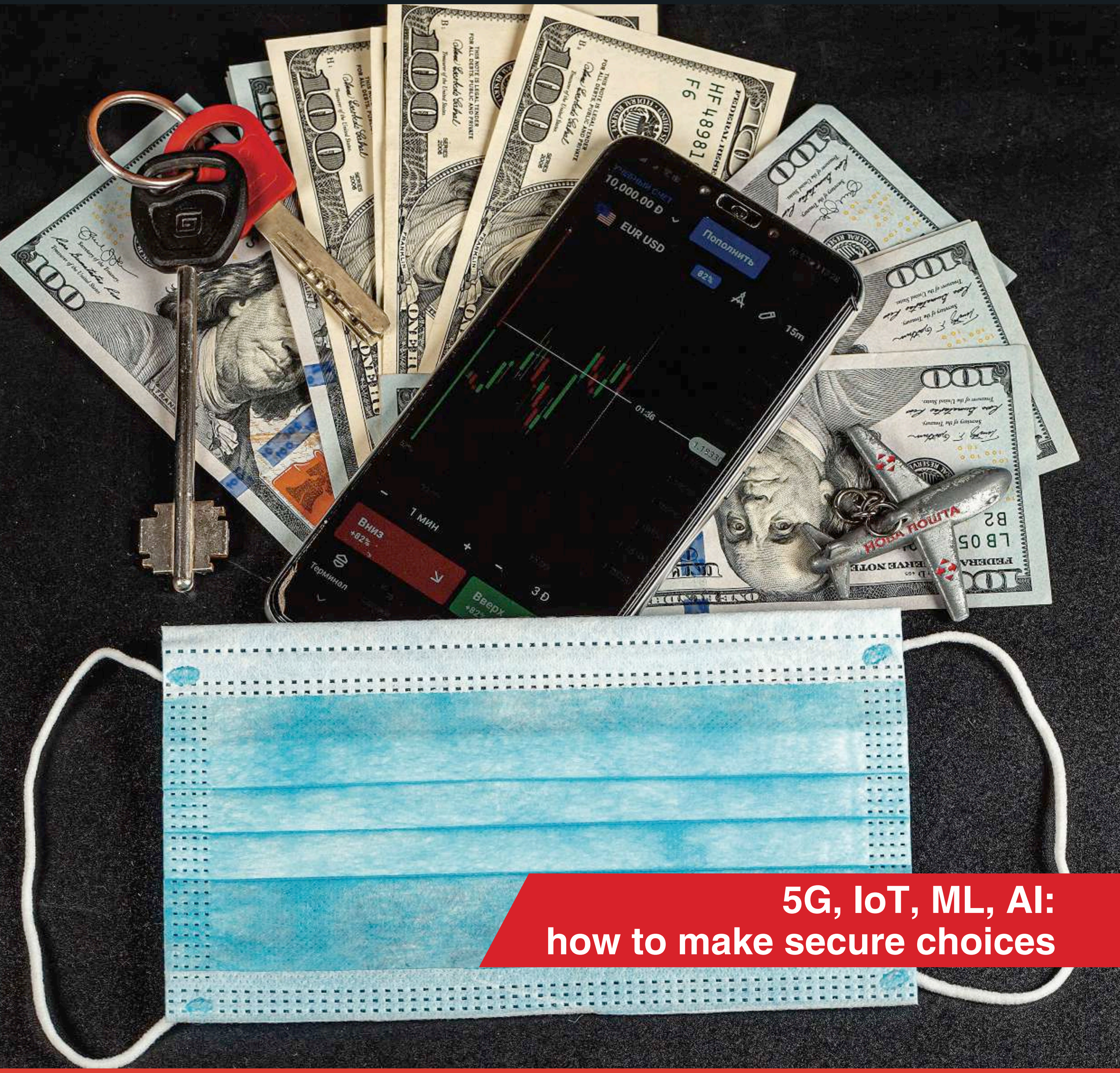
Cybersecurity Trends

UK edition n.3 / 2020



5G, IoT, ML, AI: how to make secure choices

BLOCKAPT

SMEs AND SECURITY: CHALLENGES & SOLUTIONS

Contents

Authors: Laurent Chrzanovski,
Marco Essomba, Raj Meghani

Cyber-pandemic

2020 is a turning point, with no way back, in the history of cybersecurity.

Boosted by the massive increase of homeworking, digital private and professional communications due to different lockdown stages, the final projected number of cyberattacks to December 31st will probably hit a record high. No doubt, the quantity, diversity and quality of attacks will be equal to those witnessed during the last five "conventional" years put together.

The most worrying aspect of the apocalyptic scenario we are living in today is that instead of slowing down digital innovations, the giants of the tech market have created even more of a dilemma with yet more disparate solutions for companies to "bolt on" to their existing ecosystem. Many countries, facing a tremendous fall in data speed, have implemented 5G without truly exploring the true benefits or pitfalls of doing so.

5G has made its entrance completing the 4th industrial revolution (which includes AI, ML, IoT etc.): A new digital era, where apparently nothing has changed, yet de facto everything has changed.

Entire regions and towns, previously poorly served by cable networks or 4G, were gifted with the same internet speed that was found exclusively in the most competitive areas such as the notorious business and industrial centres spread across the UK.

With uploads by far exceeding downloads due to the sheer number of connected devices, from smartphones to IoT sensors, the perimeter of defence has just exploded. All security experts urgently need to factor this into their mindset and build in adequate measures for their companies to think in the same way. There is simply… no more of a perimeter but the whole world united by an explosion in this new digital era encompassing users, customers, devices, servers, clouds, etc and the list goes on. With more than 82% of the data accessed through smartphones, the two weakest links of the security chain – the human and the smartphone – constitute a devastating explosive mixture that can be detected and detonated by hackers at any moment.

SMEs are particularly at risk. With their focus on gaining new customers, increasing revenue and maintaining profitably, just trying to survive with the impact of COVID-19 has caused its own nightmare. Focus for small businesses and entrepreneurs tend to be on product design and delivery not necessarily on how secure it is. In the last ten years, if awareness had succeeded in reaching large companies, teachers, parents and children, Government institutions, any start-up or SME founder would understand that building continuous security into their business culture is THE ONLY WARRANTY FOR BUSINESS CONTINUITY.

Moreover, the message seems to have been misplaced in communicating that security is way less expensive than many people think, and if well done it does not slow down activities but acts as a shield to prevent and safeguard their business future. Security training starts with the most basic of employee cyber hygiene education irrespective of the role or level they operate at. This training alone can preserve the company of at least half of the potential attacks, including the "banal" yet very dangerous ones like scams, phishing, spear-phishing etc.

In this edition, we focus on some crystal-clear, informative articles explaining why action is needed now. With the completion of the above mentioned revolution, digital awareness failure is another weakness we have to address urgently, if we do not want to see our environment coping with the consequences of the increasingly sophisticated and successful attacks in the next decade.

No matter how many defence technologies we have, how successfully they respond to criminals: ironically, the 4th industrial revolution, the digital sphere we live in, encompassing our physical life, sets the HUMAN firmly at the heart of all security successes and failures to come.

HUMANS must become the STRONGEST LINK. Only cultural change can make this happen, and only in this case will the historical period we live in be prosperous for the businesses of today and for the generations to come.

Let us be clear - should we fail, robots will continue to replace us. Because they will reset security in a true tech to tech war, no human failure, just the best algorithms winning: machines going head to head - AI fighting AI. Humans become superfluous in this – ergo they become the weakest link.

In this context, SMEs are the vital lymph of every single country. No nation can afford to see them closing as a result of multiple and sustained hacks, as it will be the end of our societies as they are shaped .

This new digital era needs new thinking at a cultural level – humans understand this today, machines don't. Time to raise the bar and take back control of our defences in a SMART way. ■

Small Dimensions Matter!

Author: Massimo Cappelli

Information security is a discipline for the few. Few know it, even less practise it, and only a small number of us really understand its importance.

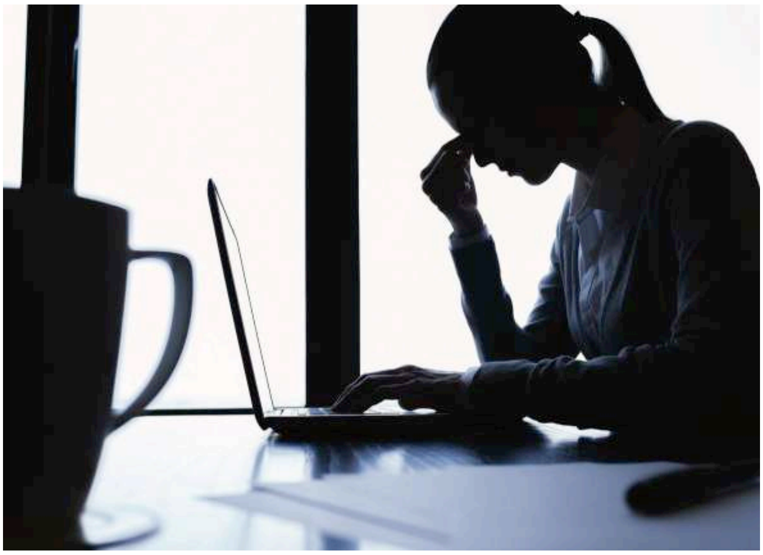
The difficulty is evident in the day-to-day activities in which insiders come across. Difficulties in getting business owners to accept security as a vital matter, while they are pressed by turnover targets and implementing new platforms quickly. Difficulties reside also in getting security accepted by product and application developers or by customer experience specialists, who are driven by the idea that the customer must easily access and use any service. Another difficulty is to make security easily understandable by all workers in the IT department itself. Not to mention the difficulty in convincing the financial officer to give the correct budget to implement a truly effective information security programme.

BIO

Massimo is the Operations Planning Manager within GCSEC (Global Cyber Security Center, Rome). He coordinates, as PMO, the research and education activities of the foundation. Since January 2017, he leads the CERT and Cyber Security of the Poste Italiane within the Information Protection Department. After his economic studies, he obtained a PhD in "Geoeconomics, Geopolitics and Geohistory of border regions" focus on Critical Infrastructure Protection Programme and a Masters in "Intelligence and Security Studies". In his previous experience, he assumed the role of Associate Expert in Risk Resilience and Assurance in Booz & Company and Booz Allen Hamilton. He also acted as consultant in several think tanks, for industrial groups as well as for the NATO.

In addition to the problematics mentioned above, there is also a great lack of adequately trained resources to work in the sector.

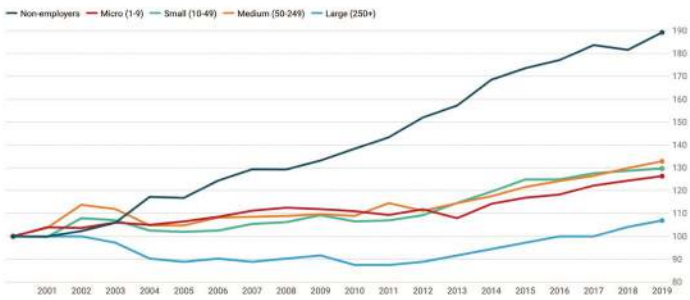
This rends the picture of a situation in which a CISO and his colleagues are fighting every day. The situation is different in small and medium-sized enterprises. The difficulties faced by entrepreneurs are greater. Small and medium-sized enterprises, especially family businesses, are even less familiar with information security. Often the systems are managed by an IT manager, or support is provided by external professionals which themselves own small companies.



The problem is twofold. The lack of expertise within the company on the one hand and the lack of budget to seriously address an information security programme on the other. Add to this the fact that the IT technicians who support such activities often lack in-depth knowledge of information security and rely on a few simple common sense rules: an antivirus, a firewall and a backup. Is that enough? Certainly not, especially if it is never updated.

Small and medium enterprises form the backbone of the UK's economy. Most of them are micro-enterprises and, above all, the management is built by a family unit. Awareness raising should be one of the cornerstones of a digital economy. Awareness raising in schools, TV, social channels, newspapers, chambers of commerce and trade associations.

Growth in UK businesses in the private sector by number of employees (2000-2019)



Source Data | Graph created by Merchant Savvy

Even the words Ransomware, Phishing, DDoS are unknown to most people. So are the words backup, VPN, encryption and multi-factor authentication. The companies that should be most concerned about this are mainly those that collaborate with large companies.

They are a major object of attention paid by attackers aiming to reach the final goal, the big company. The best example we can give took place in Great Britain, where a small to medium sized company that produced particular types of valves for military aircraft was hacked, the design of the valve was stolen and the characteristics of the valve itself could be traced back to the performance of the aircraft. The company lost the order and had to close down.

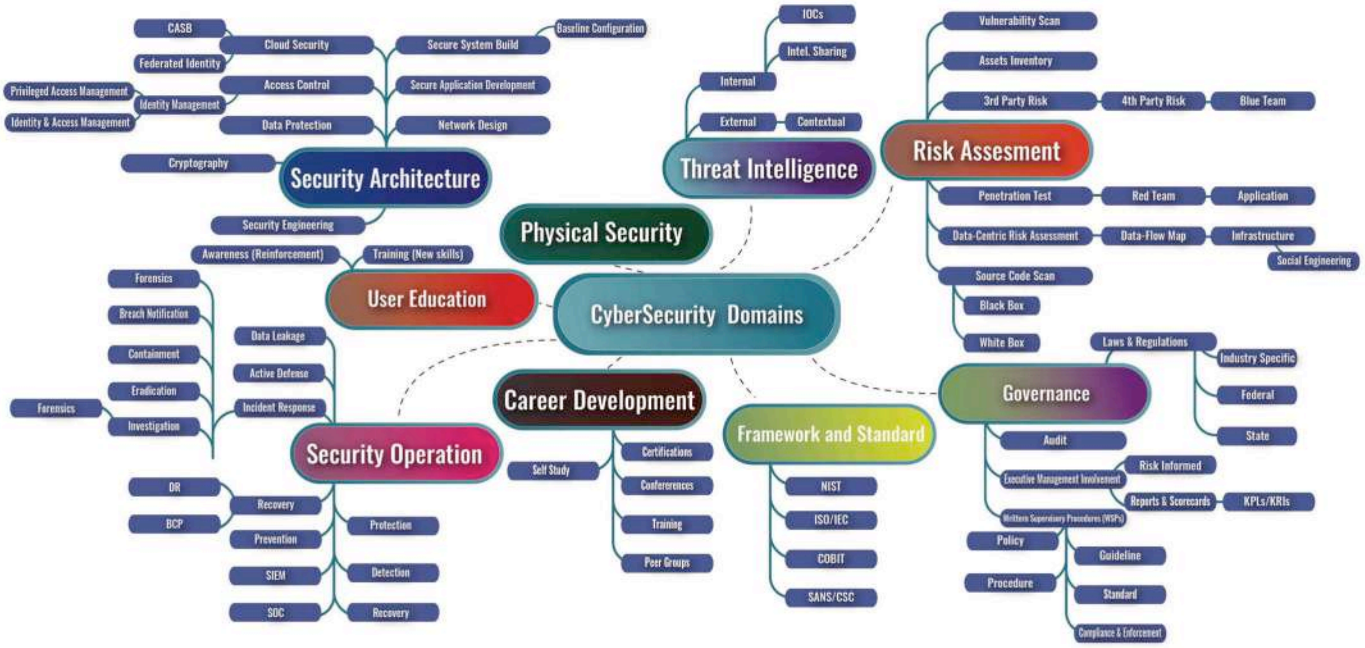
Other companies have been forced to pay ransoms to retrieve information from their servers.

Ignorance is great and the will to make up for such ignorance is little. Unfortunately, the State cannot close its eyes and, above all, cannot think that the regulations will solve everything. Regulations, certifications, directives to protect privacy, do not solve the problem. It is a subject that should be dealt with separately and more widely, at a European level. Every business is trying to cope with the lack of foresight of our governments, each with their set of rules and regulations, which are and will be bringing little in the way of global competitiveness.

We have lost the train of operating systems, of e-commerce, we have lost the train of cloud, the train of 5G and we are also losing the train of artificial intelligence. All these trains have passed and much of the old Europe has seen them running, sipping a rather snobbish tea, perhaps anchored to an idea of greatness that remained from the past centuries.

The State must commit itself. It must start a massive cyber security awareness campaign. This must be talked about in all environments. Awareness must be raised among entrepreneurs, freelancers, employees and even family members. In addition, tools should be provided to small and medium sized enterprises to make them understand the risks they run based also on their specific core business type.

▸ Is this a business where intellectual property is relevant?



SMEs: Security Bytes

- Are customers specialised in products or services that require high specialisation?
- Is it a business with a strong research and development component?
- Is it a business with a strong digital connection?
- Are the production systems computerised?
- Do commercial contracts have a service level agreement or non disclosure agreement clauses to be respected?

The entrepreneur has to ask himself a whole series of questions. The answer to them will entail a greater or lesser risk of computer compromise. Am I attractive as a target of an attack or can I still be impacted by a cyber attack? Certainly a craftsman, such as a shoemaker or a tailor would answer no to all the above questions and this is a less risky factor. The one who should be worried is the one who answers yes to even one of these following questions.

- Are we protected against information theft?
- Are we protected from an attack that could interrupt our services or production?

If you don't know then you have to start worrying.

Security experts could answer these questions but they are expensive, rare and often unavailable. An alternative solution is to rely on cloud services that often include security services.

Cloud services are also cheaper than running and maintaining a local data centre. Migrating from a local data centre to a cloud solution will certainly transfer risks to a third party that specialises in managing IT resources and has higher levels of security.

Some might argue that the biggest and most reliable clouds are in the USA, but this is a strategic issue and one of those we mentioned above in relation to lost trains. A small and medium enterprise cannot be worried if it is entrusting information to foreign companies. It has to worry about staying in the market and continuing to generate revenue.

To sum up, small and medium-sized enterprises must ask themselves questions about the type of activities they carry out. It is based on confidential intellectual property; it is subject to contracts with SLA and NDA constraints; it has a strong R&D component. If the answers are affirmative, it must assess its security status and then proceed with a return plan that may involve a change in infrastructure as well. All this requires time, resources and skills.

The State may be a support. It could provide incentives to improve safety postures through tax credits or other benefits based on the company's productive activities. It should do so because a company leaving the market implies less GDP, less taxes and more unemployment.

We keep talking about awareness raising but sadly, these remain just words in the wind. ■

Cybersecurity - a Strategic Issue for Leaders

Author: **Didier Spella**

Is cyber crime just a new buzzword?

Is cyber crime just a new way for technical solution providers to sell their equipment?

These questions may arise when talking to business or State leaders.

It is clear that we are facing a cultural paradox that can seem troubling:

On the one hand, we are constantly trying to “digitise” companies and even more so our society.

At the same time, some “priests” of this digitalisation urge us to protect ourselves.

Digitisation is often synonymous with evolution and is fastly becoming a strategic issue. However, we can already see that it often boils down to document digitisation that does not call into question the organisation as a whole and the very digital processes of a company. It also benefits from the resources that are offered, whether in terms of machines or service solutions.

Companies make very poor use of their existing IT resources. Instead of optimising them, they increase their IT resources to digitise the whole business without thinking about the very foundation of what their core business is about. And this increase in resources, often poorly controlled, only increases the number of targets and the perimeter of attack offered to cybercriminals.

BIO

A former senior officer of the French Air Force, President of Mirat Di Neride, co-Founder of the PPP congress *Charente-Maritime Cyber Security*, Didier Spella is an expert in corporate strategy and cybercrime, head of the CLUSIR - Nouvelle Aquitaine Ouest Office - He has studied the evolution of the different concepts governing today. His knowledge of both analogic and digital security, his experience in risk analysis and his expertise with USA companies have enabled him to position himself as an expert in defining security strategies. Observing and monitoring the cyberattacks that became more and more dangerous and intrusive in our lifestyles, he focuses specifically on the risks incurred by the general population and in particular the threats faced by VSEs and SMEs.

SMEs: Security Bytes

The cost generated by this technological increase prevents the entrepreneur from investing in the company's basic and vital needs, particularly in security. He or she implements security solutions proposed by service providers.

This often results in a multiplication of equipment, each one more efficient than the last, coupled with an increase of the volume of data to be stored, which must be protected in the cloud.

On the other hand, there is among leaders a lack of awareness about the risks.

Very often, they believe they are outside the perimeter of the attackers. They are in a syndrome that we could call "the laughing cow" syndrome (litt. translation from the popular cheese): too big, too small, too uninteresting, ... and we could go on listing a whole series of stereotypal ways of thinking that make them feel protected from criminals.

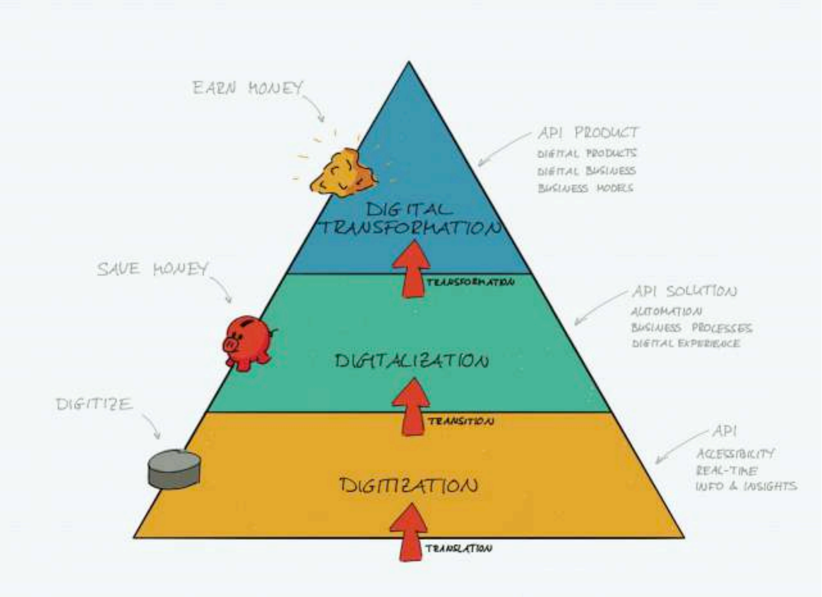
Moreover, States have not taken advantage of the recent years slow but real recovery of the 2007 crisis – now obliterated by the COVID pandemic – to impose a minimum counterpart on the assisted companies, which could in particular result in a structural change towards greater resilience.

From all this, it is clear that we continue to make cyber criminals happy.

A start would be that instead of converting a company's documents into data, it would be better to digitise the whole company, in a few words: all the company's processes should be taken over and re-thought digitally.

We can see then that this transformation can only be the fruit of a real and global awareness on the part of the entrepreneur. In order to achieve this result, he would have to manage his company in a real way, i.e. to constantly redefine its strategy according to the global business and threat panorama.

Faced with various crises, particularly the COVID-19 one, entrepreneurs chose to position themselves as heads of the company's management. They should rather take advantage of this crisis to manage their company and thus redefine their strategy. The dysfunctions that have appeared must be corrected and not just dealt with. Everyone should work on the cause and not just deal with it as the consequence of a problem. This is the big difference between management and leadership.



Let’s take advantage of these crises to implement long-term corrective solutions. Among these, cybersecurity is an crucial element.

We have therefore identified at least three factors that do not encourage the company directors to take into account cyber security issues:

The first is that, in crisis management, the business manager puts himself in a corrective rather than predictive mode, i.e. he deals with the consequences of a problem he tries to cope with and neglects or even ignores the real deep causes.

The second is that all this digitisation, which entails numerous and often costly investments, does not leave the entrepreneurs sufficient means to define a security policy.

The third is the lack of legal incentives, either at the level of the yearly bookkeeping or at the level of standardisations, through compulsory labels to be obtained in order to respond to calls for tender or to offer services, as is the case, for instance, if you choose to perform a training with a company having the “datadock” label.

What is damaging in the observation that has just been made is that the digitalisation of the company is not yet perceived as a discriminating element in the business world, while it goes without saying that this digitisation will have to take into account all the components of the information system and all the regulations related to it.

For example, very often, a GDPR compliance upgrade leads the business manager to review his entire information system. Reviewing the data and its processing allows him to optimise his procedures and, in addition, to limit the amount of data required to carry out the services he must provide.

In conclusion, in the face of the explosion of cyber attacks that affects companies since the COVID crisis started and will continue to do so, it is time for business leaders to take this issue very seriously. A regulatory incentive would be very desirable. The entrepreneur should also begin to understand the strategic importance of the whole information system and thus the level of protection and resilience that should be built to secure it. ■

SME – De-bunking myths

Author: Raj Meghani

If you are an SME - then you are at risk.

SMEs might have limited awareness of the types of risks or threats but with staff, customer, proprietary information stored in multiple locations, keeping on top of licences, certifications and renewals, understanding what a breach looks like and just as importantly how to react to a breach, etc, becomes too big a challenge for them to cope with let alone understand given time, cost and resource issues.

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

Before the COVID-19 pandemic, the top 3 biggest business challenges facing SMEs were attracting customers, increasing revenue and maintaining profitability. Infact, research has shown that 69% of small business owners say that they have been kept up at night with concerns around their cashflow.

So it's no surprise then that SME owners have their hands full. But with a small business getting hacked every 19 seconds it's fast becoming a nightmare for those who don't have security on their radar. With 1 in 5 being a victim of some form of cyberattack, it's not a case of IF but WHEN they get breached. So whether an SME employs 30 or 300 people - the cybercrime challenges remain the same and are getting increasingly sophisticated and more frequent.

With a typical SME's multiple security solution providers operating independently, there will be weaknesses exposing their business to vulnerabilities.

With cybercrime escalating – a 424% increase in authentic and new breaches of small businesses, 83% of SMEs lack the funds and expertise to deal with cyberattacks. A sobering thought and dangerous times.

There is an increasing exposure of risks facing SMEs today which have been exponentially catapulted through a cyberattackers wide attack surface. These can be broadly categorised into 3 key areas:

1 Financial

The average cost of a small business cyberattack in 2019 cost £6,160 (almost an 80% increase from 2018). The lack of specialist resource and increased training costs when purse strings are kept tight show there needs to be a balancing act.

SMEs must wake up to the fact that the actual cost of an SME investment on existing solutions versus lack of full protection or real cost impact of a breach needs a mindset change. 60% of small businesses that are victims of a cyberattack go out of business in 6 months. That's the reality facing SMEs today.

2 Reputational

It's no longer savvy or responsible for an SME to think or believe they are 'too small' for a cyberattacker to go after. The threat landscape and attack surface is changing.

SMEs may be further down the supply chain when dealing with larger enterprises, but they are the secret door into the bigger corporates who will already have their doors bolted to cyberattackers. SMEs are their gateway in – and most corporate businesses have woken up to this fact and insisting robust security measures are put in place by their suppliers.

Brand reputational damage in a playing field where referral business through word of mouth is prevalent is both lethal and destructive.

3 Compliance

The impact of GDPR on SMEs versus the larger enterprises has the same penalties. There is no allowance for ignorance.

LEGAL MAXIM

Ignorantia Juris Non Excusat

Whether you are in financial services, retail, professional services or any other sector steps must be taken and put in place to demonstrate all reasonable steps have been taken to ensure the safety of their customers data and privacy.

Raising cybersecurity awareness within SMEs is paramount. Helping to educate these businesses on how they can more effectively and efficiently utilise their existing technologies supported by access to specialised cybersecurity expertise and services will enhance their entire digital environment. This will not just help boost confidence but provide peace of mind – one less thing for them to worry about.

So let's de-bunk some of these myths.

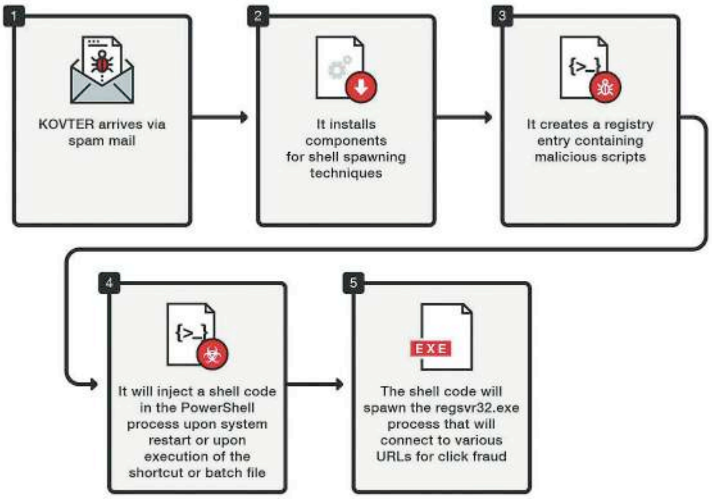
Myth #1: "I bought Norton 360, so I'm safe."

You might be tempted to think that Norton 360, or any similar security software, has the capability to keep you and your business cybersafe. This is not a surprise when product descriptions affirm a vast suite of protections from a secure VPN, a password manager, and defences against viruses, spyware, worms, trojans, malware… the list goes on. Undeniably, possessing such a comprehensive kit is a fundamental component of any sound security strategy. Nevertheless, it would be a mistake to assume that you can now put your feet up and hope for the best.

Unfortunately, cybercriminals do not take to holidays like the rest of us. Rather, they depend on our complacency to formulate their next plan of attack. Indeed, their methods continue to grow more sophisticated by the day. As security software is programmed according to a bank of existing viruses or malware, there is no guarantee that they can block, let alone identify, a new threat.

Fileless malware is a great example of a refined threat that often slips under the radar. As the name indicates, instead of installing a corrupt file, bad actors conceal malware on the back of legitimate applications already running on your device. From there, they can play mischief with the operating system whilst remaining undetected. According to TrendMicro, traditional security software programmes were pushed to their limits as they witnessed a 265% growth in fileless attacks in just the first half of 2019, compared to the preceding year.

SMEs: Security Bytes


1
KOVTER arrives via spam mail
2
It installs components for shell spawning techniques
3
It creates a registry entry containing malicious scripts
4
It will inject a shell code in the PowerShell process upon system restart or upon execution of the shortcut or batch file
5
EXE
The shell code will spawn the regsvr32.exe process that will connect to various URLs for click fraud

Example of a fileless attack © Trend Micro

In another instance, criminals have simply turned security software companies on its head, from a security providing service to the carrier of a virus. On these occasions, bogus antivirus alerts warn customers that their system is at risk, requiring them to 'update' their software.

At the end of the day, tools such as Norton 360, are useful to have but not fool-proof.

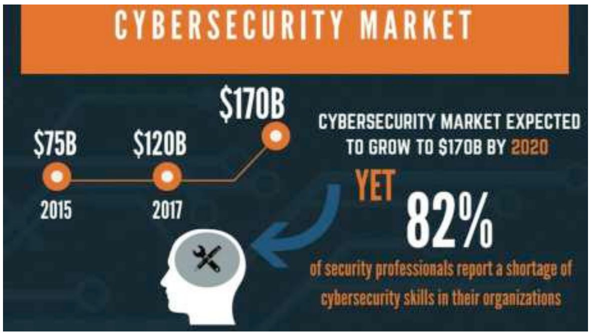
Businesses need to be proactive in their approach. There are solutions out there (tailored for SMEs such as BlockAPT) which allows its customers to stay one step ahead of the game by offering a clear picture of any and all threats across the network. The key is make sure SMEs have peace of mind that their business is safeguarded against cybercriminals.

Myth #2: "Cybercriminals aren't interested in targeting SMEs"

The notion that attackers only target the enterprise is a dangerous misconception. If you hold this belief as an owner of an SME, and it manifests in your security protocol, you are not only misinformed: you are also at even greater risk of being attacked and having your data compromised.

Given their general lack of cybersecurity expertise, skills and investment, SMEs are a soft target for cybercriminals, particularly at this time when an unprecedented number of remote workers, and their endpoint devices, are protected by inadequate solutions (or not protected at all). This climate of financial uncertainty, onset by the COVID-19 pandemic, also means the costs of a cyber-attack could be even greater than ever for smaller businesses, not least the rise in cyber insurance costs associated with heightened cyber risk.

The stresses and costs of maintaining a secure working environment during these uncertain times can be a huge drain on already dwindling resources and team morale.



To ensure SMEs stay secure and minimise costs, there are several free 60-day web security trials which they can leverage. This includes taking advantage of lots of features and benefits including:

- Fully integrated web application protection, security events management, and DDoS protection.
- Active monitoring of online web services and detection of web-based attacks.
- Automated security alerts enabling the ability to prioritise, respond and block web-based cyber-attacks.
- Fast responses to targeted web-based threats against an SMEs business.
- Mitigate against financial and reputational risks by preventing web-based malware breaches from being installed and distributed.

Myth #3: "My team have been trained - there's no chance they'll fall for a phishing scam!"

No matter how vigilant or cyber-literate, an SME's employees are not infallible! In fact, people are one of the most vulnerable components in any organisation's security infrastructure. This is because, unlike machines, we are susceptible to tiredness and stress, which leads us to make mistakes. Attackers prey on these flaws. And all they need to infiltrate a network or transmit malware onto a device is one wrong click.

A recent study I came across highlighted that 37% of the breaches they saw were as a direct result of people stress/tiredness. 35% of their overall study showed serious breaches occurring as a result of remote working. Sobering times indeed.

Once employers recognise this, it's vital they implement a robust security strategy that protects their employees and network. This means implementing multiple layers of defences using various security tools and by ensuring that users are trained to spot scams.

The first step is to ensure inbound emails are filtered and scanned using content scanners that check for malicious links and malware embedded into emails. Secondly, ongoing security awareness training must be carried to ensure that users remain vigilant, aware and abreast of new methods and iterations. Thirdly, organisations must assume that some malicious emails will eventually get through and have a strong endpoint protection in place to stop malware from executing on endpoint devices. Finally, they must have the right processes in place to detect and respond to reported phishing incidents in a fast and effective manner before damage can be caused.

Until companies stop relying on their employees' vigilance and awareness, and make the decision to protect them instead, phishing attacks will remain highly effective, damaging and costly. As cybercriminals use social engineering to exploit the coronavirus outbreak and the fear and suspicion that surrounds it, the need to take this approach has never been more pressing.

For companies, especially small and medium-sized businesses, in a position of financial uncertainty, the failure to do so could prove disastrous.

Myth #4: "My employees love me and love working here."

You and your employees get along great. Just last Friday you had a pint with them and took part in a fun quiz held on Zoom – this new reality called for a change of scenery to the usual pub by the office. You do what you can to make everyone feel valued and appreciated. So, you let your defences down and trust them to keep the company safe. They love you, they enjoy working here… why would they jeopardise that. Right?

Right. That might very well be the case. However, studies have shown that the majority of insider threat cases are not an act of malice. Indeed, according to Ponemon's '2020 Cost of Insider Threats Global Report', planned credential theft constitutes a mere 23% of overall incidents. Most cases can be attributed to the negligent employee. This individual may have left their work phone unlocked in a café, forgot to update their laptop, or inattentively opened a phishing email. This creates an opening for cybercriminals to infiltrate the system and access the business' database. On average, each breach could cost up to £1.15m. That is a hefty loss for any business, but particularly SMEs. Not to mention, the opportunity costs that might ensue from this blow to the organisation's reputation.

It is critical that security is embedded into the foundations of a business' operations, including nurturing a security conscious workforce. Education and ongoing refresher training on cyber hygiene is key.

Using cybersecurity technologies to help block and prevent Advanced Persistent Threats from cyber attackers and helping to reduce the onus on an SMEs employees to spot these sophisticated attacks is no longer an option. It's critical to provide a safety net for the business when some employees fail to protect it.

Myth #5: "My IT manager assures me that life is all good on the home front"

If your IT manager tells you this, I would advise you take it with a pinch of salt. The swift and unprecedented migration from the office to remote working has thrown up myriad security issues no one – from the enterprise to your SME – could possibly be prepared for. Ask yourself: 'Could someone really, comprehensively protect all of your company's assets, and personal connected devices being used for homeworking, without weeks, if not months, of preparation?' The answer is: they couldn't.

Many of those organisations that did manage to respond in some way were rushed implementing fundamentally inadequate and insecure remote access solutions. This poses a significant issue to all businesses whereby employees are directly targeted by COVID-19 scams which seek to exploit this remote access software by gaining unauthorised access to secure systems and sensitive data. Equally, as businesses open-up their critical infrastructure to be accessed by their entire remote workforce, cyberattackers will be looking for new ways to break into their systems. SME's may be further down the supply chain but as already mentioned they are increasingly the main target for cyberattackers looking to hijack their way into the larger enterprises.

Given the increase in the number of cyber-attacks on remote workers, SMEs, their IT managers and employees will have to step-up to defend themselves. This begins with acknowledging, rather than underplaying, the severity and enormity of the dangers at hand and adopting a vigilant and suspicious mindset.

Of course, no one solution can fully protect against the growing array of attack vectors cybercriminals have in their arsenal. Therefore, enforcing a multi-layer defence strategy – deploying various security controls at the network and endpoint levels – is imperative.

As the first line of defence, enforcing inbound and outbound network traffic security checks is crucial. At the second, it's vital to deploy a malware protection for endpoint devices by utilising both traditional malware scanning and behaviour analysis. That way, even if a system is compromised, the attack can be detected and disrupted before the damage is done. Thirdly, security awareness training should play a central role in the overall security strategy of any organisation. By raising awareness, organisations can significantly reduce their risk exposure to cyber-attacks. This becomes even more critical as we see the reliance on IoT devices increase to 74.5bn by 2025.

The trade-off between security and convenience means that employees will not be able to consistently detect and avoid targeted and sophisticated phishing attacks. Security focused activities are also often tied into an SME's office hours. This mindset needs a reset. Cybersecurity is and should always be on - 24/7/365.

We are rapidly moving towards COVID-21. A new mindset and cultural change in an SMEs business mentality is called for if they are to survive these uncertain times. ■

SMEs and IT security: the situation in Italy

Author: Imma Orilio

Cybercrime, since 2011, has not experienced any setbacks and the topic is now widely debated in all political contexts, there alas with an obviously sketchy vision, as well as in business contexts, there especially because of the *"Damocles' sword"* of GDPR sanctions. In fact, for IT managers, whatever the specific SME sector, there are many reasons for concern: from fraud to online extortion of e-commerce users, to identity theft and sensitive data theft, from industrial espionage to sabotage.

Small and medium enterprises, according to many studies carried out by various national observatories, are now beginning to invest in cyber security, and there are many reasons for this:

- as a consequence of an attack suffered by a competitor, a key moment to understand the cost that a data breach could have both in terms of loss of data and restoration costs .
- to respond to the needs of regulatory compliance dictated by the GDPR.
- after an attack that did not affect the competitor but themselves...

In any case small businesses often underestimate the growth in risk awareness among their employees and very few have specific training programmes. Yet more than 40% of threats to systems come from within the organisations themselves.

On the contrary, intentional threats (sabotage) represent no more than 10%, while the greatest damage is caused by unawareness - operator errors due to lack of expertise or unclear interfacing systems - which account for more than 15%, or by malfunctioning or inaccurate IT/OT integration (around 10%). The main reason, however, lies in the simple fact that in small companies IT (and even more IT security) is too often undersized in terms of resources (human as well as technical) and budget.

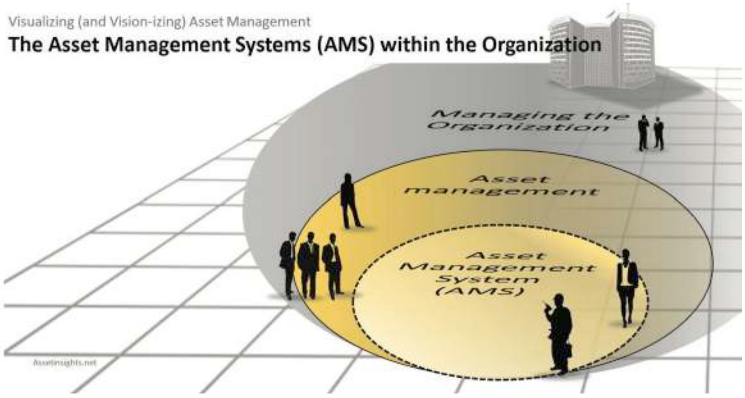
In fact, it should be made clear that the panorama that goes from the analysis of threats to the preparation of appropriate countermeasures and controls to be carried out is very broad and those who conduct it must have

BIO

The professional history of Eng. Imma Orilio is a natural evolution of an innate eclecticism. Born as a researcher at the Italian Centre for Aerospace Research where she graduated with a bachelor's degree in aeronautical engineering and specialization in composite materials and non-destructive testing. After 11 years of research she began her career in DEMA, a company in the aeronautical production sector, and then, in 2006, she received a public engagement in a healthcare company where she held the role of expert in technological innovation and CIO for 10 years. It is here that she began her journey in the field of cybersecurity, developing a project to convert the corporate data centre in 2009 according to the rules of privacy by design and default, virtualisation and realising an information system that in 2013 is "cloud ready". In 2017, she founded the company CREMETE srls, gathering professionals of high and recognised experience who deal with strategic, organisational and technological consultancy aimed at public and private health and in general at industrial production environments.

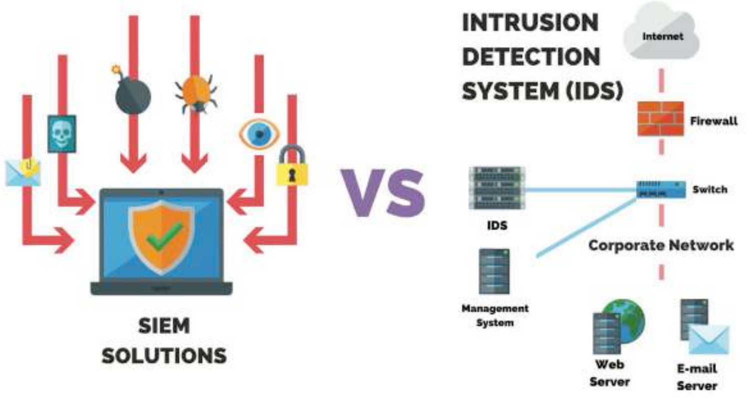
specific organisational, technological and regulatory skills. And obviously it is difficult for all these characteristics to be present in one single professional figure.

However, it is possible to identify what the essential steps are to limit the risks threatening your company.


Visualizing (and Vision-izing) Asset Management
The Asset Management Systems (AMS) within the Organization
Managing the Organization
Asset management
Asset Management System (AMS)
Assetinsights.net

Asset management system © Savid Albrice / AssetInsights

First of all, it is essential to have an Asset Management system that governs all the company's hardware - and software products used, so as to always have an updated mapping of the status including the possible obsolescence of configurations, access policies for each device, etc. Networks, devices and their access profiles must be surveyed, by defining a company regulation on individual passwords and their use.



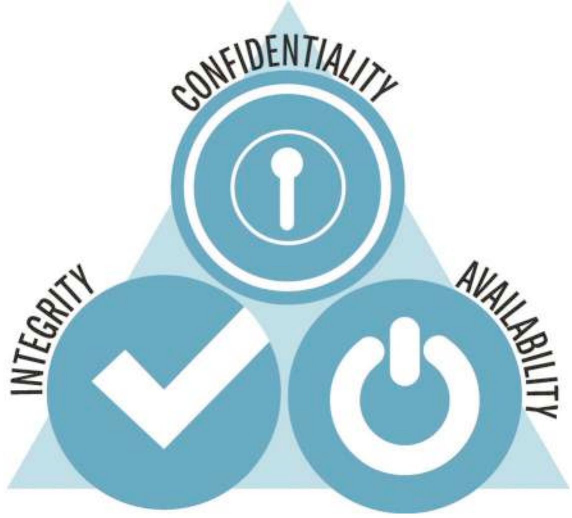
It is essential that anyone receiving a user profile has exclusive access to and protects the given credentials, and that unused accounts must be deactivated. Each business no matter how small should have SIEM (Security Information and Event Management) functionality, that tracks also the activity of the system administrators themselves.

All this, on the hardware side allows, among other things, the planning of replacement devices, aligned to the changing business needs. On the software side, such planning allows the effective management of updates and patches, on operating systems and applications, as well as antivirus, anti-malware, etc. This complete framework of knowing, anticipating, managing and planning also contributes to the indispensable construction of the data management register (art. 30 of the GDPR).

Also in terms of assessment, it is essential to have a complete list of active web services (cloud, mail, social accounts, etc.) to constantly monitor their use as potential vehicles for external threats (phishing, fraud invoice, etc.).

All the databases should in a compulsory way be classified into two main categories, each with its adequate surveillance: those where data has to be protected by law, and those that contain company relevant data (researches, patents, etc.) in order to determine the correct protection policies, each class of data should have assigned an appropriate value of ***Confidentiality, Integrity and Availability.***

Knowing one's own company means being able to govern it, but in order to move through the huge number of regulations aimed at the protection of one's own data, it is essential to rely on specialists in the sector.



Today, the COVID 19 emergency has seen companies obliged to switch their employees activities in a smartworking/homeworking way, disrupting, in many cases, the whole work organisation.

Obviously, the introduction of the smartworking concept in the context of an SME involves a substantial review of all organisational and technological assets. In fact, in order to guarantee assistance and continuity of service, the company must speed up its digitisation process projects.

This action, however, is not merely technological, but leads to a new way of conceiving the work relationship, from organisational to performance-based. It is now well established that measures to reconcile work and family life can increase individual and organisational productivity. Companies must therefore adapt their performance measurement and evaluation systems in order to asset the smartworking effect on the effectiveness and efficiency not only of their administrative action, but also on the quality of the services provided.

If the user needs to connect from home to the company because he operates in a smart work system, for example, it is necessary, at the very minimum to

SMEs: Security Bytes

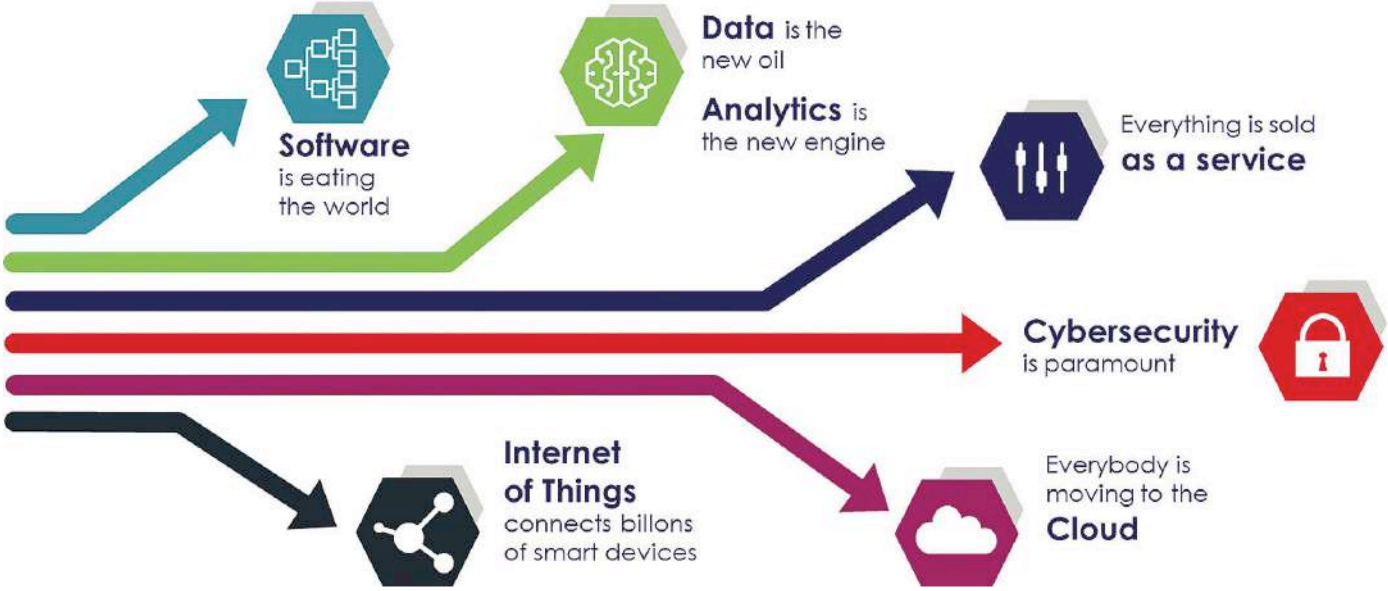
protect against intrusion, use a VPN (Virtual Private Network) connection. Hence, the company's networks must be upgraded to ensure business continuity and also disaster recovery.

In addition, employees must be trained, where they are not yet accustomed, to the use of a corporate and unified communication set of systems, which guarantees the management and sharing of documents in a protected environment, and, through a scheduled backup, allows to protect the work each employee has performed at home. Therefore, organising a small company structure based on key principles such as privacy by design is fundamental to protect the business.

If we shift the focus on privacy from a technological-organisational point of view, cybersecurity by design means planning the management of IT defences right from the planning stage with the aim of defending all the assets worthy of protection.

In Italy, SMEs are the vertebral tissue of the working system, and never as in this pandemic period are they undergoing deep reorganisations in order to adapt to the crisis.

Those that will succeed will certainly be projected towards a bright future. ■


Software is eating the world
Data is the new oil
Analytics is the new engine
Everything is sold as a service
Cybersecurity is paramount
Internet of Things connects billons of smart devices
Everybody is moving to the Cloud

Cybersecurity = the key to business continuity © Thales

Cybersecurity awareness: still a long way to go

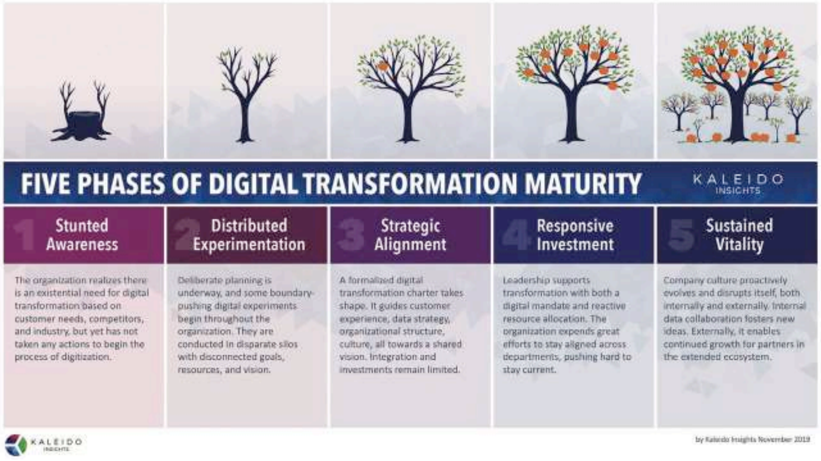
Author: Col. Marc-André Ryter

There is a fact that we should always keep in mind. Cyberspace, consisting for most of us of Internet and its connected sub-products, offers great opportunities. But the cyberspace also confronts us with many threats. The challenge is therefore to put us in a position to be able to benefit from the opportunities and at the same time remain safe from the threats. This is what cybersecurity is about and it is not an easy task.

Society as a whole needs to develop a digital culture, a set of rules that everybody applies freely and automatically in order to make cyberspace safe. However, it is also important to underline that this digital culture is not only an issue in private life. It has to be a reality during professional activities. Even if the objectives of cybercriminals might be different when they attack private persons or companies and State agencies, the digital culture can be equally beneficial for both.

BIO

Expert in security policy, Colonel Marc-André works for the Swiss Army General Staff. He holds a BA in Political Sciences and an MA earned at the NATO Defence College in Rome. He follows and studies the technological evolutions potentially relevant for the Armed Forces, in order to deduce the necessary consequences on the miltary doctrine



FIVE PHASES OF DIGITAL TRANSFORMATION MATURITY

KALEIDO INSIGHTS

1 Stunted Awareness	2 Distributed Experimentation	3 Strategic Alignment	4 Responsive Investment	5 Sustained Vitality
The organization realizes there is an existential need for digital transformation based on customer needs, competitors, and industry, but yet has not taken any actions to begin the process of digitization.	Deliberate planning is underway, and some boundary-pushing digital experiments begin throughout the organization. They are conducted in disparate silos with disconnected goals, resources, and vision.	A formalized digital transformation charter takes shape. It guides customer experience, data strategy, organizational structure, culture, all towards a shared vision. Integration and investments remain limited.	Leadership supports transformation with both a digital mandate and reactive resource allocation. The organization expends great efforts to stay aligned across departments, pushing hard to stay current.	Company culture proactively evolves and disrupts itself, both internally and externally. Internal data collaboration fosters new ideas. Externally, it enables continued growth for partners in the extended ecosystem.

KALEIDO INSIGHTS

by Kaleido Insights November 2019

Often, people link cybersecurity with technical issues and think that cybersecurity is and has to be provided by technical solutions, like antivirus softwares and filters. Artificial intelligence can support technical solutions and opens new possibilities. In particular, I would like to highlight the potential offered by profiling users of the internet. This helps identify any unusual actions and stops them immediately. This is why technical solutions are in any case an important component of cybersecurity. But they do not represent THE solution.

However, this article focuses on digital culture. It is about the behaviour of people when they face cyber threats. We often forget that our PC with internet is not the only tool we use that connects us to the cyberspace. Another device we use daily is our smartphone. This one is even more dangerous, as we forget how much data a smartphone can collect. Consequently, we are often careless about our behaviour with and towards our smartphone. Let us remember that most of today's smartphones have a million more computing capacities than all the systems used to send Apollo 11 to the moon together.

The interconnections in the cyberspace are part of the same system and a single weak point in that system, often called "weak link", is enough to endanger, respectively successfully attack, all links in that system. Of course, there can be technical weak links like a computer that is not protected. But most of the time, it is a human being, whose behaviour with his/her computer or smartphone who creates the weak link.

Investing in training for correct digital behaviour for cyberspace users is therefore as important as investing in technical security solutions. In Switzerland, Ministries have repeatedly been under attack, and some governmental agencies in the past few years were successfully attacked, and data was stolen. The targets were not always in the field of defense or intelligence, which shows clearly that any state activity can be of interest for cyber criminals. This shows that all users of internet and owners of smartphones need to be trained and to adopt a correct digital behaviour.

Switzerland has a complex federal state structure with specific competences being distributed between the federal state, the 23 cantons and the 2022 communes. This means that these bodies need to work together and share information, in other words need to be linked. This cooperation requires a safe cyberspace as it is the main working environment. All these institutions also work with external companies and, as political bodies, have contacts with the population, meaning everybody. The risk is therefore very high to have weak links in the system.

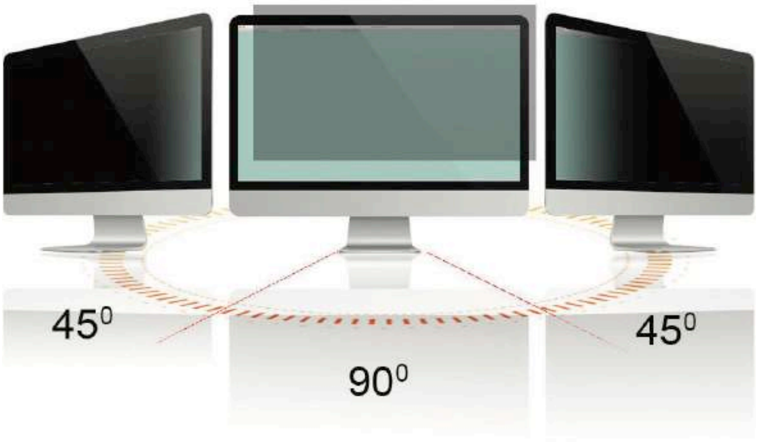
In addition, the unique Swiss military militia system also represents a cyber challenge. Mainly based on reserve, it implies that people come to accomplish military service every year for a limited period of some days up to some weeks. These military personnel come from civilian duties and bring their own digital behaviour from its private and professional activities. This is an essential feature, as these military personnel will work on defense systems. If the company from which the member of the reserve forces comes from has a developed digital culture and a safe behaviour towards potential dangers in the cyberspace, this is an asset.

However, if military personnel come with deficient digital behaviour, they constitute weak links and can create opportunities for cyber criminals. It is therefore important as well for the armed forces to train military personnel and to implement a correct digital culture. Training the people is central. All military personnel must understand the threats and integrate the security measures in their behaviour. Armed forces need to be able to train militia military personnel at a very high speed and to control all personnel accessing defence systems with the correct digital behaviour.

This has become a little bit trickier than in the past, when spying activities relied mostly on measures that were more concrete and were implemented by physical and visible persons. Nowadays, danger in the cyberspace is less tangible. Still, very simple and concrete measures can already contribute to

enhance cybersecurity. I would now like to underline some of them, which we are implementing within the armed forces.

The first and most obvious one is that you should not speak about confidential issues on the phone. If you need to, make sure you use a commercially available system like Threema that will protect your calls. This will increase massively the confidentiality of your conversations. In addition, take care of your environment when you have business calls. I am always amazed when I travel by train to hear people speaking openly and loudly about their business deals without caring about who might overhear them.



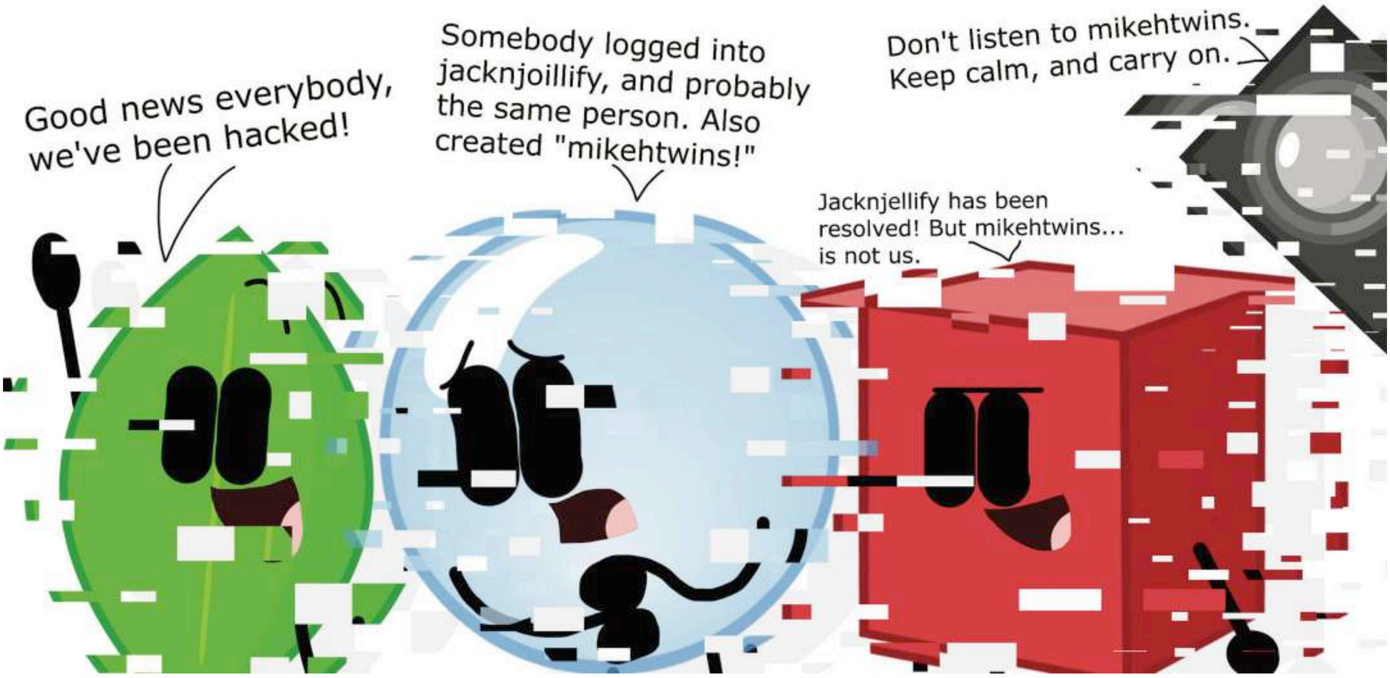
The second simple measure is to use a privacy screen protection system. These are nowadays very easy to purchase and to install and protect your screen from unwanted glances, in trains, planes, restaurants, cafés and bars, but also at your working place.

Third, most of the people do not actually know the potential of their smartphones. So there is only one rule: when dealing with sensitive and confidential issues, leave all smartphones outside the room. We have already installed lockers near our meeting rooms. It is easy, efficient, but still very difficult to implement. Most of the people are convinced they need to be permanently reachable and able to look at their emails. And do not take a smartphone at your working place if your daily work implies dealing with sensitive issues.

Fourth, companies should make sure their personnel use pcs and laptop that have inbuilt security systems and security software allowing to encrypt confidential emails. It has become a kind of standard that our laptops need a smartcard to be operational. This creates from the very beginning a much better protection measure.

I would like to conclude with a general safety measure that relies on common sense. It is necessary to train people not to open every email and attached document. If you feel something is not crystal clear, do not open. Check the sending address carefully, look at the text of the email to search for spelling mistakes or strange sentences, and if you have any doubt, do not open. In general, delete all emails promising you money or any attractive reward. Even if this seems incredible, there are still people being hacked by opening attached files promising lottery wins even if they know perfectly well they have never played this lottery.

As you see, government agencies, companies and private persons can easily and equally apply the same digital behaviour and contribute to improved cybersecurity. Nobody alone is responsible for cybersecurity, but everybody can contribute. Starting by simple things helps. ■


Good news everybody, we've been hacked!
Somebody logged into jacknjoillify, and probably the same person. Also created "mikehtwins!"
Don't listen to mikehtwins. Keep calm, and carry on.
Jacknjellify has been resolved! But mikehtwins... is not us.

5G & IoT Security: With great speed comes great responsibility?

Author: Marco Essomba

By now you can't have missed the widespread announcements about 5G and all the advancements it warrants. From outdoor billboards to your personalised social media feeds, we are constantly reminded of how 5G will make our lives better and transform how we conduct business.

In case you missed the highlights, the key benefits are greater speeds, faster downloads, connectivity without lag, increased efficiencies, and support for up to one million device connections on private 5G networks. And in the current COVID-19 era, there is a bigger incentive for organisations to rapidly adopt 5G and upgrade their IoT as it will enable:

- An advanced digital infrastructure that will permit people to continue to work remotely, attracting more talent and boosting productivity
- Industries such as construction and manufacturing to revive services with increased efficiencies when moving to 5G private networks
- Education, Government and Healthcare to benefit from providing essential services to pupils, public and patients with reliable remote access

Moreover, Government legislation and international guidelines have deemed that 5G is perfectly safe, putting any conspiracy theories to bed.

BIO

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

LinkedIn - https://www.linkedin.com/in/marcoessomba/
Twitter: https://twitter.com/marcoessomba
Company website: https://www.blockapt.com

In fact, studies from organisations including the World Health Organisation, Public Health England and the UK Health Protection Agency have all shown that 5G isn't harmful to health.

There seems to be no catch, so why not adopt this new technology immediately?

Perhaps, not so fast. While I am all up for the latest digital transformation, my security senses are tingling.

We must remember that 5G networks are virtualised and software-driven. This increases cyber vulnerability by a lot as an attacker that gains control of the software managing the network can also control the network.

The IoT market is not regulated and therefore not obligated to meet specified security standards. For attackers, these open endpoints are juicy targets for deploying malware-based scripts. The prospect for attaching billions of smart devices that are hackable to an IoT network increases vulnerabilities. The expansion of bandwidth in 5G also opens up more attack-routes.

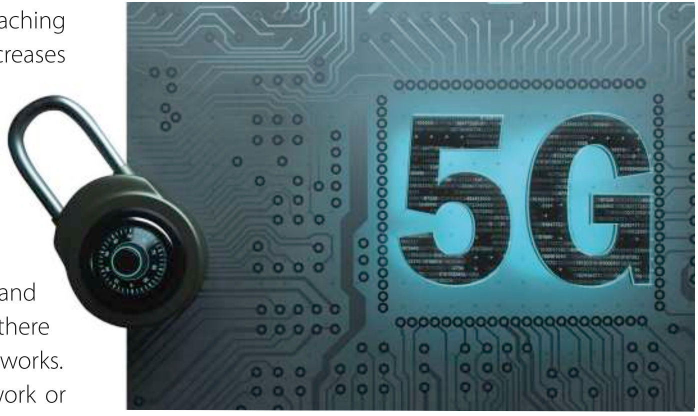
The pace of IoT innovation is also another factor. Software developers will face pressure to get services quickly to market, so critical security and vulnerability testing could be missed, as it is not often the focal point of concern.

Currently, shifting to a private 5G network is time-consuming and costly. By the time legacy network infrastructures are upgraded, there is a high chance that endpoints have already operating on 5G networks. For organisations, smart IoT without their own dedicated 5G network or adequate security knowledge could put the organisation and employee privacy at risk.

5G will no doubt question our assumptions about network security and the security of the devices and applications that attach to that network. If you plan to adopt 5G in the coming future, you absolutely must have an action plan for 5G security right now.

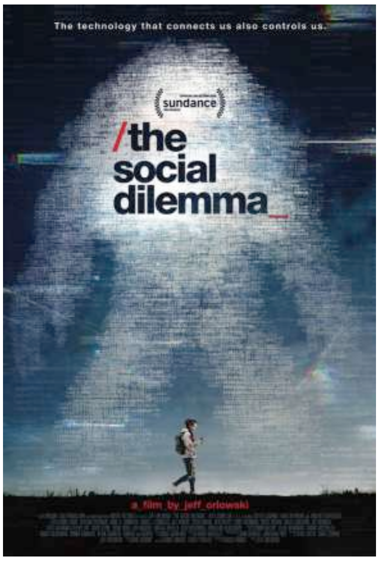
5G is no doubt coming, but security needs to catch up.

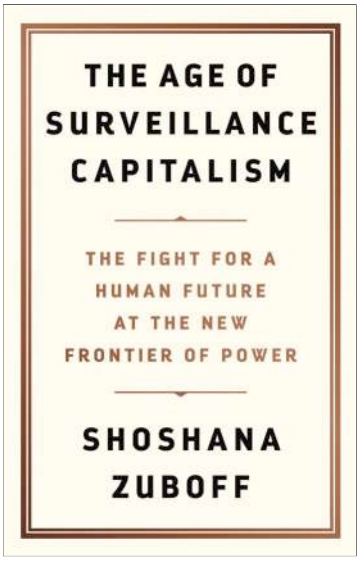
Beyond that, without stronger government regulations, policies and proactive security measures by businesses, 5G networks may remain vulnerable to cyberattacks. ■



Being responsible is no longer an option

Author: Nicola Sotira





THE AGE OF SURVEILLANCE CAPITALISM

THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER

SHOSHANA ZUBOFF

In recent weeks, there were a lot of discussions and posts on blogs and the web about the movie "The Social Dilemma" available through Netflix; moreover, I often found quotes of the film used in conferences where the movie itself is used in an instrumental way. Thanks to a series of stories by Silicon Valley entrepreneurs, the documentary gives us a behind the scenes preview about digital platforms that work on our vulnerabilities and would "manipulate" us for mere economical profit. The Social Dilemma evolves on some main axes: digital transformation, manipulation/persuasion, now seen as a product, and last but not least digital surveillance, as shown by the milestone reference published by Shoshana Zuboff.

One of the themes in the film is that of digital transformation and metamorphosis, the acceleration of technology that does not go hand in hand with our learning and our difficulties in keeping up with increasing innovation. In addition, attention is paid to highlight the dark side of the medal; on the one hand, the enormous changes are absolutely positive on a global level, and on the other hand exploits our dependency and obsessive use of different digital platforms.

The analysis develops on the subject of profit and how it is generated, a profit based on data, analysis and forecasts where the product is the consumer of the platforms. The theory that is stated is that we are no longer in a market based on the sale of products and services, but in a scenario where our data, enriched by our habits and behaviour on the net, are the new features.

Obviously all this is managed by a network of algorithms that use the whole human race as a huge laboratory guinea pig.

Finally, the film analyses the themes of persuasion and fake news; it points its finger at the use of sophisticated technologies and the use of social media for the persuasion of users who are, therefore, induced to make targeted purchases in addition to influencing political choices and managing movements of opinion.

BIO

Nicola Sotira is General Director of the Global Cyber Security Center of Poste Italiane and Information Security Manager in Poste Italiane. He is in the field of information security for over 20 years with experience in different international companies. In his previous experience, Nicola Sotira was sales Director UC&C & Security Practices in Westcon Group Italy and VP Sales Italy in Clavister AB. Professor at the Master in Network Security of La Sapienza University since 2005, Member of the Association for Computing Machinery since 2004. Promoter of technological innovation, he collaborated with several startups in Italy and abroad. Member of "Italia Startup" since 2014, he advises the conception and the development of several mobile services. Nicola is also a member of the Oracle Security Council.

The painted scenario is that of a network used as an instrument of dubious morality. A digital weapon capable of determining relevant consequences in the social and political field of a country. This last aspect is then connected to fake news and alarmism, artificially created by the algorithms managing digital platforms.

The film supports the thesis that digital manipulation has both purely commercial purposes, i.e. with a view to making pure profit, and the objective of guiding network users in an imperceptible but constant way, thus influencing society, politics and the economy.

This misinformation would be greatly amplified - thanks to the increasing use of social networks at a point - allowing them to generate in extreme cases social unrest. We have all seen, for example, the role played by disinformation on the COVID topic. So what to can we do to stem this domain, at least as presented in the film?

Surely the digital world and technology development are contributing continuously to the economic development of society and also contributing towards improving our quality of life. Certainly there are also negative aspects, which must be contrasted with culture, investments in schools and training.

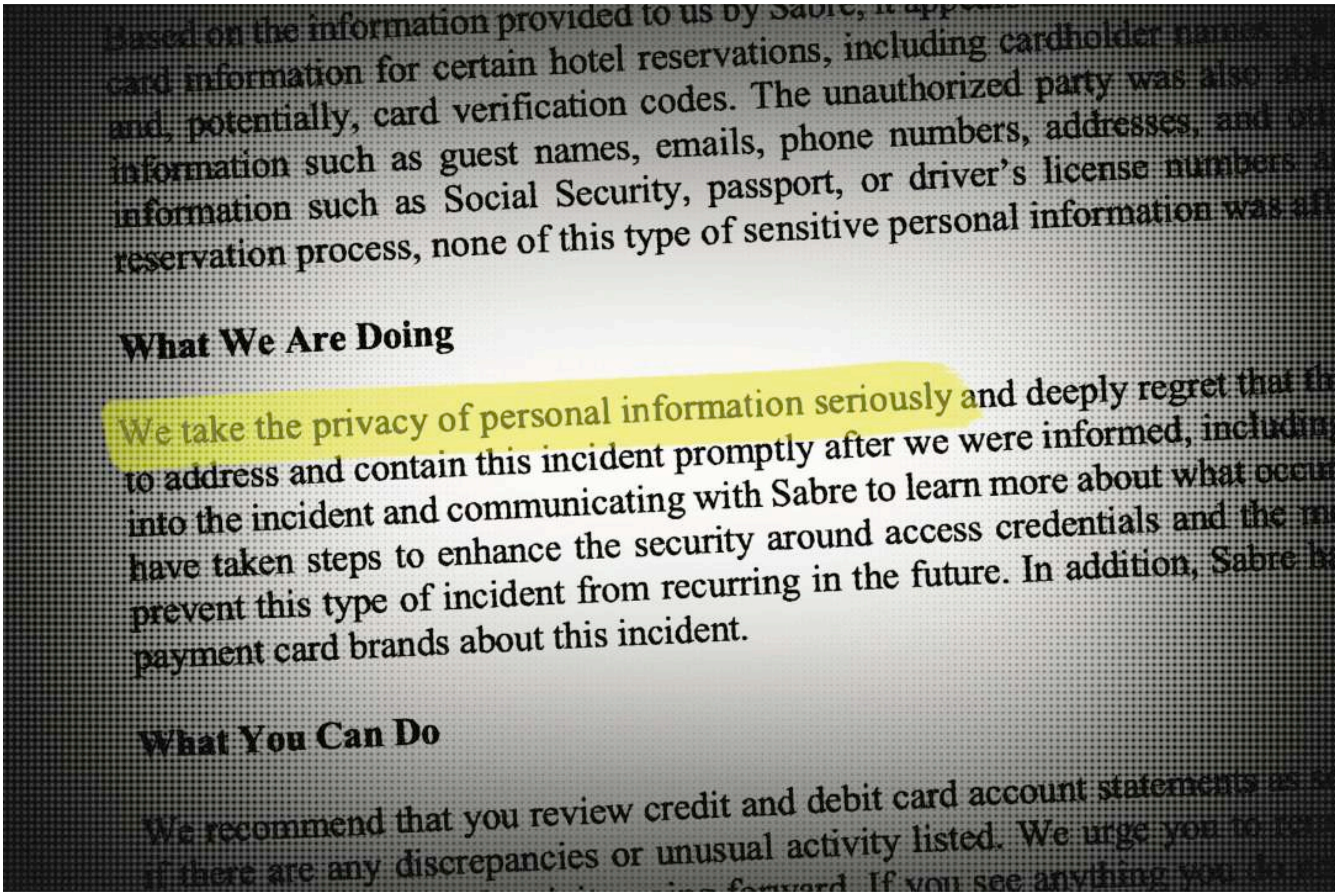
A conscious use of these tools and digital culture must become a full part of the education provided to the new generations and beyond. However, we also have an issue of responsibility that is up to any one of us alone: if a movement wants to convince us that the earth is flat, probably the responsibility of the platforms lies in spreading this theory, but we can neither adhere to it nor promote it knowing that it is an anachronistic discussion and perhaps it could have made sense in Galileo's time, but today it is just paradoxical.

It is exactly the same attitude leading us in a compulsory way to responsibly use personal protective equipment to counter the spread of COVID, the same attitude aligned to the fact we shouldn't park our electric scooter on pedestrian crossings.

In this context WE make the difference and our responsible behaviour plays a fundamental role. The social and digital platforms presented in the film are populated with algorithms, which WE write and design, and where WE always opt to use them.

WE are the engine of possible change and WE must also contribute to ethical development through our behaviour.

If we become ethical and responsible consumers, even the Silicon Valley entrepreneurs will follow this trend only because it will generate huge profits for them. ■



Based on the information provided to us by Sabre, it app
card information for certain hotel reservations, including cardholder names
and, potentially, card verification codes. The unauthorized party was also
information such as guest names, emails, phone numbers, addresses, and
information such as Social Security, passport, or driver's license numbers
reservation process, none of this type of sensitive personal information was

What We Are Doing

We take the privacy of personal information seriously and deeply regret that
to address and contain this incident promptly after we were informed, including
into the incident and communicating with Sabre to learn more about what occu
have taken steps to enhance the security around access credentials and the
prevent this type of incident from recurring in the future. In addition, Sabre
payment card brands about this incident.

What You Can Do

We recommend that you review credit and debit card account statements
if there are any discrepancies or unusual activity listed. We urge you
forward. If you see anything

Security labelling – your new IoT trust mark?

Author: Raj Meghani

The average UK household will contain 50 connected devices by 2023 as the Smart Home sub-sector booms, according to British Telecom (BT) Consumer Division. A scary statistic when you consider this is now also the same environment where remote workers are carrying out their business duties as we continue to operate within the 'new norm'.

The number of IoT devices in UK homes is increasing at a rapid rate. According to a new study from Aviva, the average home in the UK now has 10.3 connected devices accounting for more than 286 million devices nationally.

By 2025, reports estimate that there will be 75 billion Internet-connected devices worldwide – a five-fold increase in ten years.

But it appears that there are major concerns surrounding privacy and security exposure risks with the explosion of IoTs as far as cybersecurity design protocols are concerned. It leaves a lot to be desired. Many if not most of the IoT devices are designed to optimise general functionality and cost above in built security features. This could leave the customer's privacy and sensitive data vulnerable or compromised.

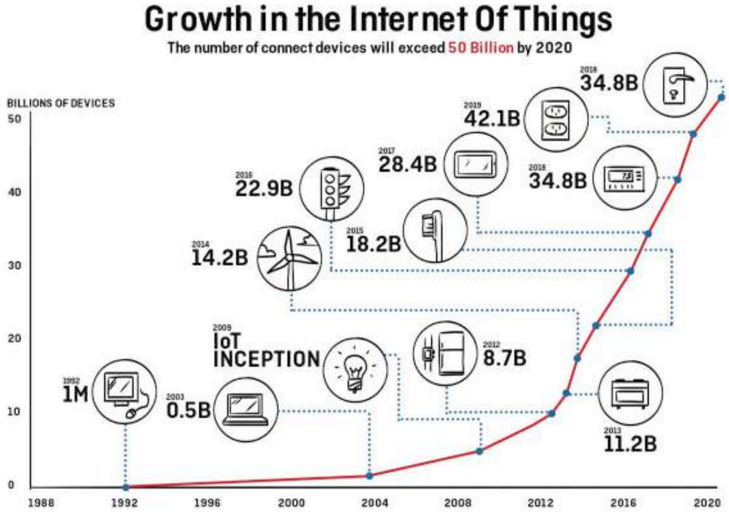
With this rapid growth in connected devices, the UK Government has created plans to ensure that millions of household items that are connected to the internet are better protected from cyberattacks.

To address this, the UK Government has looked at a much needed initiative into a new labelling scheme. The labelling scheme initiative may be similar to energy labels, with a tiered reference to cybersecurity rating levels that can guide customers into making informed decisions. The security label is intended to instill confidence in customers that their device is safe and secure according to standards.

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



Many of the internet-connected devices currently on the market still lack even the most basic cybersecurity provisions. Over 90% of 331 manufacturers supplying the UK market in 2018 did not possess a comprehensive vulnerability disclosure programme up to the level the UK Government would expect.

Manufacturers and Retailers:

Although the current preference is a voluntary initiative to help educate and raise awareness to customers, Governments will need to take a harder stance with regulatory measures if this is really going to take off. Companies may be unwilling to display a label that indicates that a product has poor security if the scheme were voluntary.

A mandatory scheme will force manufacturers and retailers to follow the 'Secure by Design' principle and ensure that basic cybersecurity features are built into products. These include:

- IoT device passwords must be unique and not resettable to any universal factory setting.
- Manufacturers of IoT products provide a public point of contact as part of a vulnerability disclosure policy.
- Manufacturers explicitly state the minimum length of time for which the device will receive security updates through an end of life policy.

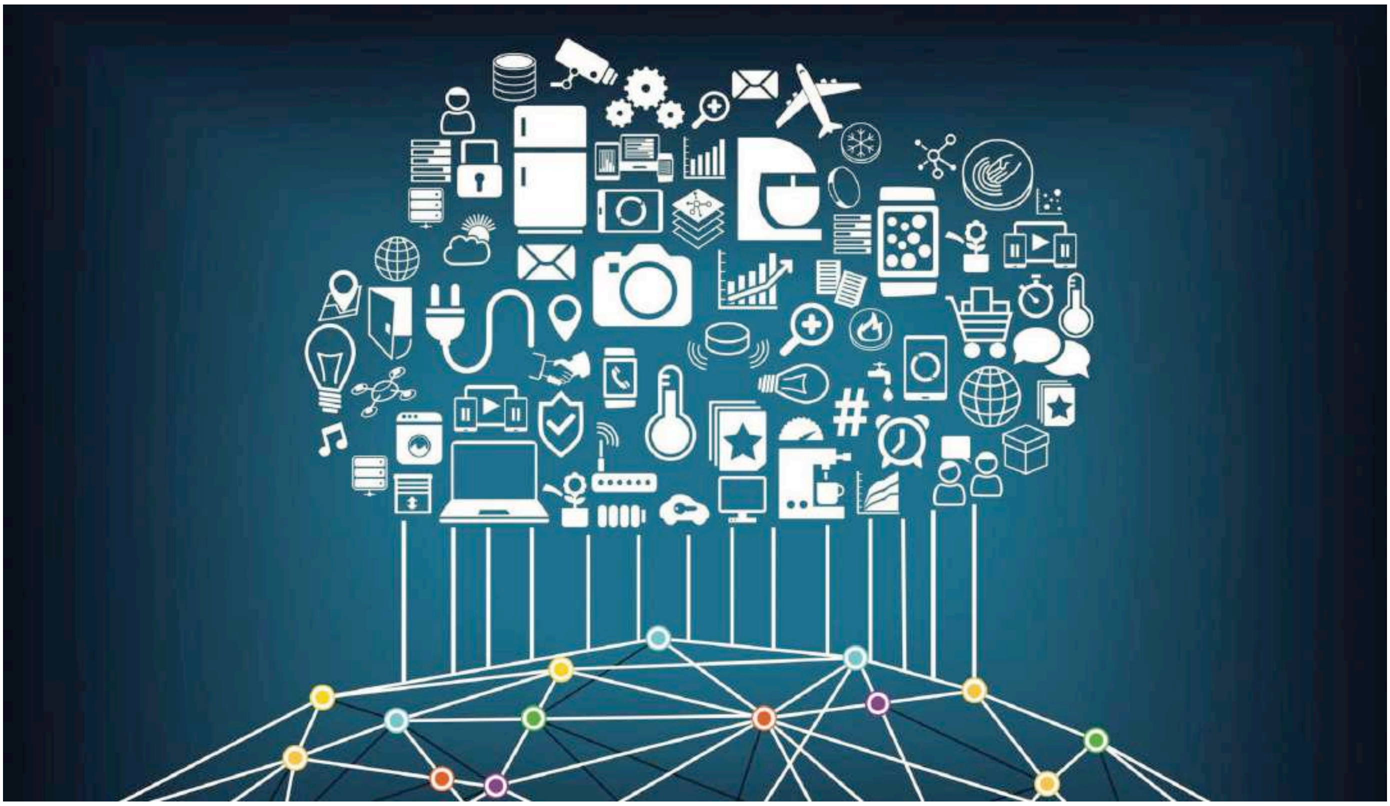
Once enforced retailers will only able to sell smart devices with an IoT security label while adhering to the 3 key points above. Interesting times ahead then.

Customers:

The labelling scheme will be welcome news for customers and industry watchdog bodies, as it will empower them to make more informed choices when it comes to purchasing and relying on the technology they are using at home or for accessing services.

However, the onus now shifts on the customer to ensure that they stay secure online.

In a similar way the food labelling industry regulations have helped customers make the right decisions for them



with the colour coded labelling system and nutritional detail upfront on products. The new labelling system will need to ensure that it can optimise this customer experience/familiarity to help expedite the take up of this initiative to aid customers understanding of colours/symbols at each of the different tiers.

Without customers being alert, they could find their personal data easily accessible by popular search engines, casual browsing or more determined attackers who could then use their connected devices to mount attacks on others or even steal personal data to commit identity fraud.

To mitigate against these loopholes, customers should:

- Research the security of a product before buying - rely on the labelling system to make an informed decision once launched.
- Ensure that their router is secure - protect the 'gateway' to all connected devices.
- Change any passwords and usernames from the default factory settings.
- Access their online account securely.
- Always use two factor authentication where possible.
- Ensure their software and apps are kept updated.
- Visit the manufacturer's website to look for the latest updates or follow Government advisories if security breaches for your manufacturer are confirmed.

It is great to see that both the UK and Singapore are leading the scheme hoping that the industry itself will find and join forces with regards to best practise for the labelling.

And it is off to a great start as Amazon, Philips, Panasonic, Samsung, Miele, Yale and Legrand affirmed their commitment to taking steps to ensure that effective security solutions are being implemented across IoT devices on the market.

Being in the security industry, I welcome this initiative and believe this cannot come soon enough.

However, I am also wary of the impact this will have on the customers purchasing behaviour. How keen will a customer be to pay for extra levels of security if manufacturers pass this cost onto customers? I've been reliably informed that one great thing about this scheme is that unlike other cybersecurity certifications, the price of the certifications is indeed more competitive. One to watch as this unfolds.

There is a real disparity between what the customer **actually thinks they are buying** and **what they are actually buying**. A disconnect between how **secure the customer thinks their IoT device is** and **how secure it actually is**.

The pace of innovation, competition and IoT race often means manufacturers and developers are rushing to get devices to customers as fast as possible.

Security may not be on top of their minds. We need all the stakeholders - Government, IoT industry and customers to come together to make our digital world a secure place.

It comes at a price – question is will the manufacturers, retailers and customers play ball together before they are forced to? Time will tell – let the game begin. ■

ML, AI, IoT: why it is important to take the time to reflect

Author: Laurent Chrzanovski

At a first glance, we can see that the topics proposed by multinationals, which have been duly addressed both by the various non sector-specific magazines and by our Cybersecurity Trends magazine with an analytical spirit, are identical to those that preceded the two "lost" years discussing almost exclusively the implementation of the GDPR and the measures that should be taken by companies.

BIO

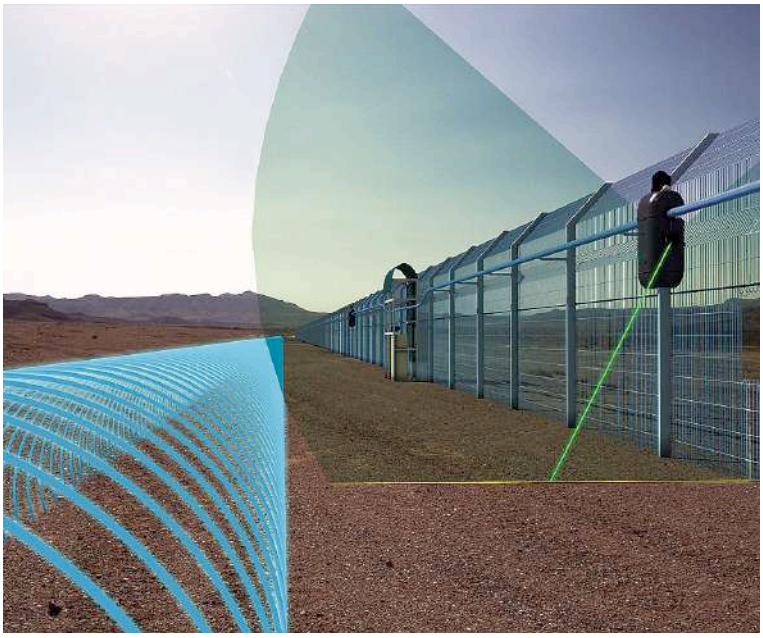
With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu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

Recently we are witnessing a "classical" paradox. For obvious reasons of global economic warfare, the issue of 5G and the new security approaches needed by any company that decides to move "from cable to wave" seem to have become taboo.

Yet the very transition from a perimeter defence to a global defence represents a real quantum leap that includes the use of new technologies and new formations: it is no longer a question of defending an intra muros structure, with its IT tools and workers, but it must now include all remotely connected employees, objects, machinery and also users.

In this sense, discussing ML, AI and IoT is vain and premature, precisely because 5G is the last and rather indispensable link to allow the finalisation of the fourth industrial revolution, which includes everything contained in

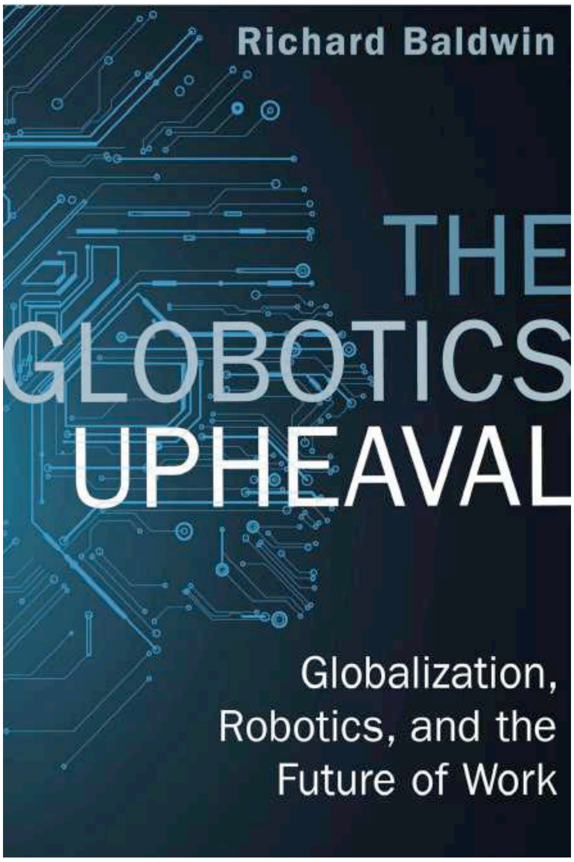


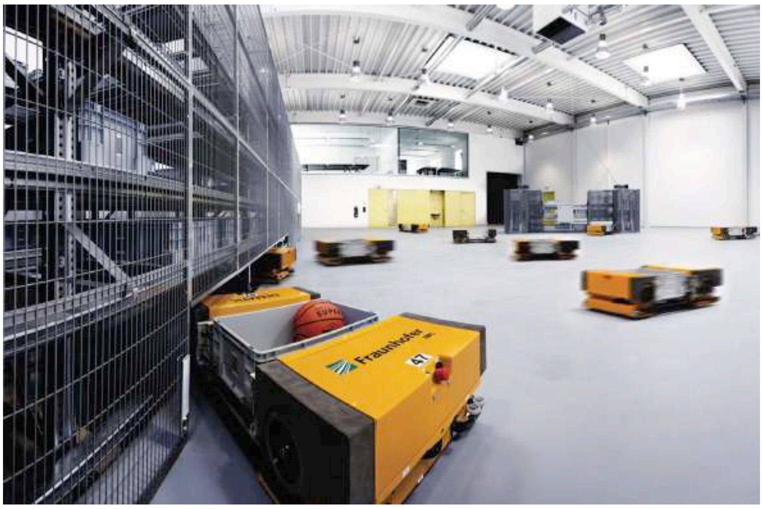
the three well-known acronyms. Arriving then to *Machine Learning*, now inseparable from *Artificial Intelligence*, we can observe two attitudes and two realities in full contrast with each other.

The progressive attitude

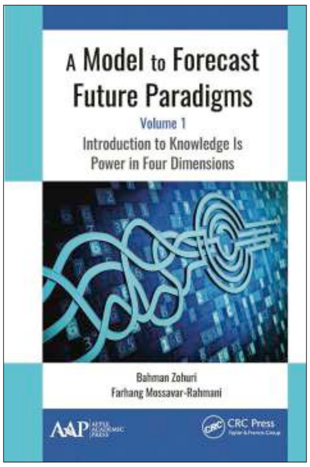
Richard Baldwin's masterpiece, *The Globotics Hupheaval*, is the perfect interpretation of the economic point of view on robotics and AI. Robots will not be able to function properly if they are not equipped with *machine learning* and *artificial intelligence*, which in turn, in order not to give counterproductive results, need powerful global infrastructures that guarantee their proper functioning, defence and limit their damage as much as possible.

So we find ourselves once again in front of another monopolistic "niche" similar to the GAFAM one, as we can observe by the small number of suppliers in the advanced robotics sector for logistics sites (4 giants: one Japanese, one German and two Americans, obviously delivering products with a majority of China-made components). The book, celebrated by the Sunday Times as *"A manifesto as proof of the future of our jobs and prosperity,"* explains where we are with these technologies, where we will be in the short and medium term, and how many benefits our companies could derive from them.





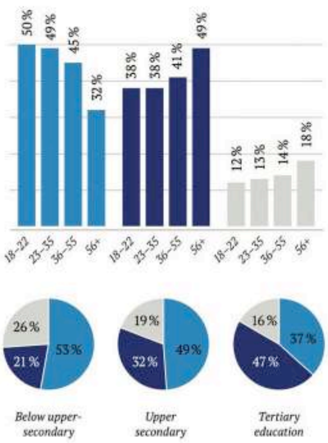
The realistic attitude of specialists and population

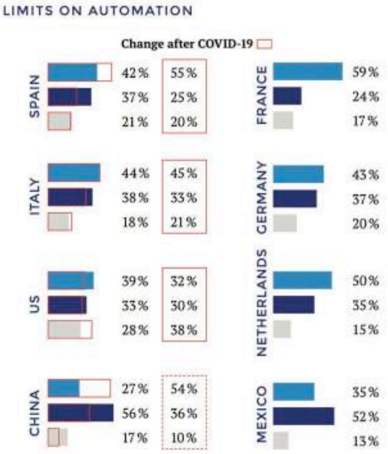

A Model to Forecast Future Paradigms
Volume 1
Introduction to Knowledge Is Power in Four Dimensions
Bahman Zohuri
Farhang Mossavar-Rahmani
AAP
CRC Press

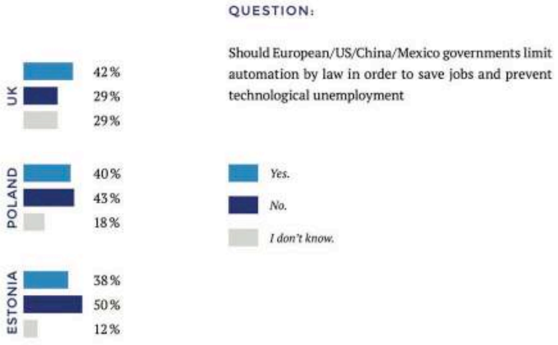
Summarising many articles and books, including the most important *"Knowledge Is Power in Four Dimensions"* by Indian researchers Bahman Zohuri and Fahrang Mossavar-Rahmani which shows how ML and AI results can only be useful in combination with human intervention that analyses and refines them. Hannah Kerner, researcher and Machine Learning specialist for food and agriculture within the NASA's "Harvest Program" makes this point: **"Too many AI researchers think real-world problems are not relevant. The community's hyperfocus on novel methods ignores what's really important."** (MIT review, 8 August 2020).

The headline of the second chapter **"More harm than good"** is even more incisive, showing how far from reality are those who invent the AI products of tomorrow. Because, as masterfully demonstrated in Gary Marcus's research entitled *"Deep Learning: A Critical Appraisal"* (White paper, New York University, 2018), researchers rely on a completely stable ecosystem. This is the reason for their success in viticulture or in preventing cardiac arrhythmias for the chronically ill patients). Most AI products, however, do not capture the "noise" of fake data and have proven to be completely ineffective for business strategies or IT development. This is due to their inability to understand different languages and cultures, in an increasingly diverse world where, precisely, those aspects are necessary for a proper understanding of an individual country (military, cyber, geo-strategic, economic, social and political potential).

On the part of the citizens we observe a healthy dose of skepticism, accentuated also by a real fear. The demand to adopt immediate State regulations that will define and limit the activity of robots and AI is now a common requirement for most Europeans (75%!). The 2019 annual report of *Mapping European Attitudes to Technological Change and its Governance* showed that *"most Europeans believe that governments should take immediate action to limit automation and address the negative effects on society".*







ie
EUROPEAN TECH INSIGHTS 2020
Unveiling the technological future that citizens want and their concerns in a changing world
2020

The 2020 report, which has just been published, notes that the urgent need for State intervention to adopt rules limiting the use of robots and automation has increased by almost a third since the start of the COVID-19 pandemic. For example, in China, maximum levels have been reached: 54% of citizens are now calling for rapid state intervention, while in 2019 this was only 27%[1].

The pragmatic reality of the economic world:

From an economic continental point of view, every repatriated euro – or pound – counts today. A company, in order to increase its competitiveness, would not bother to replace hundreds of underpaid men, women and children (in States where the law allows work from the age of 12) in the third world with a fleet of robots in Europe, despite the damage it could do to those countries with the closure of factories. In this regard, the World Bank has just denounced that, among many factors, IA and robotics will be *primarily* responsible for an additional 170 million people reaching the absolute poverty line (less than 1.69 US/day) by January 2021- while IA alone will have a greater impact in richer countries, robotics, on the other hand, will especially harm Asia.

The pragmatic reality of the security world:

AI security solutions, which aim to replace all the technological and human means used so far, are still completely immature. As such, they have been rejected by all essential services dealing with State security. In only two areas does AI/IV offer very useful results. The first area is that of technologies, implemented with AI, aimed to report and deal with APMT *(Advanced Persistent & Mutant Threat)* - the "M" was added more than a year ago - and it is precisely because these mutations are simply additions or changes to a already known patterns of a precise malware that AI can recognise and respond more quickly than a human.

The second is data sorting, because the creation of data on an hourly basis is such that it cannot be handled by humans. AI allows analysts to focus on the most serious and most urgent threats, provided they do not eliminate anything, because it is precisely from the mass of discarded data that the best specialists can extract the "weak signals", possible clues of a very serious attack that will only be implemented months or years later. We shall never forget the December 2015 attack on the Ivano-Frankivsk power plant, in Ukraine, which began one and a half years before the deadly hack, with "trivial" operations on the social networks and smartphone apps used by employees, managers, suppliers, etc.).

As many specialists pointed out, the "robots" are already in use within the military system. As such, they are already part of the assault arsenal used on today's battlefields (Afghanistan, Syria) by American and Russian armies. But no army intends to use robots instead of soldiers. All the prototypes tested by the *United States Army* and *Вооружённые силы Российской Федерациии* were found to be unable to distinguish friend from foe in modern wars, which are now all hybrid, and even worse, in an urban context with poor visibility (sand dust in particular), they are unable to distinguish between a civilian holding a rock and a terrorist holding a grenade. The two armies have expressed themselves, the first through the spokesman of DARPA and the other directly through President Putin. Yet they have, however, chosen two different options: the Pentagon, after catastrophic tests, has refused (officially) to continue to support research on *"autonomous robot killers"* - but in the same time, it has entered a very loud "verbal war" with China on who will have the first robotic battalion (Times, 13 November 2019: *China and the U.S Are Fighting a Major Battle Over Killer Robots and the Future of AI)*. Moscow, which has had great success in Syria with semi-autonomous mini-tanks (remote-controlled but with AI programs) for demining fields (Uran 6) or, equipped with heavy artillery (Uran 9), advancing in the frontline at a safe distance from infantry, wants to equip itself with mass produced prototypes to be used exclusively on a presidential order and only in a war between robots. A metaphor meaning a terrestrial war between superpowers (local, regional or total) (Interfax, 22 November 2019: *Путин велел увеличить количество боевых роботов и лазерного оружия)*.

Syria: the Russian robot «Uran-6» (anti-landmine) in action.

Why a break would be mandatory?

It is Professor Baldwin himself who reveals with due academic seriousness that we live the opposite of any progress. Not only does he write that *"the problem lies in the inhuman speed of change, or more precisely, in the confusion between the speed of destruction of jobs and the very slow creation of new jobs"* (p. 187). Worse, he points out that thanks to the "globotics", associated with the weight and implication of GAFAM, that ***"Job destruction IS the Business Model",*** the very title of the chapter following the quote.

The book's conclusions - and its heavy unspoken ones - are more than worrying. The author modestly states that, being a non-specialist he expects a political, sociological, anthropological, and an compulsory regulation model before celebrating "globotics" progression.

In fact, citing almost one hundred different sources, Baldwin places the creation of a socio-community model based on the flexibility of employees to change city, region or country and also on the willingness to learn a new job as a condition *sine qua non* for the implementation of "globotics".

The author also cites the example of Danish *"flexicurity"* which is based not on the defence of the workplace but on the employment of a citizen. Such a model would not only be impossible to adopt in countries such as the United Kingdom (in Denmark, changing job locations does not imply changing home, given the quality and speed of public transport) but it would also be incompatible with social security models such as the unemployment ones enforced in 80% of EU member states. Lack of if any training support is just one factor Denmark – through massive private aid – which guarantees this through a positive change in category of work and employment sector.

In France, where justice has not yet given its verdict on the Amazon case, President Emanuel Macron has concluded an agreement with the GAFAM giant allowing him to extend his presence, following an agreement with President Donald Trump on an *ad minimam* taxation of the GAFAM (but not of the robots as Bill Gates had long hoped).

Now, many reports by different teams working at the CNRS (National Scientific Research Centre) have shown that every workplace generated by Amazon suppresses 2.8 jobs in other companies.

The reality would be more than the 5 jobs lost for 1 created by Amazon if there were no *"road slaves"* (literal translation). Amazon's policy in France has been to choose areas not far from large motorway networks but with a high unemployment rate.

And this is how the archaeological and natural reserve of the Pont-du-Gard finds itself with a level of fine particles equal to that of a metropolis: for a mega storehouse, which created only 220 jobs (i.e. 70 x 3 shifts x 7 days), the concerned municipalities, province and region had to invest 6.6 million euros to create new road networks allowing a rapid connection from the motorway to the storehouse, where hundreds of lorries and smaller trucks are unloading and loading merchandises every day. With the new storehouses already planned or under construction, again according to CNRS reports, France will have to buy an additional 12% of CO2 emissions from other countries as soon as 2021, those additional emissions resulting from the increase in road freight traffic *exclusively* generated by the GAFAM giant's warehouses.

In addition to ecology, there is one last aspect that is far to be convincing: the model proposed by Baldwin is mainly based on the creation of new *"job types"* of a communitarian and local use based on ethics, empathy, heart and skills (according to Baldwin, these are more equally distributed qualities than knowledge and experience). These will have to replace the old CVs based on work skills and university *curricula* – which I consider to be archaic based on my professional experience. Now if we are convinced of the truthfulness of the expression *"mens sana in corpore sano"* we cannot imagine heart and empathy without mind as a *"job requirement"*.

"Mens sana in corpore sano ***cum cordam****"* would be the right measure. But to have a *mens sana* requires all the experience and knowledge that Baldwin considers totally useless because it will be surpassed by the knowledge of AI. This wishful thinking has also another reality to face: because of the ignorance and lack of general culture one can notice, in a our increasingly individualistic societies, empathy is abandoned in favour of another expression of the "heart": hatred and violence. Justified as they are "serving" a "noble cause", as in the riots we have been observing for several months now in the United States.

From historically pacifist and cultured groups, as the defenders of minorities or groups promoting a firm condemnation - but anchored in its historical contextualisation - of the horrors of slavery, we have moved on to vandalistic destruction and urban guerrilla warfare with the *LGBT/ Black Life Matters/ Antifa* "motivation"...

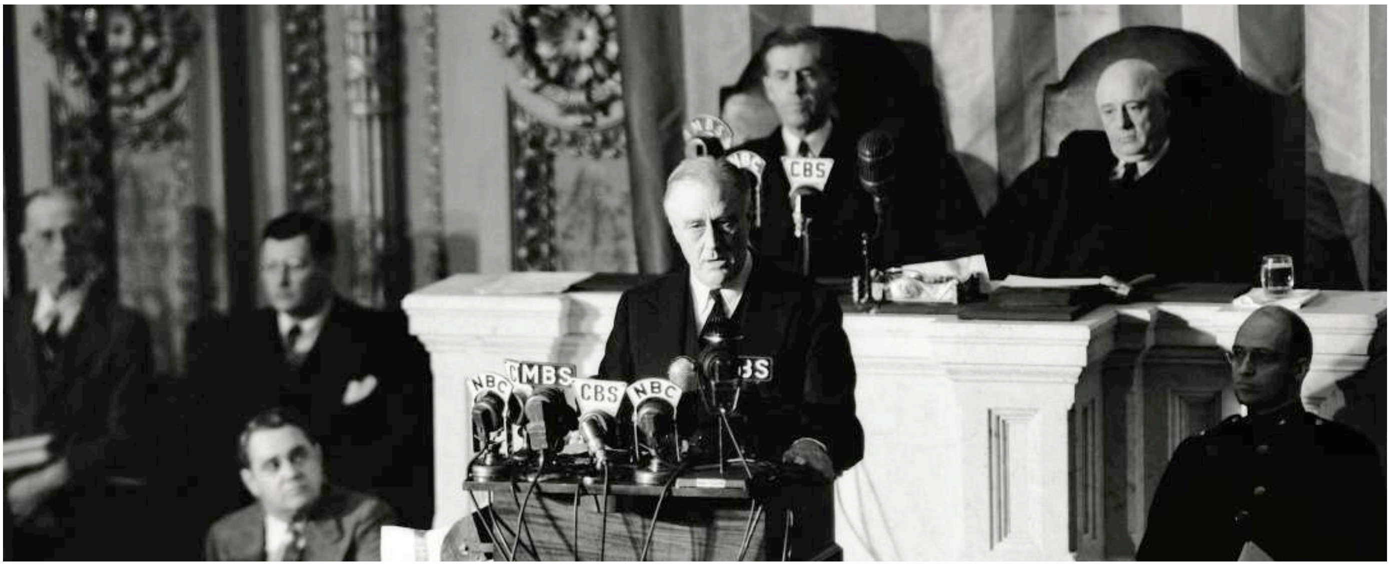
GAFAM are finishing the killing, beyond culture and history, of free will, which is based on the knowledge of FACTS, the only one that allows to have a DEBATE on their interpretation.

Let's not allow them to make us believe that with the HEART we will find a job stolen by a robot or a hundred algorithms... the same ones that have already stolen democracy in 42 elections in as many countries as for today.

In *Mapping European Attitudes to Technological Change and its Governance 2020*, by Carl Benedikt Frey, director of the University of Oxford's *Future of Work* programme, Frey has no doubt about the fact that *"regulating or not, there will be a full-speed* ***backlash****"*. He emphasises: **"When automation accelerates during a downturn, a techlash is likely to follow".**

To recall a famous phrase of President Franklin Delano Roosevelt extracted from his State of The Union speech held on January 3, 1940, after the beginning of WW2 in Europe and Asia: ***"To face the task of finding jobs faster than invention can take them away - (this) is not defeatism".*** This a year before Pearl Harbour, we see the destruction of employment by technology was already highly topical... ■

[1] (European Tech Insights, Center for the Governance of Change: www.ie.edu)



I trust you... NOT - The rise of Zero Trust

Author: Marco Essomba

If you have come across it recently, you would probably know that Zero Trust is relatively a new approach that is trending in the security world. Depending on who you speak to, it has different connotations as it rapidly evolves creating its own sub-culture.

In my opinion, it is an important security principle, but we must strip away the buzzwords around it to really understand how it applies to organisations.

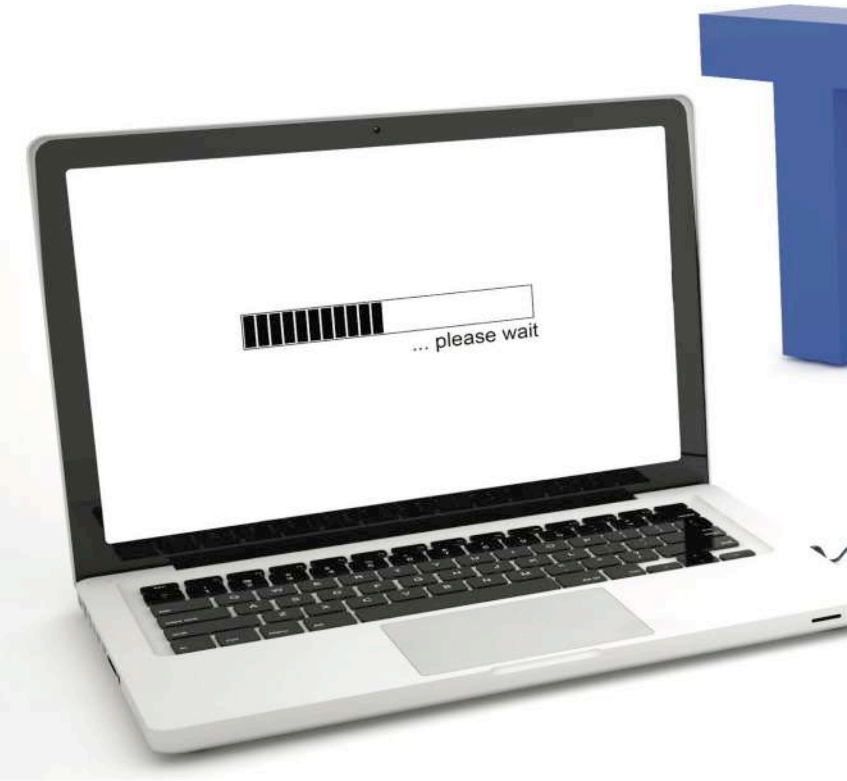
At its core, what is Zero Trust?

According to the National Cyber Security Centre (NCSC), Zero Trust is a new approach to network design that looks to remove inherent trust from the network by treating it as hostile and instead gain confidence that you can trust a connection.

Simply put it follows an 'assume breach' belief to help prevent data breaches in an organisation. According to this approach, 'Trust' is a security vulnerability. So, where the traditional security assumes that everyone inside the organisation can be trusted, Zero Trust mandates that no-one is to be trusted until proven otherwise.

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



For some, this may be a hard concept to accept, but as leaders responsible for security in an organisation how can we assume that our internal team's identities are not compromised and that all teams act responsibly and can be trusted at all times?

We must be prepared to defend against threat actors and malicious insiders who are looking to stealthily infiltrate networks, exfiltrate data and wreak havoc on organisations.

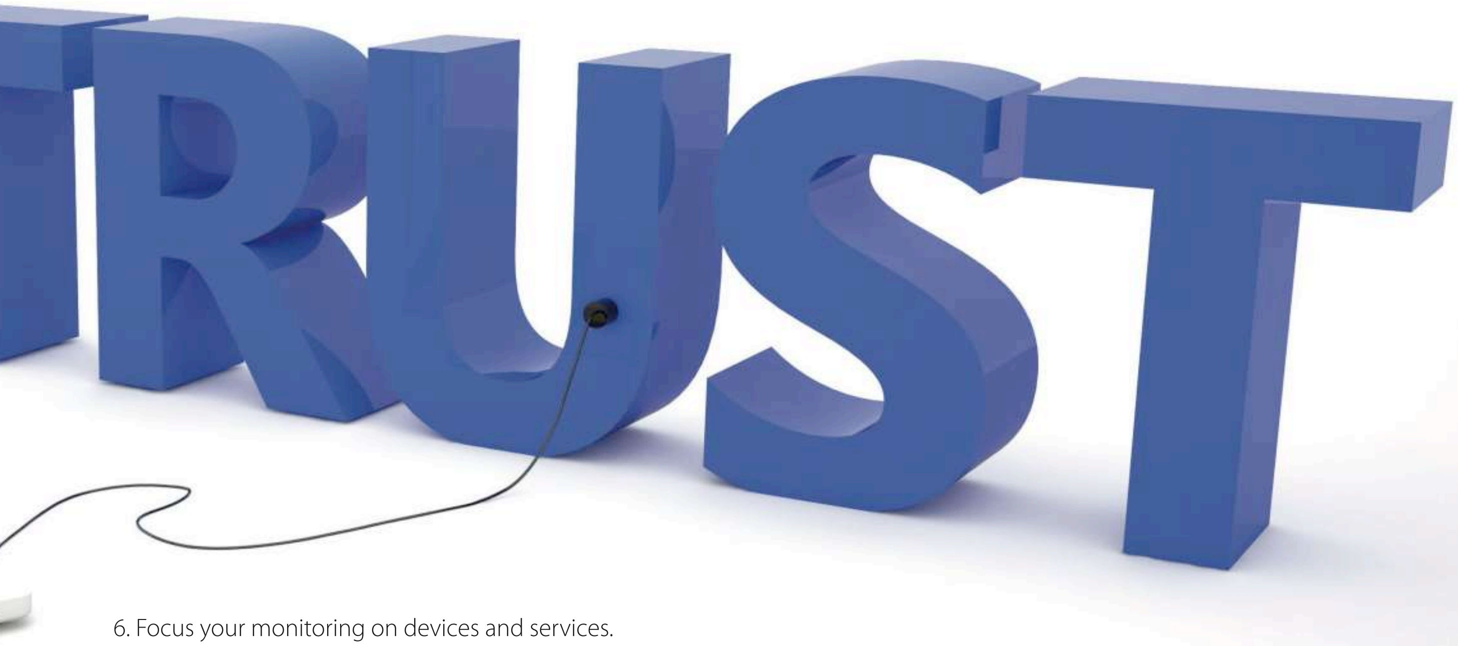
Getting started with Zero Trust

Bear in mind, Zero Trust is not about 'protecting it with new technology'. Often, we will see talk of next-level multi factor authentications, advanced identity management systems, end-point protection and environment micro-segmentations as solutions.

However, we cannot fix this issue by using the latest security solution or get it up and running in an instant. First and foremost, it is a mindset. Legacy IT systems and IT teams are inherently designed to trust their own environments. Teams have to start thinking in a new manner.

For an organisation looking to get started, the NCSC's Zero Trust Architecture (ZTA) design principles is an excellent guide. They are:

1. Know your architecture including users, devices and services.
2. Create a single strong user identity.
3. Create a strong device identity.
4. Authenticate everywhere.
5. Know the health of your devices and services.



6. Focus your monitoring on devices and services.
7. Set policies according to the value of the service or data.
8. Control access to your services and data.
9. Don't trust the network, including the local network.
10. Choose the services designed for Zero Trust.

It starts at the top

Zero Trust is a huge advancement for Information Security (InfoSec) as a whole and business boards should fully embrace this as part of their digital and security transformation strategy. A big part of this should be implemented alongside any cloud adoption or migration especially with more users going mobile or working remotely.

As always, implementing the Zero Trust model in an organisation will be an on-going process but we must move from talking about it to taking action.

If we always assume breach, could this have stopped Edward Snowden? ■

StressSec is a pandemic that is killing our SMEs

Author: Raj Meghani

'StressSec' is my coined term for being burned out by organisational cybersecurity demands, requirements and fire-fighting in the remote world.

This past year, the world has acknowledged that remote workers are constantly prone to high levels of stress and feeling of being physically and mentally drained due to navigating between technology and applications whether through emails, communication apps or video meetings. This results in loss of productivity in the organisation.

Now take this stress, multiply it by 5 and add it to a solo CISO, CTO, IT Director or a skeleton team of security personnel at an SME and we get 'StressSec'.

Imagine carrying the weight of cybersecurity on your shoulders in a remote world where you are constantly worrying of teams:

- .... clicking a phishing link
- .... falling for a spoofed email attachment
- .... using their credentials on a fake website
- .... not implementing strong passwords or 2FAs
- .... not patching, updating devices or using secure configurations
- ..... leaving end-points unprotected

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

The list goes on and on.

We hear this often from security peers and clients across the SME industry. AI launched attacks, next level ransomware threats, deep-fake phishing to possibly facing heavy regulatory fines in the event of a data breach. It all feels like an uphill battle to keep on top of security at all times.

Enterprise security teams can afford more resources but their counterparts at SMEs have to work with limited resources (Often IT management see is as a part time responsibility as they are individuals wearing multiple hats), constrained budgets, growing internal pressures, mounting workload and be on call 24/7. They also have to ensure new technologies are rolled out quickly - this leaves them almost no room to vet a new technology for vulnerabilities versus being labelled as a barrier for digital transformation in an organisation for taking too long. It is not a wonder why, according to reports, the average job tenure of a CISO is just 18-24 months when you compare it to the average of 5 to 8+ years on the job for other C-suites in the organisation such as the CEO and CFO.

When your Security and IT teams are stressed-out and possibly thinking of quitting or inadvertently letting their guard down due to burnout, we are all at risk.

SMEs need to bridge the gap between Security and Business *urgently.*

Let us agree that no team can be everywhere at all times.

Let us agree that SMEs will continue to grow, scale and rapidly adapt new technologies in order to reach new audiences, tackle competition and disrupt the market.

However, we also recognise that security has to be everywhere – 24/7/365. Increasingly, more security technology is thrown at the rising number of threats, but this adds to more disparate solutions in the organisation that again adds to the mounting workload that teams have to monitor and manage.

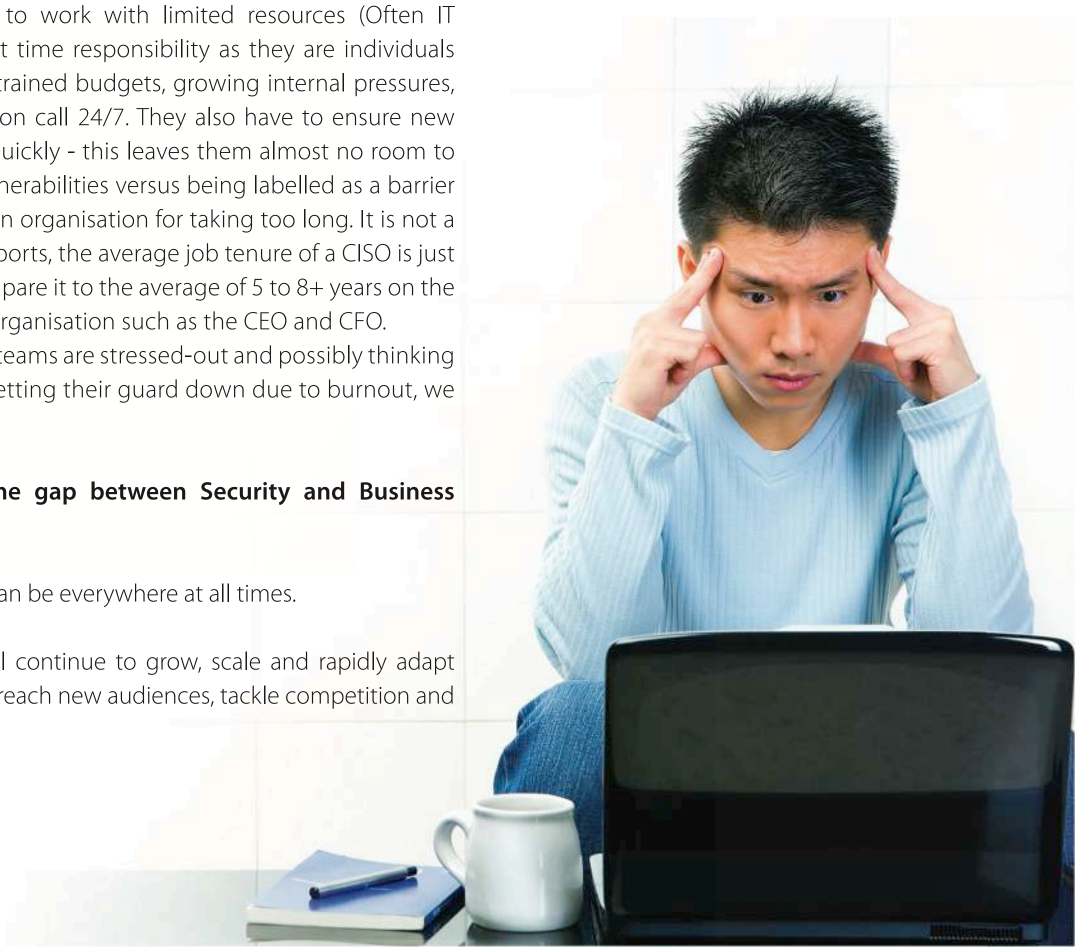
Let us agree that just adds to the many pressures already facing SMEs.

Solutions such as training and automation can impact the whole organisation positively. Implementing automation, particularly within the security environment, means teams can respond to threats and incidents with confidence through automated workflow processes/ playbooks.

Let us agree that "StressSec" is a pandemic in the making in its own right that is killing SMEs. One that we need to eradicate and bury before it spreads at an uncontrollable rate.

The goal is to reduce levels of StressSec so SMEs can focus on building and futureproofing their businesses.

Granted – it's more easily said than done. But we have made it our mission to raise awareness, educate and help SMEs win this contagious battle. ■



Smart Cities - Expectations *vs.* Reality

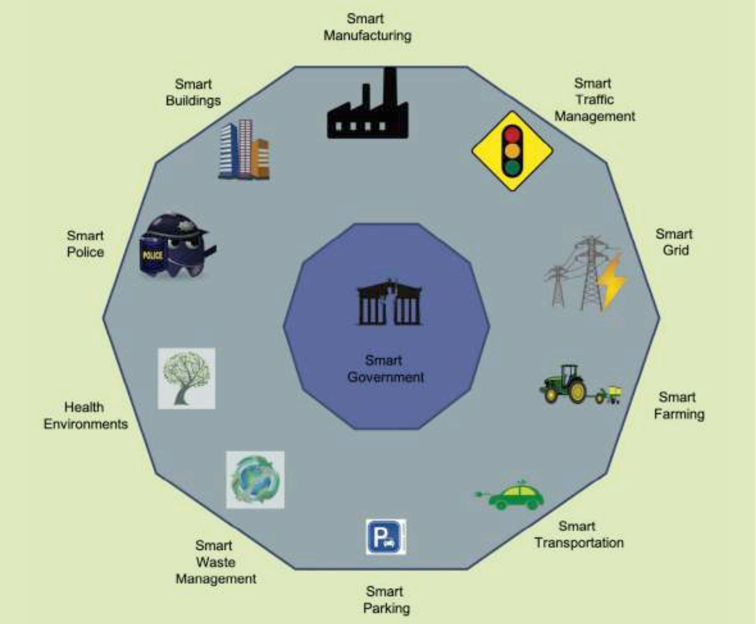
Authors: Raj Meghani & Marco Essomba

By now, it is commonplace knowledge that Big Data & IoT will drive Smart Cities. But what does Smart City mean to you?

Smart City concepts are often accompanied by buzzwords and showcased as cyber-futuristic utopias where everything is possible via AI, robotics and hyper-connectivity. Flying cars to transport you, drones to deliver your packages and hologram based communication devices for immersive interactions are examples of what has been presented.

These are advanced expectations and no doubt some of it will become a reality in the future. But we are here to take a pragmatic view of Smart Cities as they are now, particularly on how it helps residents and also raise the point that one individual's smart city life may not be comparable to another individual as the experience is deeply rooted to their own nation's goals as well as the geographical location.

Currently, Governments around the world are pacing to integrate technology into just about every part of its city's infrastructure and operations. Over time we will see technology combined into every part of our daily lives whether through utilities, mobilities or services. As it is greatly software driven, global technology giants such as Cisco and Microsoft will play a big role in bringing these cities to life.



These are some key areas which Governments will typically look into making smarter:

- Public transportation
- Urban mobility
- CCTV security
- IT connectivity
- Water
- Power supply
- Sanitation
- Waste Management
- E-Governance
- Resident participation

Here are some examples of how cities are becoming smarter but interesting to note their areas of focus differs based on their own objectives.

Singapore's focus on maintaining a clean city

A great example of how big data is being used by the Government to keep the city clean and improve daily living. The Singaporean authorities have deployed systems that can detect when people are smoking in non-smoking areas or littering from city high-rises.

They do this by using cameras around the city and converting these visual feeds into usable data. This enables them to observe in real-time various aspects like crowd density, cleanliness and vehicle movements. Sounding a bit like Big Brother? Maybe so. But this also

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

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

means they can deploy rescue operations into crowded hotspots in an event of a fire or other hazards around the city.

Dubai's focus on delivering Smart E-Government Services

The Smart Dubai initiative has already seen 50+ digital services rolled out across multiple Government entities. Their focus is on integrating multiple services via their Dubai Now application as a centralised point of service and information hub for citizens.

The application allows citizens to pay speeding fines, pay utility bills, tax vehicles, route packages, hire a taxi, track visa status, contact authorities and much more. This improves efficiency for residents and reduces strain on government bodies when it comes to delivering services physically. Here we see examples of collaboration and integration work in true harmony.

Barcelona's focus on energy-saving technology

Barcelona has invested in public and roadway lighting that adapts to activity by dimming and brightening up as needed using advanced motion detect sensors. They have also launched a real-time Smart Parking application that informs drivers of free parking spots across the city. Parking spots use metal detectors and curb lighting to determine if the spot is free or occupied. That is truly smart at the height of an individual's driving experience.

Furthermore, Barcelona has an automated tunnel based waste collection solution that eliminates the need for garbage trucks and thus reducing noise pollution and odour while keeping costs down.

What about London?

London's scale - 33 local authorities, more than 40 NHS Trusts, large regeneration opportunity areas and major public agencies like TfL and the Met serving a population of nine million citizens - presents a tremendous opportunity to 'test-bed' SMART city ideas.

Smarter London Together was launched by the Mayor of London in 2018 and can be classified into 5 mission areas of focus:

- More user-designed services
- Strike a new deal for city data
- World-class connectivity and smarter streets
- Enhance digital leadership and skills
- Improve city-wide collaboration

Current smart city resources within London include City Hall's London Datastore, which holds over 700 sets of big data that help address urban challenges and improve public services, and the rise in cashless payment methods for transport. London may appear to be playing catch up with the likes of Singapore and Dubai, but we say – watch this space.

Smart Cities will be an evolution of processes

As you can see, Smart Cities are already here and these cities across the globe have different interpretations of what makes cities smarter. It is also dependent on technology and investment availability as transforming cities will initially come at a huge price tag. Eventually, the benefits will outweigh the investments costs. However, we can expect to see these changes in layers. This is why we see some cities more advanced than others.

As residents, we will slowly adapt and rely on these technologies without realisation.

New innovations will replace existing practices as an on-going process. A new way of building and living is already underway.

The next few years will see an exponential increase in the emergence of truly integrated technologies that can sit at the heart of a city's infrastructure.

Just don't expect a big unveiling of a floating city in the sky. And that is the expectations versus reality when it comes to Smart Cities. We must focus on what is practical and beneficial for people and the environment now and keep one eye firmly open on what the future holds. ■

A tetralogy for a mature information society

Author: **Massimiliano Cannata**

Introduction *by Laurent Chrzanovski*

World-known Professor Luciano Floridi (Professor of Philosophy and Ethics of Information at the University of Oxford) is achieving the last part of his milestone research (four volumes introduced by two further books, all published by Oxford University Press) on understanding the information world, also named *"infosphere".*

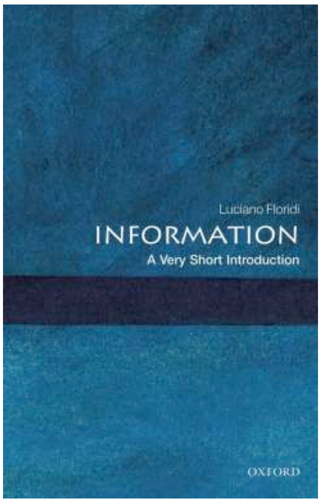
Prof. Luciano Floridi.
Photo: courtesy of Arthur Bullard

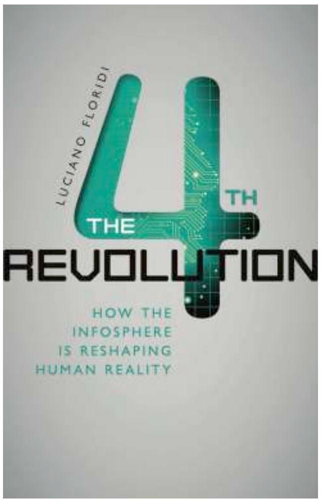
The scholar perfectly explains his *"research on the nature, dynamics, and uses of information"* and how his achievements led to the publication of a *"Tetralogy on The Foundations of the Philosophy of Information (Principia Philosophiae Informationis)"* on the scheme published on his website (www.philosophyofinformation.net/research/), as shown hereunder.

With the English version of his latest book to follow, this article focuses on the translated review by Massimiliano Cannata.

For English-readers desiring to know more, there are plenty of recent interviews with Prof. Floridi on the topic of the last *opus* (1), more crucial than ever as it deals with the politics of information, a subject which makes daily headlines not only in general media but also in technological, strategic, humanistic, philosophical and even military top academic journals.

In addition, you can hear the author's key views, in a keynote delivered at the 2017 University of Melbourne's Networked Society Symposium: "The Green and the Blue" (2), and, with the same title, in a scientific article published last year in Oxford University's *Yearbook of the Digital Ethics Lab* (3).





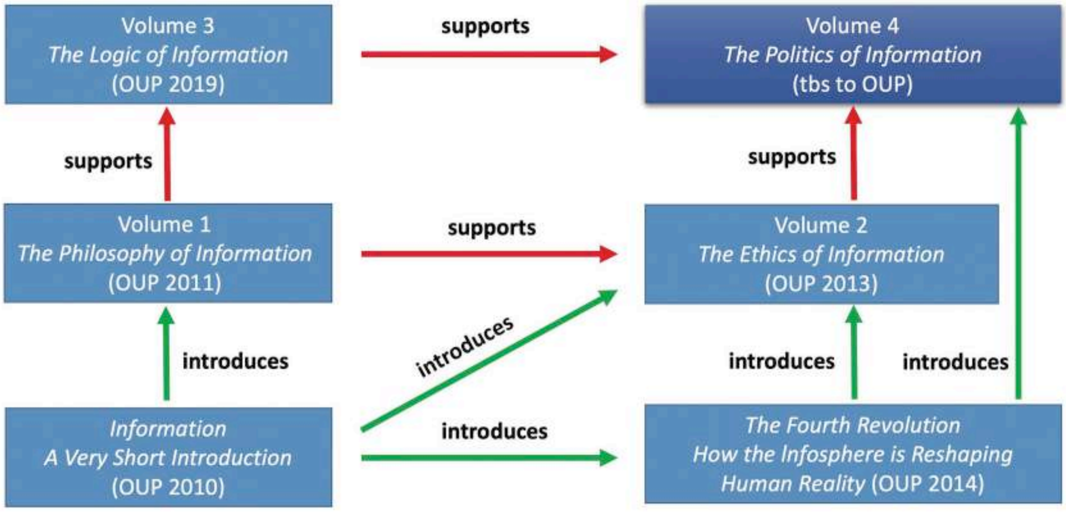
(1) We can recommend the interviews of Prof. Floridi made by Davide Perillo for ENI and Maciej Chojnowski for Artificial Intelligence / Sztuczna Inteligencja) at the following URLs:

https://www.eni.com/en-IT/global-energy-scenarios/luciano-floridi-technological-gambit.html

https://www.sztucznainteligencja.org.pl/en/luciano-floridi-to-me-the-green-and-the-blue-is-the-plan/

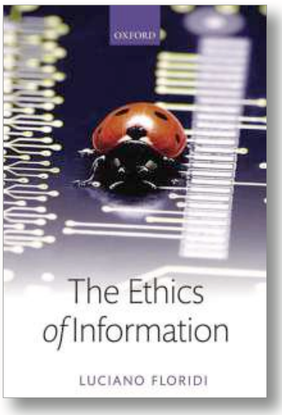
(2) Luciano Floridi, "The Green and the Blue", original speech held at the 2017 University of Melbourne's Networked Society Symposium (1h03): https://soundcloud.com/networkedsociety/floridi-keynote-nss17

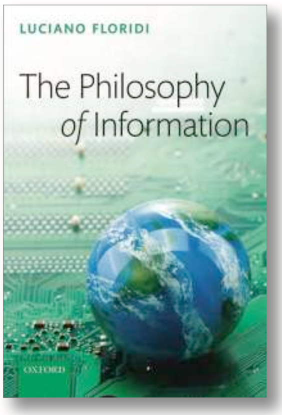
(3) Luciano Floridi, The Green and the Blue: Naïve Ideas to Improve Politics in a Mature Information Society, in The 2018 Yearbook of the Digital Ethics Lab, Oxford 2019, pp. 183-221.

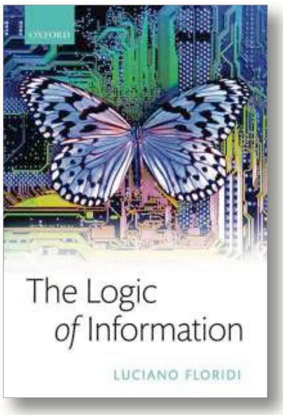


Reconstitution (L.C.) of Prof. Floridi's scheme

Literary Review







LUCIANO FLORIDI
il verde e il blu
Idee ingenue per migliorare la politica
Raffaello Cortina Editore

The green and the blue, the achievement of an immense research publication project

"Il verde e il blu" (ed. Raffaello Cortina, Milano, May 2020) by Luciano Floridi is an essay inspired by a precise aim: to offer "naive" ideas (the author's clarification has the appreciable taste of Socratic *"learned ignorance"*) to improve politics, in order to revise the foundations of democracy, with a view to creating credible premises for the construction of a mature information society.

To better understand the discussion it is certainly useful to consider previous writings by the same author - *"The fourth revolution"* and *"The logic of Information"*. The former addresses the economic, social and cultural implications of the paradigm shift from analogue to digital. Real and virtual, the underlying thesis of the book, are categories of being that can no longer be separated. The world in which we live is the result of the dense contamination between these two areas.

Such a clear "leap" forward needs a philosophy to be explained. Philosophy, in the context of systematic thinking to understand the very nature of information, to predict and manage the ethical impact of ICT on us and our environment, to improve the dynamics of *web society* development and, last but not least, to identify a path of meaning in the wake of a globalisation marked by many contradictions.

"Thinking of the infosphere" gives strength and dignity to "useful" speculation, free from the useless trappings of erudition, to the identification of practicable solutions by humanity. What follows takes on the innovative contours of conceptual design. This vision of the world is grafted into the last work: ***"The green and the blue / Il verde e il blu".*** Through these colour-concepts, an itinerary of transformation of society unfolds.

The book is built on one basic trust: there is "good politics" and is admirable for its synthesis of different visions, needs and ideological positions. But trust is not enough. The failures of the present impose a change of gear, an authentic renewal of the parties, and of the way of exercising democracy. *"The mistake,"* explains the author, *"is to think of acting from within a mechanism that has broken down. One must not improve politics in politics, but work for politics, an objective that can be achieved if we raise citizens' expectations. Let's not settle for a fixed price menu thinking that there is only one restaurant in the country, but let's oblige those in power to enrich their offer with transparency, quality and commitment".*

Why we must know how to take care of the world

The human project that Floridi has in mind is of vast proportions, and for this reason he dedicates an entire chapter of the book questioning the entire vocabulary of science and philosophy of politics: democracy, state, public administration, sovereignty, environment, justice, solidarity and citizenship. The prerequisite for what appears to be a "cyclopean" work of transformation, especially if it is tackled without the right cultural and professional tools, lies in the ability/willingness to go back to elaborating long-term strategies, an ability that seems to have been lost by the elites for too long. To put it in a nutshell: short-sightedness cannot be admitted when the fundamentals of the social contract in all its articulations have to be put into action.

The author often uses simple metaphors to convey complex messages. In this case he resorts to music: *"It is necessary to give the"* la *"to our rulers - just as one does with an orchestra - so that they start playing with the right harmony. In concrete terms, this means seriously starting to take care of the social, political, physical, geographical and technological environment that surrounds us. My idea of green has a very wide meaning. When I speak of blue, my attention is on those instruments of technology that are changing our lives: the Net, 5G, artificial intelligence, social platforms, increasingly sophisticated smartphones...".*

A good starting point lies in the radical change of perspective we need to adopt. "The party is no longer for us, the world is not at our disposal, we must adopt - this is one of the strong thesis of the book - a decentralisation of the ego, in order to rediscover the dimension of the other". This is not only a demanding epistemological turning point, but rather a structural change that invests work and the productive sector from the very foundations. We could call it the "economy of experience", centered on services, the quality of what we do rather than quantity, a quality that must be negotiated in constant dialogue with the citizen, user or consumer. It is clear that in order to align with these different dynamics it will be necessary to modify the organisational structure and the way of doing business. *"For me, being in the 21st century means adopting a different point of view from a past based on the exploitation of the ecosystem, greed and ignorance. Those who have not understood where we are going - are not capable of living the present, let alone being able to govern it".*

Experience and design, therefore, will be the codes of an ethical capitalism, oriented to the satisfaction of needs, open and inclusive, which has nothing to do with what we have nurtured over time of the "industrial modernity" that has brought the earth and those who live on it to extremes.

The "daughter" writing of a suffering planet

Floridi's points are emphasised by a planet wounded in consciousness, and today even more exhausted in the body by the pandemic. The disease that has spared no corner of the globe is, in fact, the last alarm that should lead us to understand that we must change our ways. *"Companies and institutions should understand that digital is not the icing on the cake but the whole cake, just as green is not a cost but a necessary investment without which it will be impossible to sustain the pace of transformation of the contemporary world".*

On this ground the "human project" takes shape, the proposal that is the beating heart around which the book revolves. To give concrete effect to the idea it will be necessary to combine "individual and totality", to respect the subjects without forgetting the society of which they are part. A difficult synthesis by the author's own admission, but absolutely necessary. The "isms" have had their day. The individualism that dominated the second half of the twentieth century as a reaction to totalitarianism is no longer sufficient. The leg of individual rights must be associated with the second important leg of social rights. The crisis of the UN and the difficulties of Europe are indicators, which require a high level of coordination (another important thesis of the essay),otherwise there is a fear we will never get out of the depression into which we have fallen.

In *"Politics has no logout"* (see thesis 77 p. 243) Floridi affirms a convinced Europeanism, because epochal problems such as social justice, increasing poverty, inequality, minority rights, global warming, air pollution, regulation of migration flows do not admit limited and partial solutions. The "five hundred" has come to a halt, it must be pushed together, not just one who turns the key. *"When we start using words like people, nation, race, the individual remains crushed, with good peace of liberty rights costing years of struggle and sacrifices".*

The time has come to move from the "social contract to the universal trust". This *"quantum leap"* can help us to perceive the planet as a legacy received, to be cared for and left to future generations in conditions of high health and liveability. The rigid certainty that everything can be resolved in a contract is linked to a mythology and a narrative that has no repercussions in everyday life. Each of us is born in particular circumstances, is "thrown" into the world, and must therefore feel respect for the ecosystem.

We are always within the perimeter of the inheritance (the trust) that we have received as a gift, being born in the richest part of the world. We must not squander it, rather we must show talent and intelligence, we must try to deserve a *"loan of honour"* that the state must assign to young people, knowing that it can recover with interest all that is spent to promote the capital of wits. Here the reversal of the current trend could not be more clear-cut. Citizenship, besides being a fundamental right, is a patrimony that must be made profitable, which can return to the deficit turnover of any company. ■

A publication

web for business
swiss webacademy

edited by:

BLOCKAPT

Copyright:
Copyright © 2020
Swiss WebAcademy and BlockAPT.
All rights reserved.

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

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

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

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

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

5th anniversary VIP interviews

It was June 2013. During a privileged personal meeting with the Secretary-General of the International Telecommunications Union (UN-Geneva), then Dr. Hamadoun I. Touré, His Excellency asked us to consider the possibility of organising a Central-European Public-Private Dialogue Networking Platform, duly technically assisted and logistically helped, during its launching years, by the ITU's Europe and Cybersecurity departments.

Three months later, in September 2013, the Romanian-based NGO Swiss Webacademy launched the 1st edition of "Cybersecurity Dialogues - Romania" in the medieval and baroque city of Sibiu.

The Sibiu-based 2-days conference had such high success in the quality and number of VIP attendees that the ITU reported it in 2015 as the *"best practice example for the European continent".* This extremely rare distinction motivated many Western and Southern EU institutions and private entities the ask us to reproduce and adapt the congress to the specific needs of their ecosystems congress. In 2017, the Mediterranean and the Western European versions of "Cybersecurity Dialogues" were successfully launched, in Italy and in Switzerland (www.cybersecurity-dialogues.org).

Meanwhile, in early February 2015, the ITU's cybersecurity department asked us to examine the possibility to offer to the broadest audience possible a regular publication based on the congress' core concepts: enriching dialogues and VIP points of views from different states and sectors, in a crystal-clear, non-vendor and non-technical style.

Cybersecurity
Trends
Nr. 1 / 2015
Tendințe în criminalitatea informatică
Cooperare pentru securitate cibernetică
Tendințe de securitate cibernetică în România
Cover Story
HEALTH

One week later, we were sipping a coffee together in Bucharest with our late friend Romulus Maier, our best media partner. We remember this moment as if it was yesterday. Romulus, switching to our long and passionate debates, came back to a telegraphic style he used only when it came to very, very hard challenges: *"Well, let's do it. First edition next month".* No pressure then…!

In March 2015, the 1st edition of our free quarterly awareness journal, "Cybersecurity Trends", was printed and set online. Two years later, the ITU as well as number of our International partners asked us to publish the journal in versions adapted to the different European ecosystems and languages. In March 2017, "Cybersecurity Trends" was launched in its Italian, English and French versions.

INTERVIEWS

Commemorating the 5th anniversary of the journal, our December Romanian edition will be made with 70 identically structured interviews, answered by established VIPs who are active in different fields of security in over fifteen countries.

The concept we desired is radically different if compared to our traditional "VIP interviews", as it is aimed to offer to the readers a small insight into the personal personality and the thoughts of each VIP.

The first topic, of course, given none of them belong to the "digitally born generation", was why did each one choose to work in in cybersecurity?

Moreover, after so many years of activity, what do they think we missed in the field of cybersecurity awareness in the last decade and what should we do in the next decade?

Then, following our own professional curriculum, we chose to ask them to "materialise" the digital world. If this world was a book, a piece of art, a musical composition, a primordial element, which one should it be?

The beautiful and eclectic "painting gallery" at the end of the interviews is probably the most interesting achievement of this fascinating exercise. From fear to joy, from ideal but empty cities to abstract works, security specialists reveal a tiny part of their emotional vision of this daily-changing technological sphere which now encompasses all the moments of our life.

We highly recommend you admire each masterwork listed, while listening to the piece of music chosen by the respective VIP.

We are convinced that the answers, even if short, as well as the book references, will give each reader a lot food for thought, and a privileged, unique opportunity to know a tiny part of the **HUMAN** lying behind the very skilled professional you may already know in person or by reputation.

Thanks to Marco Essomba and to Raj Meghani, we include in this edition, the first set of twelve interviews, answered by some of the most influential and respected people we had the privilege of meeting in our previous congresses. They are truly "representatives" of many different countries and sectors of activity.

We would like to end this special introduction by thanking all our interviewees. In the very specific defence sector, many declined our invitation as they considered that many questions reached "too personal" aspects. Those who honoured us by accepting their involvement have demonstrated their trust and belief in our journal. In consequence, last but not least, we have to reproduce the disclaimer everyone requested:

Every answer reported in the following interviews is only the interviewee's personal point of view. None of the interviews reflect in any shape or form the opinions of the institution or the company the interviewee works for. ■

VIP Biographies

GEN. ANTON ROG

Director of the National CYBERINT Centre of the
Romanian Intelligence Service (SRI)

Brigadier General Anton Rog leads the CYBERINT Centre, which is the responsible institution for a 24/7 proactive detecting, analyze and countering malware against systems and networks critical for Romania's national security. Within the SRI, Anton Rog previously held several technical development positions including software and systems design. He also worked as a deputy director inside the Central IT&C Department of the SRI. He is active with the academic community as Associate Professor at DRESMARA (Regional Department of Studies For the Management of Defense Resources) in Brasov. Anton Rog graduated from the University of Bucharest in 1998 with a B.S. in computer science and has achieved in 2011 at DRESMARA a postgraduate diploma in "Program and Project Management." He received the the "Order Manhood and Faith" award (Knight) in 2014 and the "Order of Military Virtue" (Knight) in 2005, by two different Presidents of Romania.

DAVIDE FANIA

Managing Director,
XTN Cognitive Security

At the beginning, I was an Analyst Programmer, Application Specialist and Project Manager in a wide variety of business applications. Particularly specialized in Production & Planning solutions. Over the past 15 years, I've created and led some private organizations that initiated breakthroughs in areas as diverse as computer software for textile, food and biomedical markets. I'm one of the pioneers who created, installed and improved the automation system for specimen processing named WASP (www. copanitalia.com) I created the LIS (Laboratory Information System) Interface connector Architecture (UIC™ - Universal Interface Connector) necessary to updload and download patient and specimen data from/to Hospital & Laboratories Management Software. I'm the inventor of MALDItrace system (now Colony Picker for WASPLab automated system), a patented equipment created for specimen and organism's traceability in mass spectrometry.

DIDIER SPELLA

Co-founder and Manager,
Charentes-Maritime Cyber Sécurité

A former senior officer of the French Air Force, President of Mirat Di Neride, co-Founder of the PPP congress Charente-Maritime Cyber Security, Didier Spella is an expert in corporate strategy and cybercrime, head of the CLUSIR - Nouvelle Aquitaine Ouest Office - He has studied the evolution of the different concepts governing today. His knowledge of both analogic and digital security, his experience in risk analysis and his expertise with USA companies have enabled him to position himself as an expert in defining security strategies. Observing and monitoring the cyberattacks that became more and more dangerous and intrusive in our lifestyles, he focuses specifically on the risks incurred by the general population and in particular the threats faced by VSEs and SMEs.

DOTAN SAGI

Co-CEO, Lotan Group International;
Founder and Manager, BeST.

Dotan is a Managing Partner of the Lotan Group and a veteran of managing war games as part of risk management for governmental and commercial entities around the world. He has been part of the team designing the use of computerised platforms for crisis simulations with an emphasis on the aviation and financial sectors. With more than 15 years in the field of crisis management and multiple war-gaming projects, Dotan has led many organisations through an effective and efficient process to achieve their goals.

IONUȚ STOICA

Cybercrime Training Officer within the European Union Agency for Law Enforcement Training (CEPOL).

Before joininng the CEPOL, Ionuț was a Senior Project Officer, within the Council of Europe - Office for the Fight against Computer Crime (C-PROC), having responsibilities in the field of implementation of program of assistance to developing states in terms of strengthening the capacities to prevent and combat cybercrime. He is a graduate of the Faculty of Law of the A.I.Cuza Police Academy, of the Faculty of Communication and Public Relations of the National School of Political and Administrative Studies, and he holds a master's degree in Management of International Police Cooperation, having numerous certifications in the field of prevention and combating computer fraud. He has more than 12 years of experience in the field of combating cybercrime, previously holding the position of head of the Office for Combating Information Fraud and those with Electronic Payment Means of the General Inspectorate of the Romanian Police.

LUCA TENZI

Corporate security and security convergence expert.
Organisation Resilience consultant for the International Atomic Energy Agency

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 financial 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).

MARCO ESSOMBA

Founder & CTO, BlockAPT

Marco Essomba is the Founder & CTO of BlockAPT – a UK based innovative cybersecurity company. An influential thought leader in cybersecurity with almost 2 decades of working with some of the largest and well known institutions. Marco's passion, expertise and knowledge has culminated in the design of the unique central management BlockAPT platform which allows businesses to Monitor, Manage, Automate & Respond (MMAR) to cyber threats 24/7 in real time. Marco is often called upon as a panellist at cybersecurity conferences and has been a host ambassador at CyberTalks, one of London's largest cybersecurity events. He is often sought after for his quick problem solving approach and helping businesses future proof their security infrastructure.
To find out more about Marco Essomba, please visit https://www.linkedin.com/in/marcoessomba/ or https://twitter.com/marcoessomba

MOHAMED SAAD

President of the Association of
Users of Information Systems in Morocco
(AUSIM)

Mohamed Saad is an actor in the world of Information Technologies since 1991. Digital Evangelist; President of AUSIM and Director of the Resources Pole of the Casablanca Stock Exchange, he has operated in the service, industry and banking sectors. In terms of associations, he is a founding member of Isaca-Casablanca, the Moroccan chapter of ISACA, Vice-President of CCAM (Morocco's Club of Business Continuity), member of Project Management Institute. He is a graduate of INSEA and holds an MBA, as well as CISA, PMP, CRISC, ISO 27001 certifications. Mohamed Saad is the author of several articles on IT Governance, IT risks, IT ROI, IT standards and baselines, and many others.

VIP Biographies

COL. MARC-ANDRÉ RYTER

Swiss Army

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Schweizer Armee
Armée suisse
Esercito svizzero
Swiss Armed Forces

Expert in security policy, Colonel Marc-André works for the Swiss Army General Staff. He holds a BA in Political Sciences and an MA earned at the NATO Defence College in Rome. He follows and studies the technological evolutions potentially relevant for the Armed Forces, in order to deduce the necessary consequences on the miltary doctrine.

MIKA LAUHDE

Vice-President, Cyber Security & Privacy,
Global PACD, Huawei Technologies Co., LTD

HUAWEI

Mika's role is including leading public relations teams to understand and provide insight of governments Cyber security and Privacy policy, public opinions, threads, technologies, laws, regulations, inside informations, situation and trends. His work in Huawei is to understand the "big picture" on Cyber Security and its requirements globally. Prior joining Huawei Lauhde worked in SSH Communications Security as VP, Government Relations and Business Development. Engaging governments, industry partners, and customers on important security and privacy issues such as critical infrastructure protection, compliancy, software assurance, risk and identity management. In Nokia Corporation Lauhde was heading Business Security and Continuity, where he was accountable globally Government Relations in Cybersecurity and Privacy area, Criminal compliancy and forensic, Nokia wide crisis management as well terminal and manufacturing related security tool manufacturing. Mika has extensive experience with cyber security related topics and governmental institutions both in Europe, ASIA and USA. Currently he is a Member of ENISA (European Network and Information Security Agency), Permanent Stakeholder Group and Europol Cyber security and privacy adviser as well Senior Fellow, Maastricht University, Faculty of Law, Centre of Data protection and Cyber Security (since 2017), Member of ENISA (European Network and Information Security Agency) PSG (since 2009), EUROPOL Cyber Security Advisor (since 2016) EUROPOL Privacy Expert (since 2015).

NICOLA SOTIRA

Information Security Manager, Poste Italiane

Nicola is in the field of information security for over 20 years with experience in different international companies. In the previous experience, Nicola Sotira was sales Director UC&C & Security Practices in Westcon Group Italy and VP Sales Italy in Clavister AB. Professor at the Master in Network Security of La Sapienza University since 2005, Member of the Association for Computing Machinery since 2004. Promoter of technological innovation, he collaborated with several startups in Italy and abroad. Member of "Italia Startup" since 2014, he advises the conception and the development of several mobile services. Nicola is alos a member of the Oracle Security Council.

CPT. PATRICK GHION

Head of the Forensics Section,
Geneva State Police

Patrick has been working for the Geneva State Police for 19 years. Until recently Head of the Computer Crime Unit, Patrick Ghion is now the of the Head of the Forensics Section of Geneva State Criminal Police – constituted by 4 brigades among which the Cybercirme one. Before joining the Law Enforcement Forces, he worked in several Swiss banks and also lived a while as diving instructor in Asia. Father of two kids, his main hobbies are scuba diving and being an aviation pilot.

Gen. Anton Rog
Director of the National CYBERINT Centre of the Romanian Intelligence Service (SRI)

- What did you dream of becoming when you were a child?

I wasn't even thinking, of course, about a career in the field, as I was born during the Ceaușescu regime. I thought I would become a teacher.

- Which faculty or professional training did you choose after school?

Mathematics Faculty at the University of Bucharest.

- What was your first job?

Software developper in a private company.

- How and when did choose cybersecurity as your specialty?

After a few months in the private company, as I was the 4th year of University, one of the chair professors was replaced by a teacher who proposed to those with an "A" (maximum) on his exam to call a phone number if they wanted "a special career". During the phone call, I found out it was the Romanian Intelligence Service (SRI). We were in 1996. From that moment, I spent 19 years in the Service, in technical departments, after which the strategic management appreciated that I was the best choice to lead the Cyberint National Center.

- What do you enjoy the most in this field?

The state of effervescence is what I like the most. The speed with which things happen, the eternal novelty character and the quality of the people I work with.

- What's your best experience in this field?

I would name three such aspects:

- Once we discovered a type of cyber threat, which, once shared with our partners, was found to be unique in the world;
- The yearly National Cybersecurity Exercise (CYDEX);
- The European Cyber Security Championship (ECSC), where the Romanian National Team became European Champion in 2019.

- What's your worst experience in this field (you went through or generic/ about evolution of the society/of a sector)?

When we discover a threat from a state actor and that threat persists in a computer system/network of an infrastructure we need to protect.

- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

Looking back, ten years ago the subject of cybersecurity was particularly new, and even the few discussions on the subject brought together few people or specialists. Today, people have perceived the importance of the subject and significant steps are being taken to counter this threat. We gained a lot of knowledge about threat, detection and countering methods, but we were also able to gradually introduce the concept of security-by-design.

In general terms, the world began to pay attention to the cyber topic quite late and very late in the field of preparation/education in cyber security. On the bright side, Romania is one of the countries that has addressed this issue at the forefront.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

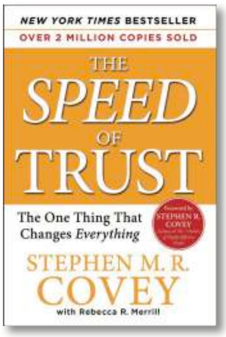
Technology has already penetrated all aspects of our lives, which is why all approaches (educational, economic, etc.) must take into account the threat associated with this technology. Artificial intelligence will be present not only in "big" technological solutions, but in all the devices that we will use on a daily basis. Malicious actors will use machine learning and A.I. to create increasingly complex tools that cannot be countered with traditional methods. This is why the cybersecurity industry needs to focus its research and development on solutions based on the same technology.

- If the digital world was a musical piece, which would it be?

Radetzky March, by Johann Strauss Sr.

- If the digital world was a painting or a piece of art, which would it be?

The Lugubrious Game, by Salvador Dalí

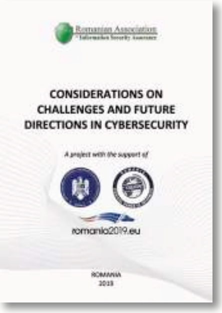

NEW YORK TIMES BESTSELLER
OVER 2 MILLION COPIES SOLD
THE SPEED OF TRUST
The One Thing That Changes Everything
STEPHEN M. R. COVEY
with Rebecca R. Merrill

- If the digital world was a novel or a book, which would it be?

The Speed of Trust: The One Thing That Changes Everything, by Stephen Covey

- For you, if digital world was an element, would it be air, earth, water or fire? Why?

It would be fire, because it consumes those who decide to get involved, but also because it propagates at the speed of fire.


Romanian Association
CONSIDERATIONS ON CHALLENGES AND FUTURE DIRECTIONS IN CYBERSECURITY
A project with the support of
romania2019.eu
ROMANIA
2019

- What is the last book you've read?

"Considerations on Challenges and future directions in cybersecurity". ■

Davide Fania
Managing Director,
XTN Cognitive Security

- What did you dream of becoming as a child?

I always dreamt of being a fighter pilot, in the Frecce Tricolori (Italian Air Force best pilots, acrobatic team).

- Which school or vocational training did you choose after school?

I did professional training as an Analyst Programmer for CASE environment (Computer-Aided Software Engineering) and then as a Certified System Administrator for IBM legacy environments.

- What was your first job?

During university, I worked in the evening shift for a famous supermarket brand to raise some money for my studies.

- How and when did you choose to make cybersecurity your specialty?

I passed to the dark side six years ago.

Curiously, before approaching cybersecurity, I had been working in a Biomedical R&D Company (Microbiology and Virology) for 15 years. I was dealing with viruses and biological attacks instead of digital ones.

- What do you like most about this field?

Competition and never-ending challenges.

On the one hand, I find it fascinating that the human being is capable of finding complex solutions to achieve goals, whether benevolent or malevolent. Being on the right side and trying to protect the defenseless is rewarding.

On the other hand, I find it unacceptable that there are some individuals (criminals, to use the right word) who choose to strike people and misappropriate their work indiscriminately. They are also cowards because they hide behind a digital wall instead of doing it in person.

- What is your best experience in this field?

XTN Cognitive Security is a dynamic company. It's a bunch of bright and talented young people, supported by wise and capable managers who have been able to deal with established international entities and overcome demanding challenges. Being part of this team is my best professional life experience.

- What is your worst experience in this field?

I use a quote from manager and friend of mine: "You can't make it go wrong". I have no negative experiences to report to date.

- How do you see the last decade of cybersecurity (2010-2019)? What did we materialise, what did we do and what did we miss?

Cybersecurity is a sector with dozens of specialisations, and today more than ever, I can say that too many people tend to generalise. The evolution of this sector has been incredibly fast, with extremely significant solutions offer. Still, cybersecurity "incidents" have increased over the past decade. It is a side effect of digitisation. I also believe that is, above all, a lack of attention from companies and even more from consumers/users. This happened because nobody has developed a sufficient cyber-security awareness and culture. Only in recent years, awareness campaigns started to spread, but the perception is that we prefer to consider the security issue as a problem that only affects others. It seems that everyone prefers "to close the stables when the cattle have already run away."

- How do you see the next decade of cybersecurity (2020-2029)? What will we continue to do, what are we ready to face, what new trends will emerge and what will we have to face / with what will we have to coexist?

I imagine the next decade precisely like the one just ended. I believe in constant growth with new solutions, new ideas, and new technologies that will be available for both "defenders" and "attackers." The tendency to rely on artificial intelligence black boxes will always put at risk of exposing "his own left" against organisations determined to pursue their criminal purposes because I think that the creativity of the human being will always prevail over digital systems. The enthusiasm for originality and innovation will always have to deal with the real truth of the market.

- If the digital world were a piece of music, what would it be?

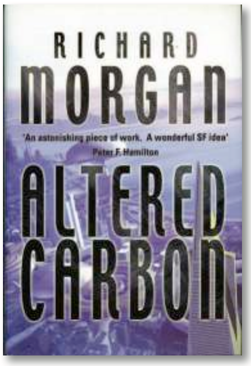
Eminence Front by The Who

- If the digital world were a painting or a work of art, what would it be?

The ideal city (a work attributed to several artists, like a teammate gig), preserved at National Gallery of the Marche (Urbino).

- If the digital world were a novel or a book, what would it be?

Bay City (a.k.a. Altered Carbon) by Richard Morgan



- If the digital world were an element, would it be air, earth, water, or fire (or a combination)?

The Earth, because we walk through it virtually every day, and the Fire because sometimes something goes wrong.

- What is the last book you read?

WTF?: What's the Future and Why It's Up to Us, by Tim O'Reilly. ■

Didier Spella
Co-founder and Manager,
Charentes-Maritime Cyber Sécurité

- What did you dream of becoming when you were a child?

Fireman

- Which faculty or professional training did you choose after school?

Electronics High School

- What was your first job?

Teacher in Electonics

- How and when did you choose to make cybersecurity your specialty?

As soon as I finished the High School

- What do you enjoy the most in this field?

Its perpetual innovation

- What's your best experience in this field (you went through or generic/about evolution of the society/of a sector)?

To design and install a network of 450 PCs at a Confidential Defense security level

- What's your worst experience in this field (you went through or generic/about evolution of the society/of a sector)?

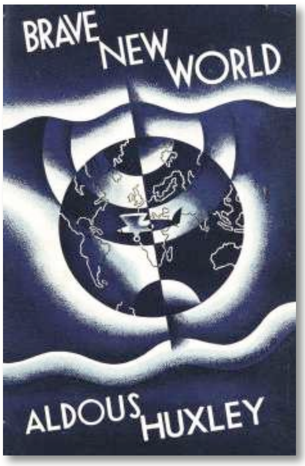
The end of centralized sites

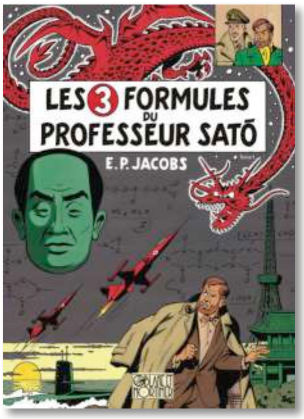
- How do you see the last decade of cybersecurity (2010-2019)? What did we materialise, what did we do and what did we miss?

The user is more and more constrained and loses the pleasure of working on digital tools.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

This digitisation of processes must be reviewed and replaced by digital processes.





- If the digital world was a musical piece, which would it be?

Swan Lake by Tchaïkovski (the spectator can choose among several possible conclusions).

- If the digital world was a painting or a piece of art, which would it be?

Freedom guiding the people (E. DELACROIX).

- If the digital world was a novel or a book, which would it be?

Brave New World - Aldous Huxley.

- If the digital world was an element, would it be air, earth, water or fire? Why?

Water, because it can be solid, liquid and gaseous, and it does not respect the laws of change of state.

- What is the last book you've read?

The 3 formulas of Doctor SATO (Blake and Mortimer cartoon). ■

Dotan Sagi
Co-CEO, Lotan Group International;
Founder and Manager, BeST.

- What did you dream of becoming when you were a child?

A musician.

- Which faculty or professional training did you choose after school?

Political sciences.

- What was your first job?

Airport Security.

- How and when did you choose cybersecurity as your specialty?

In 2017, when we saw that there was a huge disparity between how the tactical side of cyber operations and the strategic level of organizations fail to work together while managing crisis.

- What do you enjoy the most in this field?

The continuous level of threats that keep developing meaning we have to be on our toes and one step ahead.

- What's your best experience in this field?

The understanding that cyber is a strategic part of the organization. It is not only the CISO or CTO's responsibility. It is the whole organization's responsibility and CEO's or the Board of directors cannot shirk from responsibility.

- What's your worst experience in this field?

When I see an organization carrying out simulations or training just for the compliance part and not really interested in the performance based processes. We see less of this today, but from time to time it pops up and it's a bummer.

- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

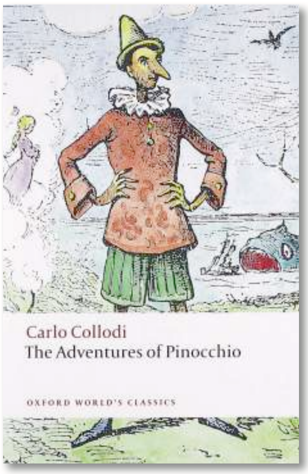
We missed much already with regards to hardware, software and processes but mainly about our behaviours.

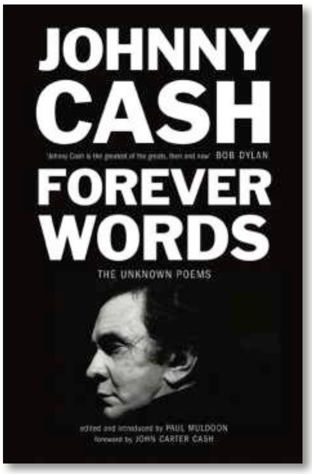
- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

The threats will change, software and hardware will change. The question is, will humans change their behaviour as well?

- If the digital world was a musical piece, which would it be?

Growing up by Bruce Springsteen




JOHNNY
CASH
'Johnny Cash is the greatest of the greats, then and now' BOB DYLAN
FOREVER
WORDS
THE UNKNOWN POEMS
edited and introduced by PAUL MULDOON
foreword by JOHN CARTER CASH

- If the digital world was a painting or a piece of art, which would it be?

Convergence, by Jason Pollock

- If the digital world was a novel or a book, which would it be?

Pinocchio, by Carlo Collodi.

- If the digital world was an element, would it be air, earth, water or fire? Why?

Fire as its blazing hot.

- What is the last book you've read?

Forever words, the unknown poems of Johnny Cash. ■

Ionuț Stoica
Cybercrime Training Officer within the European Union Agency for Law Enforcement Training (CEPOL)

- What did you dream of becoming when you were a child?

My dream was to become a police officer.

- Which faculty or professional training did you choose after school?

I chose to follow Faculty of Law within the Romanian Police Academy and Faculty of Communication and Public Relations within the National University of Political Studies and Political Administration.

- What was your first job?

My first job was a cybercrime investigator within the General Inspectorate of Romanian Police, Central Cybercrime Unit.

- How and when did you choose cybersecurity as your specialty?

During the last year as a student of Romanian Police Academy I got a specialization on cybercrime which definitely changed my perspective and my career path.

- What do you enjoy the most in this field?

By its nature, cybercrime must evolve to survive. Not only are cybersecurity experts constantly working to prevent cyberattacks, but technology itself is evolving day by day. Cybercrime is like a "cat and mouse game", cybercriminals are constantly creating new attacks to fit new trends, while cybersecurity experts and criminal justice authorities need to adapt constantly to prevent and mitigate the attacks and prosecute the offenders.

- What's your best experience in this field?

There are a lot of reasons to pursue a career in cybercrime or in the cybersecurity field.

In today's world, almost all the crimes include a cyber-component and digital evidence and the role of cybercrime investigator for me was very fulfilling in gathering all crucial evidences to solve the puzzle of different cybercrimes.

- What's your worst experience in this field?

I cannot say that I had very bad experiences during my activity as a cybercrime investigator. However cybercrime is the most transnational of all the crimes and collecting digital evidence from different jurisdictions might represent a real challenge sometimes.

- How do you look backwards at the last cybersecurity decade (2010-2019)? What have we achieved? What have we made and what have we missed?

Cybersecurity companies adapted constantly their approaches to security and solutions to align with the new environment by adopting cloud infrastructure and improving of security for IOT devices. However, the frequency and magnitude of cyber-attacks increased constantly during the last period and one of the best examples is probably the Wannacry ransomware campaign from 2017 which affected more than 200,000 computers across 150 countries.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

To understand how cybercrime and cyber-security might evolve in the future, we should first look back to see how it emerged in the past. Traditional techniques used by the attackers for cyber-attacks and online frauds (phishing campaigns, spoofing, social engineering) will mainly remain in trends but the new technologies such as crypto currencies, darkweb, artificial intelligence and IOTs might facilitate even more criminal activities in the future. On the other hand, cyber threat intelligence can help cybersecurity professionals prevent and identify future cyber threats.

- If the digital world was a musical piece, which would it be?

I want it all - by Queen.

- If the digital world was a painting or a piece of art, which would it be?

The Eye by Salvador Dalí.

- If the digital world was a novel or a book, which would it be?

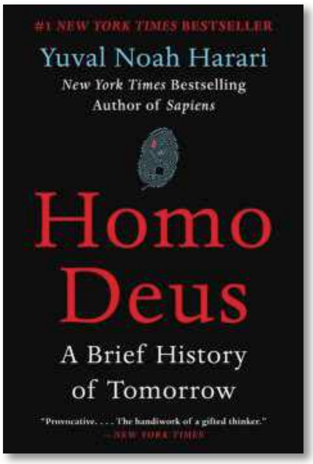
Homo Deus by Yuval Noah Harari.

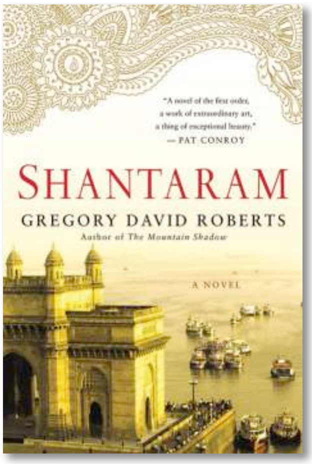
If the digital world was an element, would it be air, earth, water or fire? Why?

I would go for "air" as nowadays it almost impossible to live considering this one is involved in almost every aspect of our life, making it more comfortable. As we cannot live without air, it becomes more and more difficult to live outside the digital world.

- What is the last book you've read?

Shantaram by Gregory David Roberts. ■


#1 NEW YORK TIMES BESTSELLER
Yuval Noah Harari
New York Times Bestselling Author of Sapiens
Homo Deus
A Brief History of Tomorrow
"Provocative. . . . The handiwork of a gifted thinker."
—NEW YORK TIMES


"A novel of the first order, a work of extraordinary art, a thing of exceptional beauty."
—PAT CONROY
SHANTARAM
GREGORY DAVID ROBERTS
Author of The Mountain Shadow
A NOVEL

Luca Tenzi
International Atomic Energy Agency,
Organisation Resilience consultant

- What did you dream of becoming as a child?

I wanted to be a military aircraft pilot, I even tried but didn't make it.

- Which school or vocational training did you choose after school?

Slow start for me, but after my political science studies I became interested in security and criminology and from there the step was short in continuing my studies in this direction.

- What was your first job?

As a teenager in the summer I worked at my parents' campsite on Lake Lugano. A little bit of everything from coffee to latrines to bathroom cleaning. But I also had many laughs and made new friendships.

- How and when did you choose to make cybersecurity your specialty?

Given that I am not a cybersecurity expert, I believe it is the natural evolution of the world of corporate security that has brought me closer to the dark side of technology.

- What do you like most about this field?

The continuous technological evolution, the speed this evolves at allowing us to do new things or more easily. The duality of technology, used for good and evil, stimulates me to try to understand its possible malicious use. But also try to understand its weaknesses, because human will always try to by-pass the system or find shortcuts to achieve a purpose..

- What is your best experience in this field?

In recent years, those transversals collaborations with the technological world for the convergence of physical / logical security. Projects realised and not only hypothesised. We can no longer speak of two distinct and distant sectors.

- What is your worst experience in this field?

Talking about the worst experience is perhaps exaggerated, but the lack of medium to long term vision by some corporate security experts always leaves me stunned.

- How do you see the last decade of cyber security (2010-2019)? What have we achieved, what did we do, what did we miss?

In less than a decade we have gone from a hatched subject to only a select few to a constant and continuous informative, cognitive trend. By now everyone talks about it, everyone has an opinion, and everyone has the keys to it. We certainly missed that technological cybersecurity had to be by design, but quoting a speaker in a past year conference "now we buy technology as if it were buying a car without a door or tail light, and expecting they will be fixed while driving". We have certainly created a two-speed world, with a technology divide not only geographically but also generationally. Concretely, even following the COVID-19, we managed to enter that famous fourth industrial revolution that many thought was just science fiction.

- How do you see the next decade of cybersecurity (2020-2029)? What will we continue to do, what are we ready to face, what new trends will emerge and what will we have to face / with what will we have to coexist?

I think we will come to a point of technological saturation. I hypothesise a slowdown in the acquisition and use of new technologies by the general public while research will continue its evolutionary run. The next decade will see man at the center of technology, with important developments in the bionic field and man / machine interaction. Not only in the medical field but also in the military and civil sphere. In the first phase of the decade, artificial intelligence will dominate but also in this area, a saturation point will be reached by the end user. We will see the first interstate conflicts in the fourth dimension, the cyber dimension. Privacy will have another flavor.

- If the digital world were a piece of music, what would it be?

Métamorphoses by Jean Michel Jarre.

- If the digital world were a painting or a work of art, what would it be?

Composition VII, by Vasiliy Kandinsky.

- If the digital world were a novel or a book, what would it be?

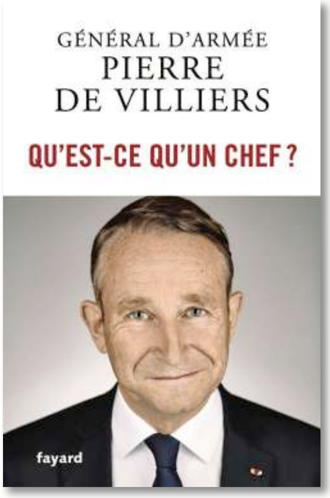
Maybe a little obvious but not too much: I Robot by Isaac Asimov.

- For you, if the digital world were an element, would it be air, earth, water, or fire (or a combination)? Why?

Water, for its versatility, for its various forms, its strength and sweetness.

- What is the last book you read?

Qu'est-ce qu'un chef, by French Army General Commander (ret.) Pierre de Villiers. ■



Marco Essomba
BlockAPT Founder and CTO

- What did you dream of becoming when you were a child?

An Architect (Building)

- Which faculty or professional training did you choose after school?

Electro Mechanical Engineering.

- What was your first job?

Application Support Engineer.

- How and when did you choose cybersecurity as your specialty?

After high school, I dropped out from my Architecture course and joined the Computer Science Club. Got hooked and never looked back!

- What do you enjoy the most in this field?

Constant learning. Relentless pursuit of knowledge. Never knowing enough.

- What's your best experience in this field?

From engineer, to consultant, to security architect. Three phases of my computer science learning path that are intricately linked and have provided the best experience, an inquiring mind, and a framework for learning more computer science skills.

- What's your worst experience in this field?

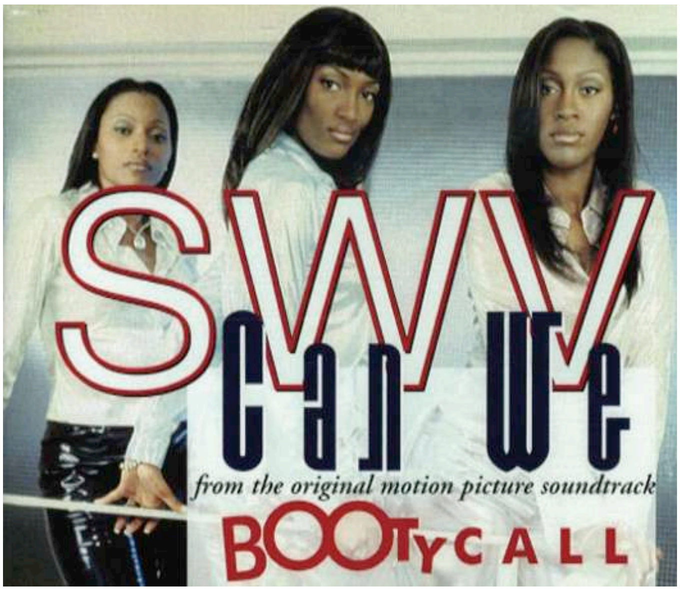
Building a security product from the ground up. Learning the hard way that great technology must be matched with a great team and people skills to succeed.

- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

The last decade in cybersecurity was all about point solutions and how to solve specific challenges. There are a myriad of technologies that are very effective and do a great job at preventing cyber threats. However, those technologies are not working very well together which creates its own sets of challenges.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

The next cybersecurity decade will be ripe for consolidation. Point solutions will be combined in a much more effective way to deliver a broader and comprehensive protection. As cyber attacks get more automated, it is expected that the real challenge that lies ahead is machines fighting machines due to the rise of AI and automation.



- If the digital world was a musical piece, which would it be?

Can We, by SWV.

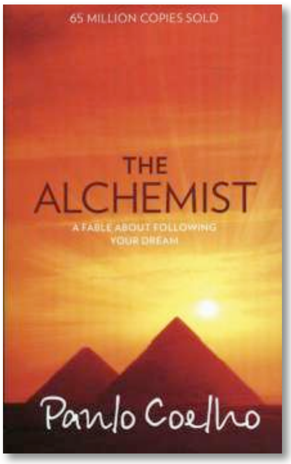
- If the digital world was a painting or a piece of art, which would it be?

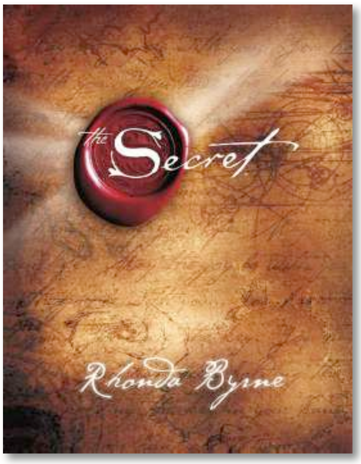
Power and Religion by Abdoulaye Konaté.

- If the digital world was a novel or a book, which would it be?

(1984 (Orwell), Alice's Adventures in Wonderland (Dodgson), War and Peace (Tolstoj), Twilight of the Idols (Nietzsche), etc…)

The Alchemist, by Paulo Coelho.





- If the digital world was an element, would it be air, earth, water or fire? Why?

Water - without it we die!

- What is the last book you've read?

The Secret by Rhonda Byrne. ■

Mohammed Saad
Casablanca Stock Exchange,
CIO

- What did you dream of becoming when you were a child?

Like many other children with eyes lit by the sky, freedom and a taste for discovery, I always dreamt of being a plane pilot... and I have succeeded, as a student military pilot. Except that it turned out to be short lived because one of the components of the dream, which is freedom, was not there and, as a result, I revised my list of dreams by moving towards computer science, as it was called at the time, a field that offered and continues to offer more development, innovation and creation.

- Which faculty or professional training did you choose after school?

After my Baccalaureate and as noted above, I joined the Royal Air Force School Base for a while. Then I moved to the National Institute of Statistics and Applied Economics, the only institution that offered engineering training in "Computer Science". Thereafter, and throughout the last 30 years, I continued to learn, which allowed me to pass seven certifications in the field of IT, security, IT risk, project management, etc.

- What was your first job?

Like any IT engineer wanting to build a career in the factory, I opted for a Computer Services and Engineering Company (SSII) and it was very formative, because it allowed me to work with several project managers, to learn a lot about different areas, and to be in an IT services environment. From the first week I was assigned to a team that was in charge of the IT overhaul of a large insurance company in Morocco. The assignment lasted 24 months and allowed me to participate in a strategic project for the client, which started with process re-engineering led by a team in charge of the organisation and, subsequently, our team took over to implement the new application infrastructure of the said insurance company.

- How and when did you choose cybersecurity as your specialty?

Cybersecurity is an automatic part of the life of every IT specialist. In 2001, I attended a training course on information systems auditing which led me to prepare for the CISA (Certified Information Systems Auditor), administered by the Chicago-based ISACA (Information Systems Audit and Control Association), which promotes best practices in IT Governance, It was then that I realised that the tsunami of innovation that is hitting IT with the uncontrolled development of the Internet comes with risks, vulnerabilities and threats that now need to be managed at the highest level of the company. The governance of IT security has also been given a high profile with the advent of the BS 7799 framework, which is the basis for ISO 27001. A few years later, I started my ISO 27001 certification, which led me to further deepen my knowledge of security and the fight against cybercrime. I then started preparing for CISM and CISSP, without going all the way through my project, but it did allow me to develop other skills in IT security.

- What do you enjoy the most in this field?

First of all, this is a very challenging area, because it never stops in terms of innovation and development. Institutions, and then society as a whole, need guardians of the temple to preach the good word and ensure that good practices are followed in planning, assessing and responding to risks and, secondly, to assess the maturity level of processes and prepare to counter the bad intentions of outsiders.

- What's your best experience in this field ?

The Casablanca Stock Exchange's ISO 27001 certification remains one of my best achievements in the field. Compliance with a standard is not an end in itself, but the work required for an upgrade takes years, and then one wonders whether to go ahead or not. Certification brings a certain assurance, because as soon as we embark on it, it's a non-stop journey of continuous improvement, of implementing the required measures, but also of auditing, correcting, improving and optimising. The exercise also requires a corporate culture and group work, because everyone is concerned about the security of information systems.

- What's your worst experience in this field?

I have had some rather unfortunate experiences with certain members of AUSIM (Association des Utilisateurs des Systèmes d'Information du Maroc) who have been the object of brutal attacks that have sometimes led to the encryption of management servers and ransom demands, or others who have had rather large amounts stolen by exploiting the vulnerability of changing the IBAN code when transferring money abroad.

- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

The picture is rather bleak due to the development of technology, the proliferation of social networks and the lack of awareness in society. The scourge has also taken advantage of the lack of cooperation between nations and the legal gap that exists in the world. Admittedly, there are more and more activists who have made the fight against cybercrime a major objective, and I welcome the actions launched by Prof. Laurent Chrzanovski through the research he is conducting in several countries, through his publications and other conferences to demystify cybercrime and to work together with government authorities to curb this scourge or at least reduce its impact.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

First of all, it is necessary to remain on guard, raise awareness, educate and train more and more cybersecurity specialists. We need to be careful and monitor the use of AI in cybercrime. We will use the same weapon in the future to provide solutions that are less static, but more intelligently and dynamically. AI will also be able to rely on Big Data by correlating different sources of information to understand the behaviours and techniques of cyber criminals.

- If the digital world was a musical piece, which would it be?

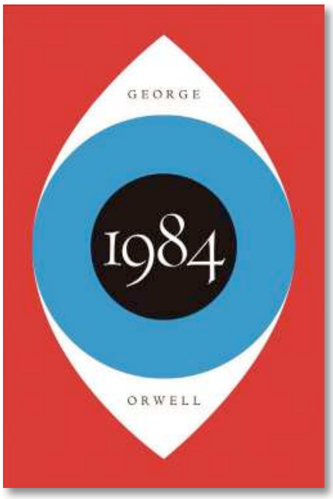
What I've done by Linkin' Park

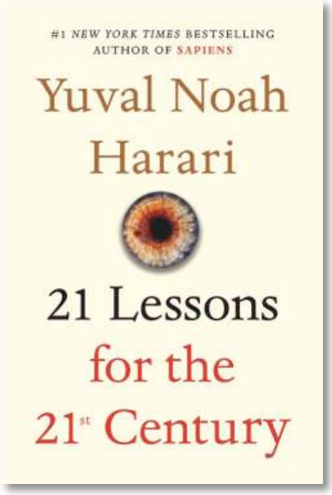
- If the digital world was a painting or a piece of art, which would it be? (ex: Guernica (Picasso), Mona Lisa (Leonardo), etc..)

Guernica, by Picasso.

- If the digital world was a novel or a book, which would it be?

1984, by George Orwell.




#1 NEW YORK TIMES BESTSELLING AUTHOR OF SAPIENS
Yuval Noah Harari
21 Lessons for the 21st Century

- If the digital world was an element, would it be air, earth, water or fire? Why?

A combination of air and fire. An antinomic combination, because fire cannot progress without the oxygen contained in the air and, at the same time, as it develops, it destroys the ambient air that serves as its breeding ground.

- What is the last book you've read?

21 Lessons for the 21st Century, by Yuval Noah Harari. ■

Col. Marc-André Ryter
Swiss Army

- What did you dream of becoming when you were a child?

Airline pilot.

- Which faculty or professional training did you choose after school?

Faculty of Social and Political Sciences.

- What was your first job?

Political asylum procedure officer.

- How and when did you choose cybersecurity as your specialty?

I have followed the evolution of technology and its growing impact on society since the widespread diffusion of personal computers in the 1990s. The interest in cybersecurity has naturally materialised as a logical continuation and necessity of this development, especially with the increase in the importance and privacy of the data processed.

- What do you enjoy the most in this field?

Its societal, i.e. global character, with the fact that it has an increasing impact on all dimensions of our lives. This makes it exciting.

- What's your best experience in this field?

The growing, if slow, recognition of the absolute need to protect oneself by promoting cybersecurity. And, in concrete terms, that certain political decisions have been taken to do so.

- What's your worse experience in this field?

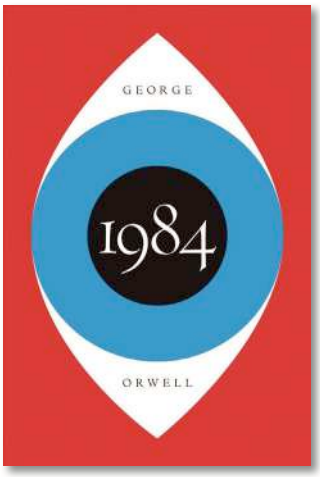
The denial of the need to promote cybersecurity by some actors and the slowness of decision-making in general, coupled with the too limited means available.

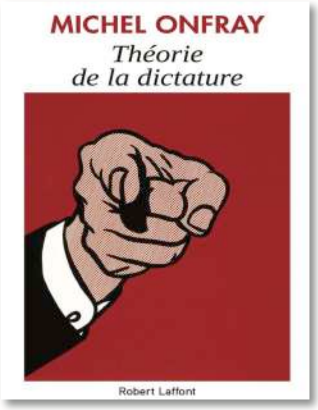
- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

Certain advances in cybersecurity have been largely undermined by the increased capabilities of malicious actors. As a result, the situation remains very unstable and we are still a long way from a safe cyber space where our personal data is safe from abuse. However, States have become aware of the extent of the problem, which no longer concerns only State security and issues such as espionage, but all citizens and the security of society as a whole.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

The confrontation between new tools for cybersecurity and new malicious tools will continue. However, few actors will be able to be at the forefront of the malicious side and the increasing implementation of high-performance security tools (multidimensional platforms supported by artificial intelligence) will still allow for an overall improvement in cybersecurity, without, however, making it possible to exclude successful attacks.





- If the digital world was a musical piece, which would it be?

Symphonie Fantastique, by Hector Berlioz.

- If the digital world was a painting or a piece of art, which would it be?

Golconde, by Magritte.

- If the digital world was a novel or a book, which would it be?

1984 by Orwell, not only for the surveillance dimension, but above all for the normative dimension of citizens' lives.

- If the digital world was an element, would it be air, earth, water or fire? Why?

Air, which is essential for living and which can penetrate everywhere.

- What is the last book you've read?

La Théorie de la dictature, by Michel Onfray. ■

Mika Lauhde
Huawei Global Vice-President
Cyber Security & Privacy.

- What did you dream of becoming when you were a child?

Airline pilot or racing driver.

- Which faculty or professional training did you choose after school?

Graphical industry - Automation - Electronic.

- What was your first job?

Gardener in the city of Vantaa.

- How and when did you choose cybersecurity as your specialty?

When my management company (then Nokia) made the decision that somebody needed to take care of Cyber issues… I was asked to take care of that.

- What do you enjoy the most in this field?

Ability to sort out complicated technical and political challenges

- What's your best experience in this field?

That in these 30 years in telecom and cyber, we have just been seeing the impact of cyber is widening.

- What's your worst experience in this field?

At the moment, most people understand cyber only at headline level. You need long term experience to understand all dependencies in this area (full stack understanding).

- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

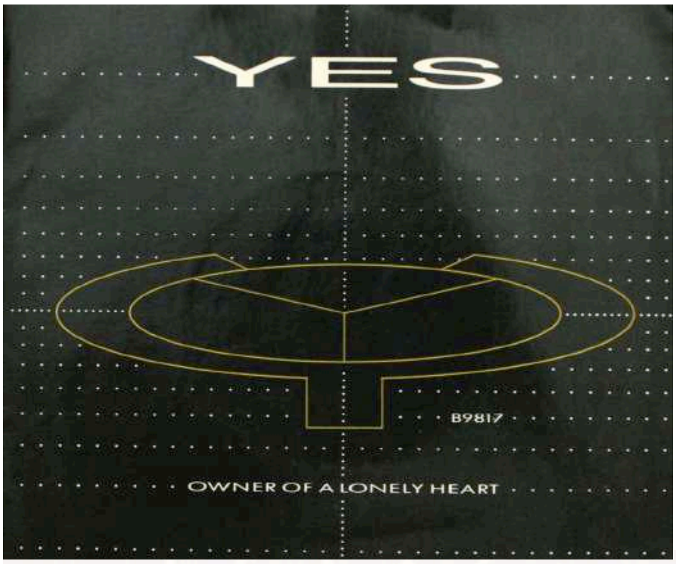
The biggest change has been that Europe has been declining in Cyber and ICT area. In the last 10 years, Europe has lost most of the technologies and competences. Only few small private companies are left. Even Nokia and Ericsson have most of their people outside of European soil.

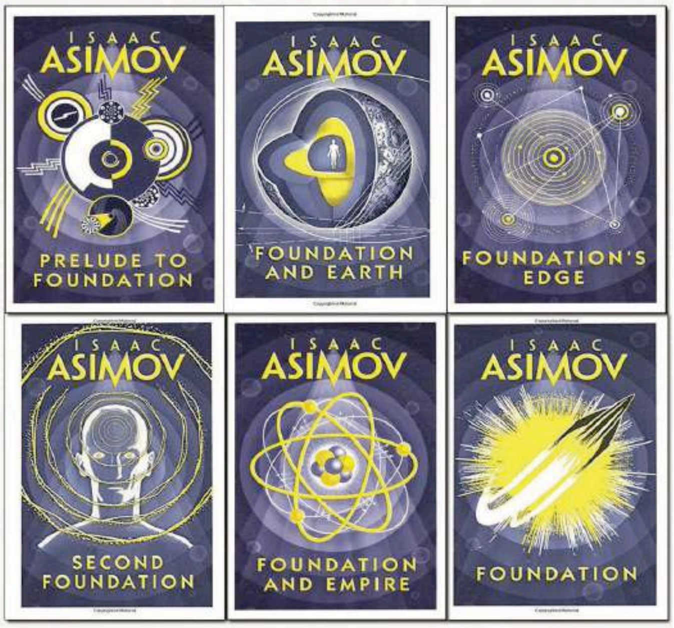
- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

In the case where Europe will start to defend the digital sovereignty, European patents, standards, certification competences and technologies, we still have a chance that there will be a credible European ICT and cyber competences. If decisions go the other way, Europe just will not go through easy times and these issues will be dealt outside Europe.

- If the digital world was a musical piece, which would it be?

Owner of a lonely heart - by Yes.





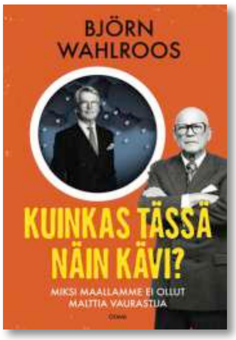
- If the digital world was a painting or a piece of art, which would it be?

"Skrik" (The Scream), by Edvard Munch.

- If the digital world was a novel or a book, which would it be?

The Foundation, a book series by Isaac Asimov.

- If the digital world was an element, would it be air, earth, water or fire? Why?



Air. Everyone is able to feel it, but very few are seeing it.

- What is the last book you've read?

"Kuinkas tässä näin kävi?"(How this happened here), by Björn Wahlroos (the Chairman of the Board of Sampo Group, Nordea and UPM-Kymmene), an analysis of why Finnish economy has not been growing in the last 10 years, followed by predictions on its future. ■

Nicola Sotira
Information Security Manager,
Poste Italiane S.p.A.

- What did you dream of becoming when you were a child?

A surgeon in order to help cure diseases.

- Which faculty or professional training did you choose after school?

I have always remained in the technical and programming sector. In particular, I did specialisation courses in Z80 programming.

- What was your first job?

During my studies, I worked as a radio and TV repairer.

- How and when did you choose cybersecurity as your specialty?

I started working on network security in the 90's during the first developments of the Internet in Italy.

- What do you enjoy the most in this field?

The continuous evolution of scenarios, complexity, knowledge, a world where you learn all the time, a domain where the challenge between good and evil travels the web...

- What's your best experience in this field?

In Poste Italiane I found a dynamic environment, a society that is making an extraordinary digital transformation. But above all I have found a team with huge motivation, great team spirit and competence. Being part of this team is exciting.

- What's your worst experience in this field ?

There are no problems, only opportunities, as my boss used to say openly during staff meetings in Sweden. You just need to know how to look and you will always find something positive even in situations that may seem adverse. That's why I don't have negative feelings.

- How do you look backwards at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

In those years the evolution of digital and services continued its course while crime moved more and more from the physical to the cyber space. We are surrendering the national sovereignty of our data, a missed opportunity that security management alone will probably fail to compensate. Awareness has certainly increased across the boards of companies, but we are still seeing little impact, and incidents are often linked to trivial computer hygiene that we struggle to make effective outside the slides.

- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what we shall be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

We will continue to have scenarios where good and bad will face each other, scenarios where new technologies will dictate agendas. The cloud will transfer many of these issues to the responsibility of operators, leaving more room for small and medium sized businesses to focus on core activities by fully delegating infrastructure and security. What should we coexist with? Certainly with less privacy...

U2
NEW YEAR'S DAY
(LONG VERSION)
TREASURE (WHATEVER HAPPENED TO PETE THE CHOP)
PLUS LIVE VERSIONS OF
FIRE
I THREW A BRICK THROUGH A WINDOW
A DAY WITHOUT ME

- If the digital world was a musical piece, which would it be?

New Year's Day by U2.

- If the digital world was a painting or a piece of art, which would it be?

The origins by Mark Kostabi.

- If the digital world was a novel or a book, which would it be?

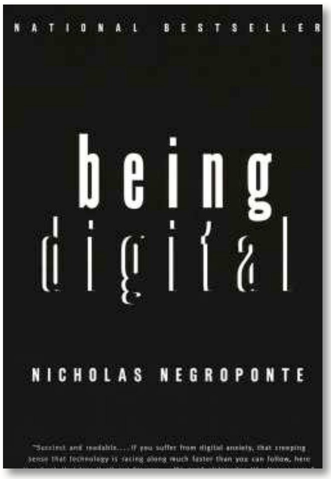
Being Digital by N. Negroponte.

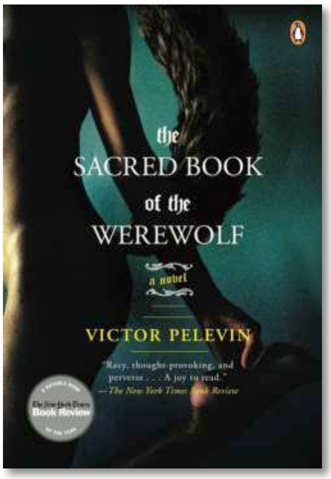
- If the digital world was an element, would it be air, earth, water or fire? Why?

Water to quench your thirst for knowledge.

- What is the last book you've read?

The sacred book of the Werewolf by Victor Pelevin. ■




the SACRED BOOK of the WEREWOLF
a novel
VICTOR PELEVIN
"Racy, thought-provoking, and perverse . . . A joy to read."
—The New York Times Book Review

Cpt. Patrick Ghion
Head of the Forensics Section,
Geneva State Police

- What did you dream of becoming when you were a child?

I remember an episode when I was in primary school when I was looking at the sky and thinking that one day I would be an airline pilot. The dream of flying followed me, since at 16 I took the exams to become a fighter pilot. Unfortunately, it didn't work out. However, later on in life I was lucky enough to get my private pilot's licence, with certain additions such as night flying or planes with retractable landing gear, for example. Today I fly a lot in the United States, France and of course Switzerland.

- Which faculty or professional training did you choose after school?

After secondary school, I started a banking course. This world has always fascinated me and I was lucky enough to do an internship at the "corbeille", the nickname of the Geneva Stock Exchange, when it still existed. Experiencing the atmosphere of the stock exchange with screaming brokers and the omnipresent pressure was one of my best memories. It was only much later that I attended the University of Geneva for a master's degree in Global Security and Conflict Resolution.

- What was your first job?

I started my professional career as a bank employee at Credit Suisse in Geneva. Even though I only stayed there for two years, it was an extraordinary experience and what I learned there and the people I met still enlighten me today.

- How and when did you choose cybersecurity as your specialty?

I've always been passionate about IT in the broadest sense of the word. As a child, I remember some television programmes where we learned the basics of the concept with IBM. Later on, and thanks to holiday jobs, I was able to buy myself a Commodore 64. I still remember nights programming in Basic. Later, when I was a police inspector assigned to the burglary squad, a position as an inspector in the Computer Crime Squad opened up and I applied. It was one of the great opportunities of my life. I literally plunged into the fight against cyber crime in all its aspects. I am very grateful to the Geneva Police for having been able to train me and improve my knowledge over all these years.

- What do you enjoy the most in this field?

The complexity and difficulty of claiming certainties. I explain myself along two lines, firstly about techniques that evolve at such a crazy speed, so that what is true today can be the opposite tomorrow. For example, in 2003, we learned that during searches we had to unplug the computer (Pull The Plug). Today, it is the opposite, we must not pull the plug because of the information to be retrieved in the RAM for example. The other aspect is potentiality. When I'm asked if it's possible to do this or that, my answer is often: "It depends". It's the delta between potentiality and the actual result that I find fascinating.

- What's your best experience in this field?

In the field I work in, we are always in the race with the latest technological developments that can be used for criminal purposes. The best experiences are then counted by the number of perpetrators arrested for offences ranging from financial crimes to sexual abuse of children.

- What's your worst experience in this field?

Bad experiences are those cases where we were not in conditions to confuse a criminal, or worse, to save a life.

- How do you look back at the last cybersecurity decade (2010-2019)? What have we achieved, what have we made, what have we missed?

From a police point of view, it is exciting to note the evolution of the fight against cybercrime over the years. In particular, with regard to the means and procedures put in place from a technical point of view. What was the rule in terms of searches a few years ago has evolved towards its opposite. The obsolescence of the means and techniques used in the fight against cybercrime requires police specialists to be permanently adaptable, which generates professional stress that must be taken into account. Training and professional networks remain essential actors in maintaining the performance of these specialised police officers. Although legal developments do not always allow a correlation with technology, the different actors have become aware of the urgency of an agile society.

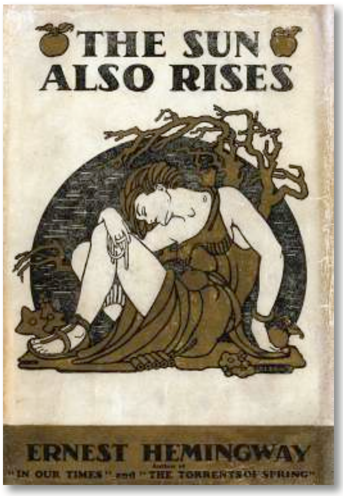
- How do you look forward to the next cybersecurity decade (2020-2029)? What shall we continue to do, what shall we be prepared to face, what new trends will emerge and what will we have to cope/coexist with?

Exciting! Ten years ago, it was very difficult for us to make projections on the evolution of technologies that we would have to master, especially in the fight against crimes generated by technological developments. Within the Geneva Police, we work on several strategic and operational levels which have enabled us to maintain relevant growth in the fight against cybercrime.

The implementation of a Bill for a credit of 1.2 million, the creation of the Cyber Competence Centre for Western Switzerland, the development of the PICSEL national centre for online serial crimes, the national directorate for ransomwares coordinated by NEDIK and recently with an important development in the fight against child pornography. Although the organisation of the fight against cybercrime at the Geneva Police has proved its worth, it is essential for us to maintain a permanent questioning and a total capacity to adapt. At the Geneva Police, we can count on highly motivated specialists, trained to a very high level and aware of the importance of the task entrusted to them.

- If the digital world was a musical piece, which would it be?

Waltz of the Flowers by Piotr Ilyich Tchaikovsky.



- If the digital world were a painting or a work of art, which would it be?

The portrait of Adele Bloch-Bauer by Gustav Klimt.

- If the digital world was a novel or a book, which would it be?

Fiesta: The sun also rises, by Ernest Hemingway.

- If the digital world was an element, would it be air, earth, water or fire? Why?

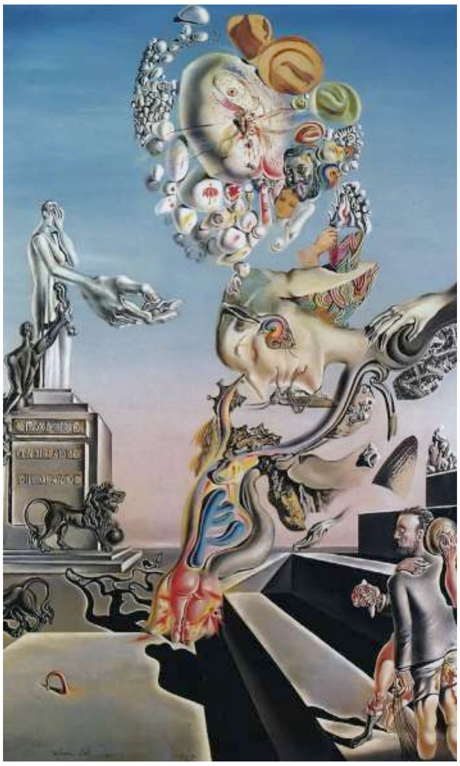
Water, because like digital technology, it allows the transmission of any type of vibration, without limits and all over the world.

- What is the last book you've read?

Painted Veil, by Somerset Maugham. ■

VIP Art Gallery

Davide Fania
Unknown artist
The ideal city (1475-1480)



Anton Rog
Salvador Dalí
El juego lúgubre (Lugubrious Game) (1929)

Didier Spella
Eugène Delacroix
La Liberté guidant le peuple (1830)

Dotan Sagi
Jackson Pollock
Convergence (1952)

Ionut Stoica
Salvador Dalí
El Ojo (The Eye) (1945)

Luca Tenzi
Wassiliy Kandinsky
Composition VII
(1913)

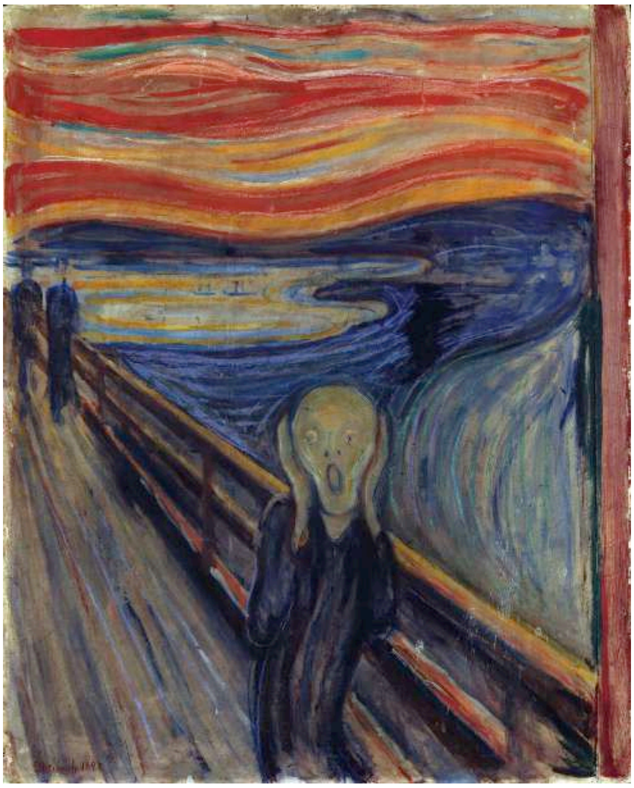
Marco Essomba
Abdoulaye Konaté
Pouvoir et Religion
(Power and Religion)
(2011)

Mohamed Saad
Pablo Picasso
Guernica (1937)

VIP Art Gallery

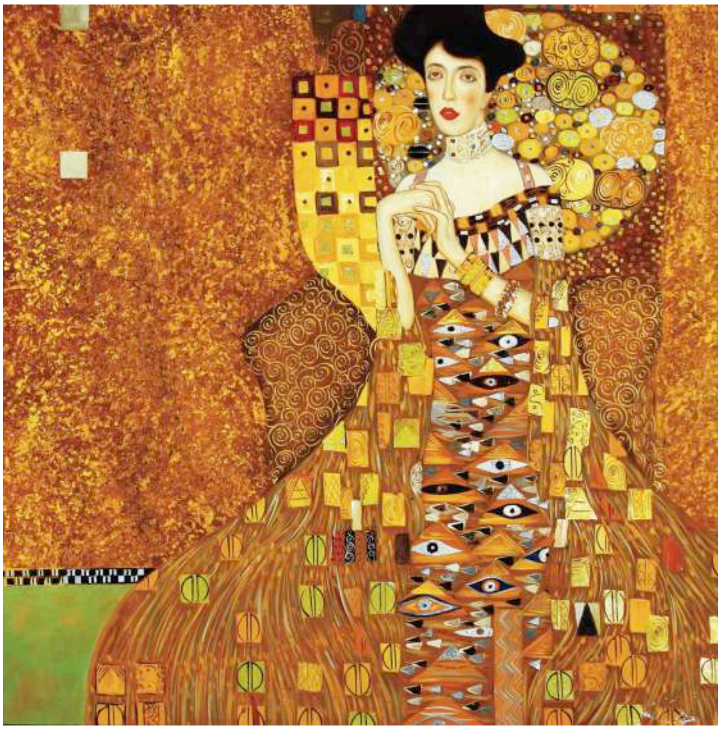
Marc-André Ryter
René Magritte
Golconde (1953)

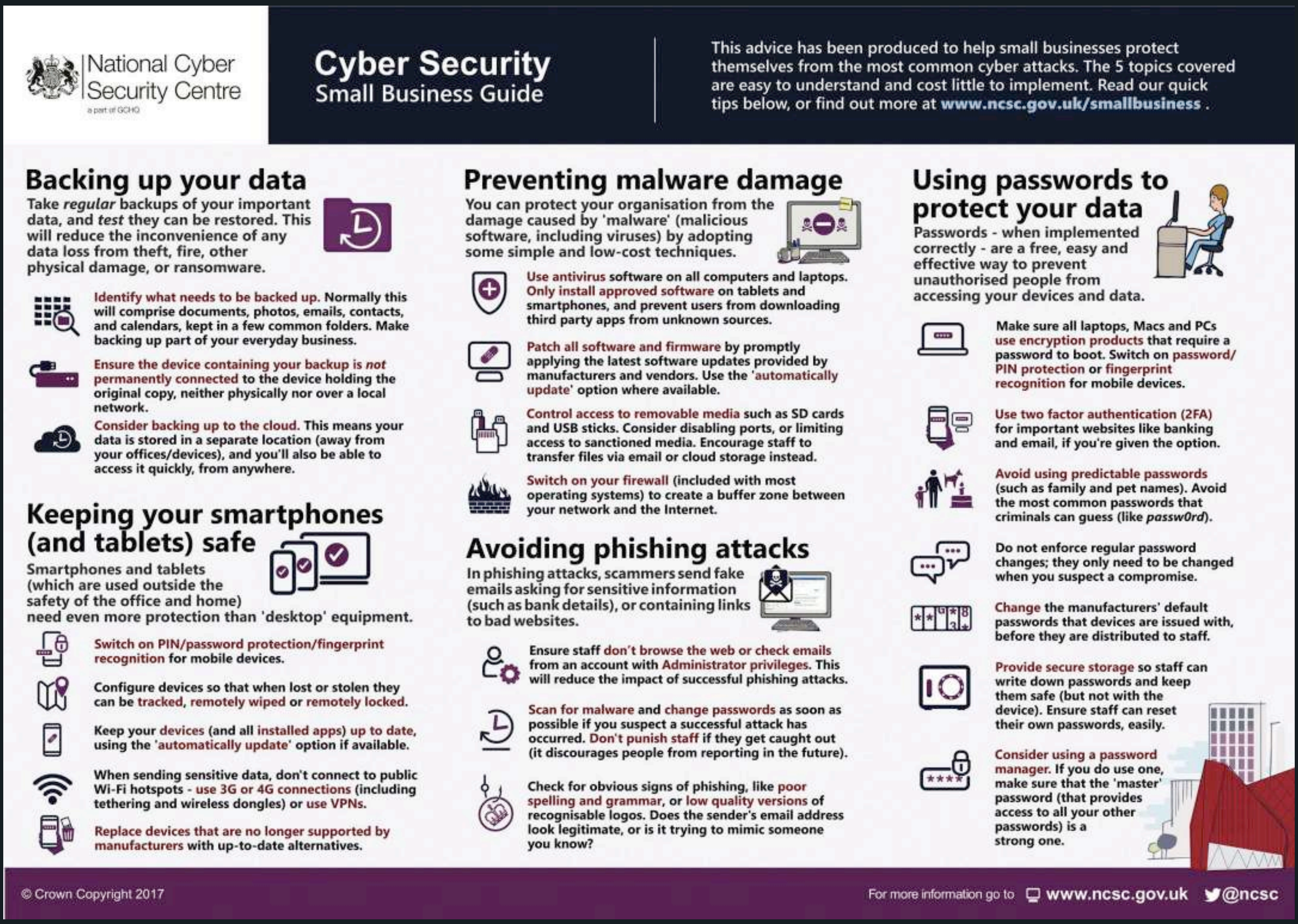
Nicola Sotira
Mark Kostabi
The origins (Hommage to
De Chirico) (2010)



Mika Lauhde
Edvard Munch
Skrik (The Scream) (1893)

Patrick Ghion
Gustav Klimt
Portrait of Adele Bloch-Bauer (1907)





National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.

Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.

Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, Macs and PCs use encryption products that require a password to boot. Switch on password/ PIN protection or fingerprint recognition for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

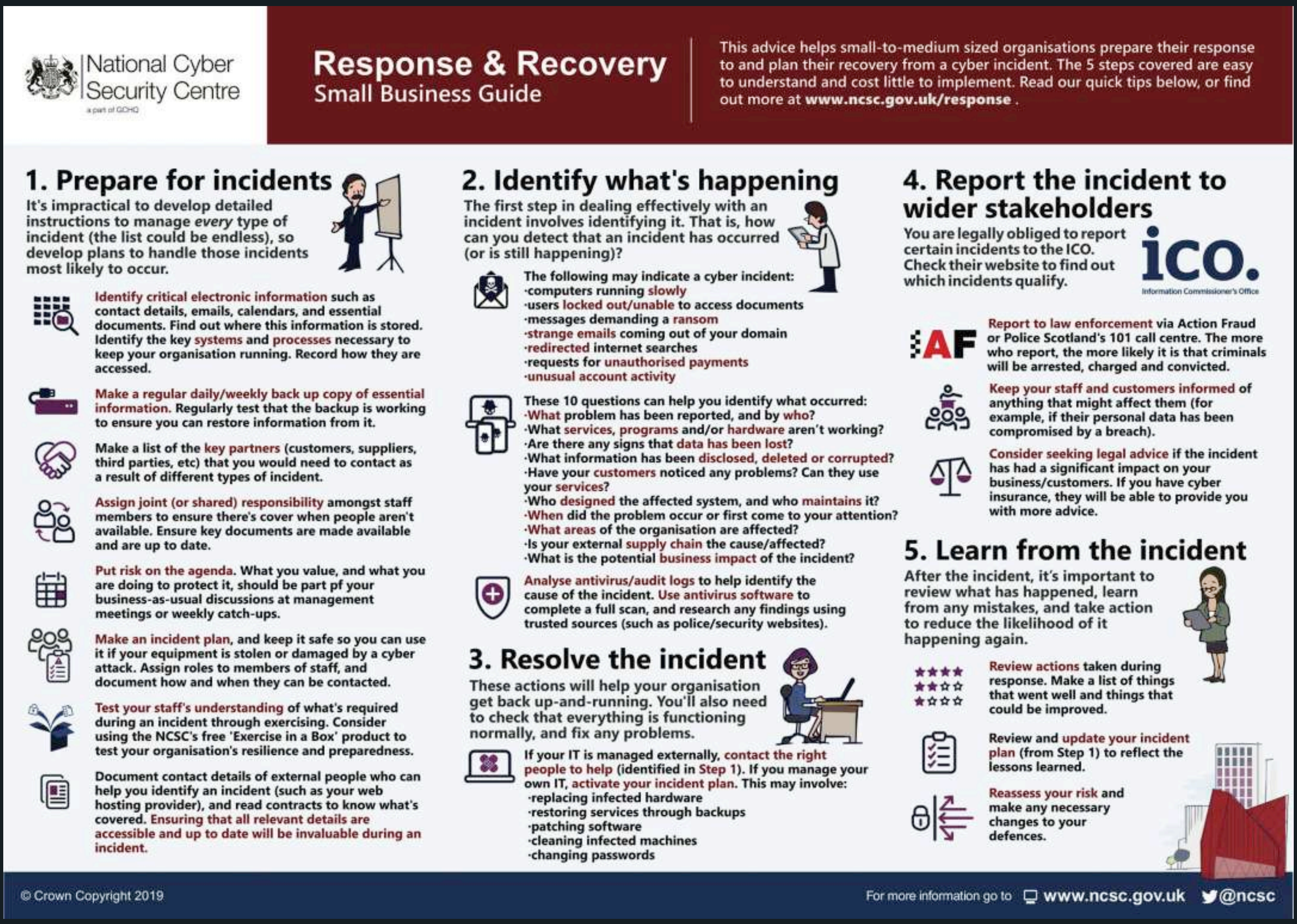
Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc



National Cyber Security Centre
a part of GCHQ

Response & Recovery
Small Business Guide

This advice helps small-to-medium sized organisations prepare their response to and plan their recovery from a cyber incident. The 5 steps covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/response** .

1. Prepare for incidents

It's impractical to develop detailed instructions to manage *every* type of incident (the list could be endless), so develop plans to handle those incidents most likely to occur.

Identify critical electronic information such as contact details, emails, calendars, and essential documents. Find out where this information is stored. Identify the key systems and processes necessary to keep your organisation running. Record how they are accessed.

Make a regular daily/weekly back up copy of essential information. Regularly test that the backup is working to ensure you can restore information from it.

Make a list of the key partners (customers, suppliers, third parties, etc) that you would need to contact as a result of different types of incident.

Assign joint (or shared) responsibility amongst staff members to ensure there's cover when people aren't available. Ensure key documents are made available and are up to date.

Put risk on the agenda. What you value, and what you are doing to protect it, should be part pf your business-as-usual discussions at management meetings or weekly catch-ups.

Make an incident plan, and keep it safe so you can use it if your equipment is stolen or damaged by a cyber attack. Assign roles to members of staff, and document how and when they can be contacted.

Test your staff's understanding of what's required during an incident through exercising. Consider using the NCSC's free 'Exercise in a Box' product to test your organisation's resilience and preparedness.

Document contact details of external people who can help you identify an incident (such as your web hosting provider), and read contracts to know what's covered. Ensuring that all relevant details are accessible and up to date will be invaluable during an incident.

2. Identify what's happening

The first step in dealing effectively with an incident involves identifying it. That is, how can you detect that an incident has occurred (or is still happening)?

The following may indicate a cyber incident:
·computers running slowly
·users locked out/unable to access documents
·messages demanding a ransom
·strange emails coming out of your domain
·redirected internet searches
·requests for unauthorised payments
·unusual account activity

These 10 questions can help you identify what occurred:
·What problem has been reported, and by who?
·What services, programs and/or hardware aren't working?
·Are there any signs that data has been lost?
·What information has been disclosed, deleted or corrupted?
·Have your customers noticed any problems? Can they use your services?
·Who designed the affected system, and who maintains it?
·When did the problem occur or first come to your attention?
·What areas of the organisation are affected?
·Is your external supply chain the cause/affected?
·What is the potential business impact of the incident?

Analyse antivirus/audit logs to help identify the cause of the incident. Use antivirus software to complete a full scan, and research any findings using trusted sources (such as police/security websites).

3. Resolve the incident

These actions will help your organisation get back up-and-running. You'll also need to check that everything is functioning normally, and fix any problems.

If your IT is managed externally, contact the right people to help (identified in Step 1). If you manage your own IT, activate your incident plan. This may involve:
·replacing infected hardware
·restoring services through backups
·patching software
·cleaning infected machines
·changing passwords

4. Report the incident to wider stakeholders

You are legally obliged to report certain incidents to the ICO. Check their website to find out which incidents qualify.

ico.
Information Commissioner's Office

Report to law enforcement via Action Fraud or Police Scotland's 101 call centre. The more who report, the more likely it is that criminals will be arrested, charged and convicted.

Keep your staff and customers informed of anything that might affect them (for example, if their personal data has been compromised by a breach).

Consider seeking legal advice if the incident has had a significant impact on your business/customers. If you have cyber insurance, they will be able to provide you with more advice.

5. Learn from the incident

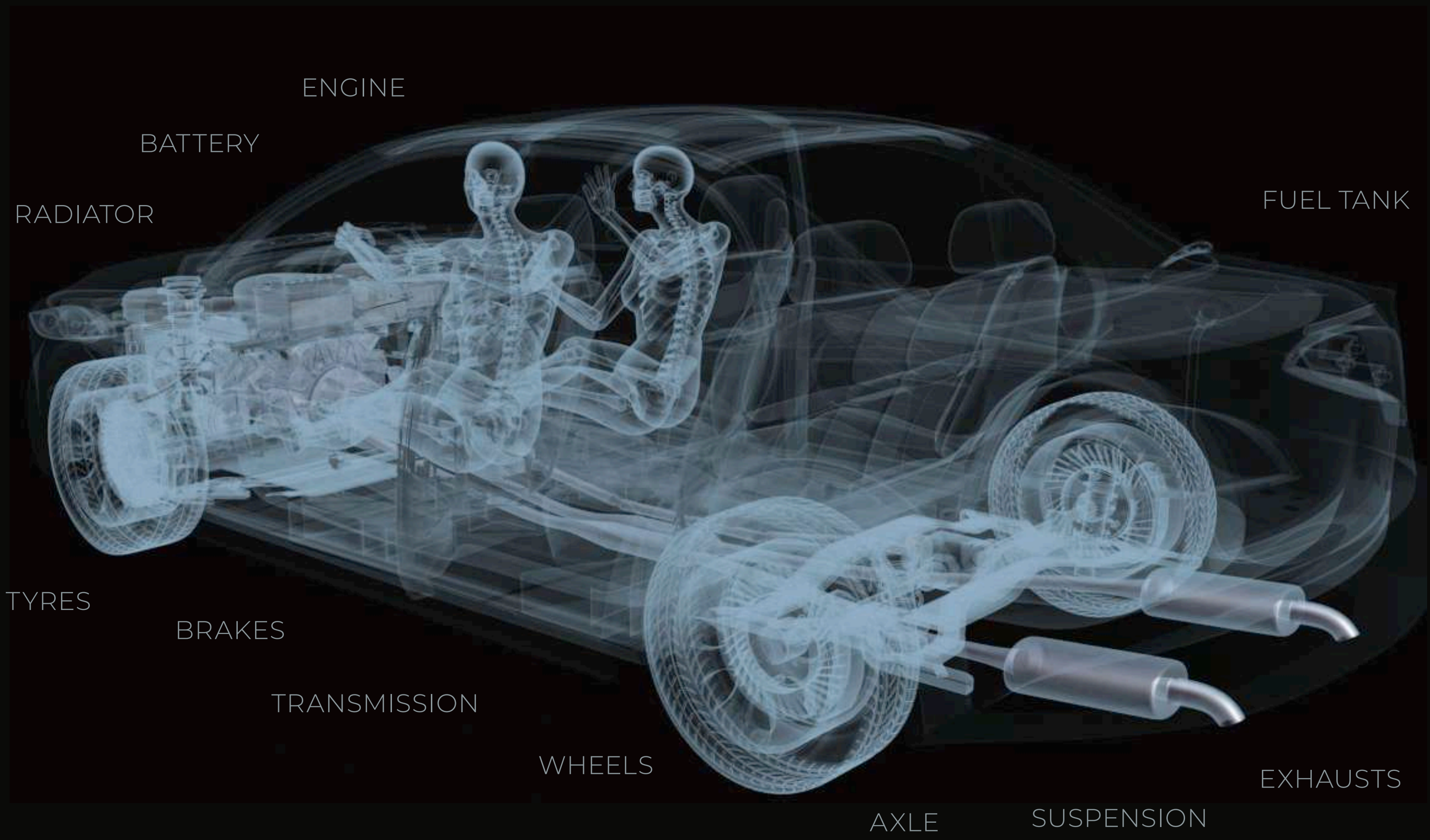
After the incident, it's important to review what has happened, learn from any mistakes, and take action to reduce the likelihood of it happening again.

Review actions taken during response. Make a list of things that went well and things that could be improved.

Review and update your incident plan (from Step 1) to reflect the lessons learned.

Reassess your risk and make any necessary changes to your defences.

For more information go to www.ncsc.gov.uk @ncsc


ENGINE
BATTERY
RADIATOR
FUEL TANK
TYRES
BRAKES
TRANSMISSION
WHEELS
EXHAUSTS
AXLE
SUSPENSION