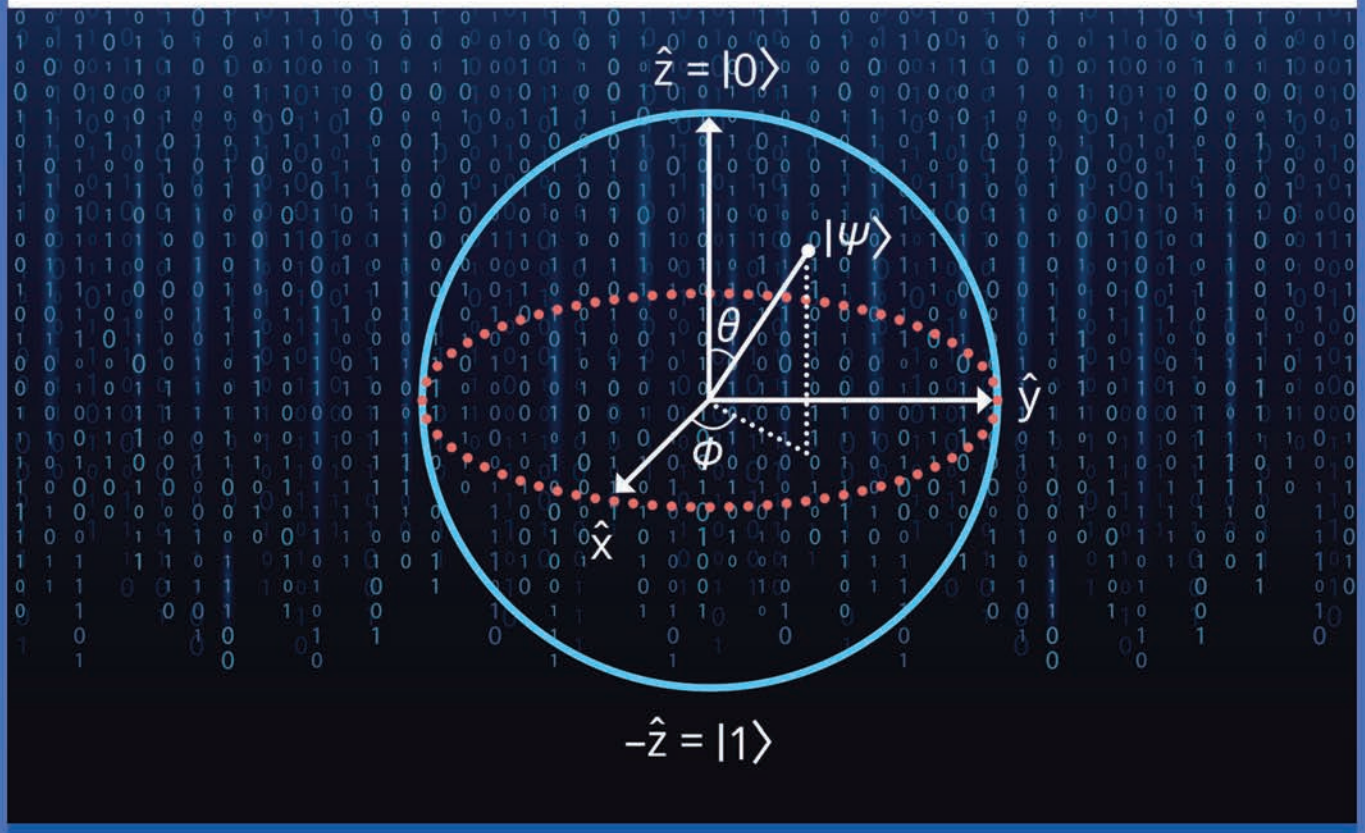
All controlled by our MMAR* technology.

Monitor - Manage - Automate - Respond*

blockapt.com

@blockapt

EUROPEAN UNION AGENCY
FOR CYBERSECURITY



POST-QUANTUM CRYPTOGRAPHY

Current state and quantum mitigation

FEBRUARY 2021

The latest book published by the European Agency for Cybersecurity is online:
https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation