Cybersecurity Trends

UK edition n.2 / 2021

SUPPLY CHAIN RISK MANAGEMENT, RANSOMWARE AND FRAUD, DIGITAL TRANSFORMATION, VIP INTERVIEW…

Contents

EDITORIAL

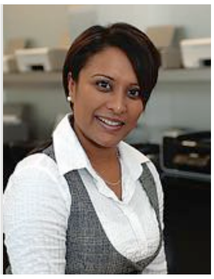
SUPPLY CHAIN RISK MANAGEMENT

60 SECONDS IN THE SPOTLIGHT

RANSOMWARE AND FRAUD

AT THE HEART OF TRANSFORMATION

The summer of security outlook, as unpredictable as the weather.



Authors: Marco Essomba, Raj Meghani,
Laurent Chrzanovski

In our last few editions, we talked about how nation-states want to defend themselves and attack others. Meanwhile, on the home ground, rampant threats like Ransomware highlights the challenges and subtleties of cybersecurity.

Currently, ransomware has become the biggest threat to British people and businesses.

A recent attack against a fuel pipeline operator has focused world leaders' attention on the scourge of ransomware, and the issue is considered serious enough to merit discussion at the recent G7 summit of world leaders in Carbis Bay, Cornwall.

While the ongoing political cyber-warfare is certainly tropical, we decided instead to focus our attention on businesses, especially as markets open up and organisations have ramped up their digital transformation

to adopt hybrid working models as well as their service models/route to market.

This propels '*cyber risk*' to the forefront now more than ever with added considerations being made to prepare and test at every stage to benefit from a robust risk management model.

According to Lindy Cameron, Chief Executive of the NCSC, "Far more worrying is the cumulative effect of a failure to manage cyber risk and the failure to take the threat of cyber criminality seriously. For the vast majority of UK citizens and businesses, and indeed for the vast majority of critical national infrastructure providers and government service providers, the primary key threat is not state actors but cybercriminals."

We wholeheartedly agree with Lindy's statement. In our view, cybercriminals are getting braver and bolder by upping their stakes when it comes to demands without really having to get any more creative with their methods. And that is due to organisations still not having caught up to addressing vulnerabilities and essentially leaving their doors wide open to uninvited, disruptive guests.

In this issue, you will hear from many of our industry peers, security thought-leaders and experts on the length and breadth of managing cybersecurity risks as a way to help organisations not only with their defences but also mindset and behaviour change when it comes to security.

The cyber risk management process is an ongoing one - it shouldn't be seen as a one-off. Every company in some shape or form will update their IT systems or integrate with more technology and software applications. This all adds pressure on the individuals whose job it is to manage and stay ahead of the cyber attackers.

Just because previous risks have been mitigated does not mean the organisation is safe. New risks will emerge as attacks get more sophisticated and vulnerabilities will be exposed leaving the attack surface open to advanced persistent threats.

The solution is fairly simple but requires a new transformation and mindset to make it tightly locked. Built into this mindset includes raising security awareness, ongoing training, use of automated and advanced cybersecurity solutions to respond and act quicker on cyberattacks, adopting a 'risk-free' culture to adopt an organisation's way of doing things traditionally to a more effective and secure approach - it's a lot to take in let alone implement.

We believe the time to act is now - reducing complexities is the enemy of security but in order to do so and stay ahead of the cybercrime, every business must work on the basis that they **WILL** suffer a breach.

Organisations must embed into their DNA that it's **EVERYONE's** responsibility to prevent cybercrime. The Ponemon Institute's research reveals that only 16 percent of CISOs said employees in their organisations were held accountable for cybersecurity today. Not good enough in today's day and time.

Small steps in eliminating weaknesses make a big difference in protecting organisations and their supply chains.

As the old adage by John Heywood goes - 'Rome was not built in one day'. ■

Supply Chain awakening.

Author: Nicola Sotira

We continue to receive, these days, lessons from these years in which we have all, probably, underestimated the issue of the supply chain and the importance of fully understanding the supply chain and the impacts there can be when one of the links in this chain breaks.

The pandemic has had a disruptive effect on several issues, such as digital, but above all, issues related to the world of healthcare and dependencies in the supply chain will undoubtedly require a complete review of rules and processes.

Raw materials and pandemia

'Restarting' is now the keyword in newspapers and news reports; all countries have plans and actions to start a new positive cycle in the global economy. However, the issue that is beginning to afflict some productive sectors is the availability of raw materials to be transformed into finished products. The interruptions, the closure made in some Chinese factories during the pandemic periods, have already created some slowdowns, for example, in the automotive sector. China, for example, is one of the leading suppliers of mechanical, textile and chemical industries. Many of the electronic components have their major production centres in China.

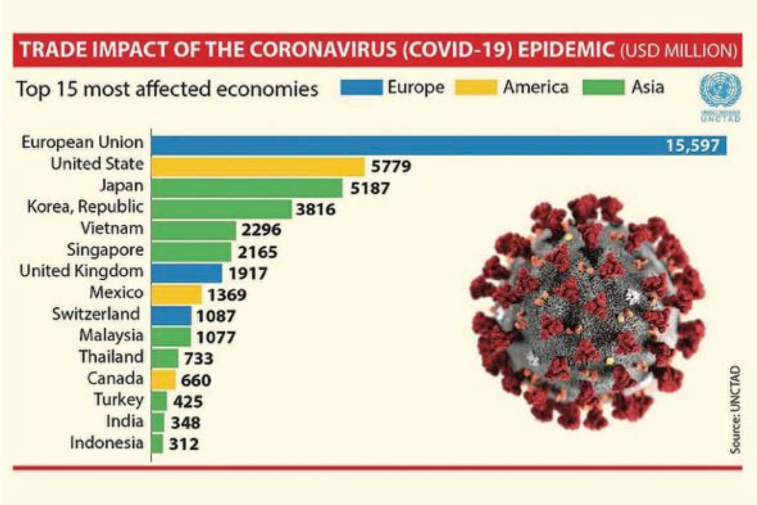
In recent years, all manufacturers have introduced plans that envisage a just-in-time approach, which in this circumstance has probably highlighted its fragility, requiring a rethink of the value chain.

Even here in this period, the issue touches on it as people are trying to renovate homes and buildings, where delivery times for some materials have increased dramatically. The problem, in this case, touches on iron ore material. For example, in Brazil, major mining facilities have suffered from staffing issues, and there have been slowdowns in reopening some sites.

In South Africa and India, the pandemic has led to substantial cuts in production, which is worth about 10% of the iron ore trade in these countries. To understand, then, how everything is connected in this

BIO

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



ecosystem is enough to think that even the collection of scrap iron has dropped dramatically; in this case, we consumers have also contributed, postponing our purchases of cars, appliances, renovations, and demolitions.

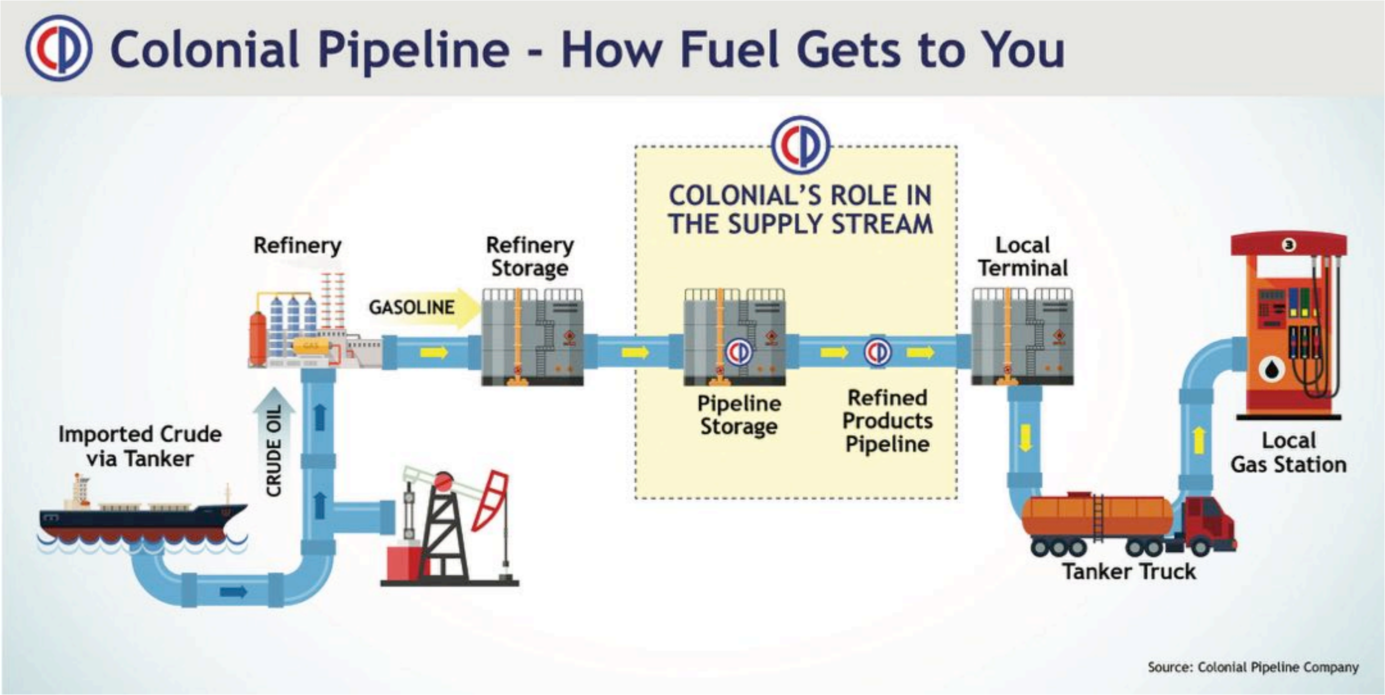
Cyber and supply chain

In May, filling up your car with gasoline in the U.S. was complicated both by lines at the gas pumps and by Americans' pockets. The average price of a gallon of petrol suddenly spiked, the reason being a ransomware attack on the Colonial Pipeline. This infrastructure is the largest oil pipeline in the U.S., with about 9,000 miles of pipes carrying fuel estimated at 3 million barrels per day. Cyber attacks on digital infrastructure and even a pipeline are connected to the network today and have increased dramatically over the COVID period.

Smart working and the massive use of digital technology have often widened the perimeter of companies, opening up potential entrances to attackers who have seized the opportunity. In the Colonial case, the attackers entered the network through a VPN account that allowed some users remote access to the corporate network. According to FireEye sources, the account was no longer in use at the time of the attack but still had valid credentials that allowed access. According to FireEye sources, the password was in a database of stolen passwords on the dark web. The employee was likely using the same password on different accounts, which, together with weak passwords, continues to be present in all organisations. In this case, we are talking about an employee in a remote access context, but in many other cases of similar attacks, remote connections belonging to consultants and suppliers who had access to the company network were used. Cybersecurity dynamics often influence the supply chain, but they have relevant consequences for both governments and civilian population in the above cases.

Step one: Increase visibility

At this particular time, when we are all making our contribution to the recovery, organisations must increase visibility into suppliers and their supply chain, especially for that cluster that is critical to the business. More governance needs to be applied to this cluster of suppliers and reporting KPIs identified. The best approach would be to digitise the entire control process and monitor vital metrics in real-time. This will allow the organisation to quickly assess the production and inventory issue and correct it at any


Colonial Pipeline - How Fuel Gets to You
COLONIAL'S ROLE IN THE SUPPLY STREAM
Imported Crude via Tanker
CRUDE OIL
Refinery
GASOLINE
Refinery Storage
Pipeline Storage
Refined Products Pipeline
Local Terminal
Tanker Truck
Local Gas Station

Source: Colonial Pipeline Company

time. The same goes for supplier issues that develop software; again, you will need to verify the quality of what is being delivered and ensure that suppliers are also implementing the organisation's processes and security policies. This monitoring process will provide you with greater visibility into second-tier suppliers and help improve the organisation's resilience.

Supply Chain Risk Management (SCRM)

The activities of an SCRM program relate to supply chain risk management and consist of the timely identification and assessment of events that may disrupt the supply chain to control risk exposure and minimise negative impact. The activity consists of the continuous development of strategies to contain and reduce the risk, then introduce appropriate preventive measures to limit the consequences as much as possible to ensure business continuity. An activity that must be supervised in any companies and fully integrated with risk management and business continuity activities.

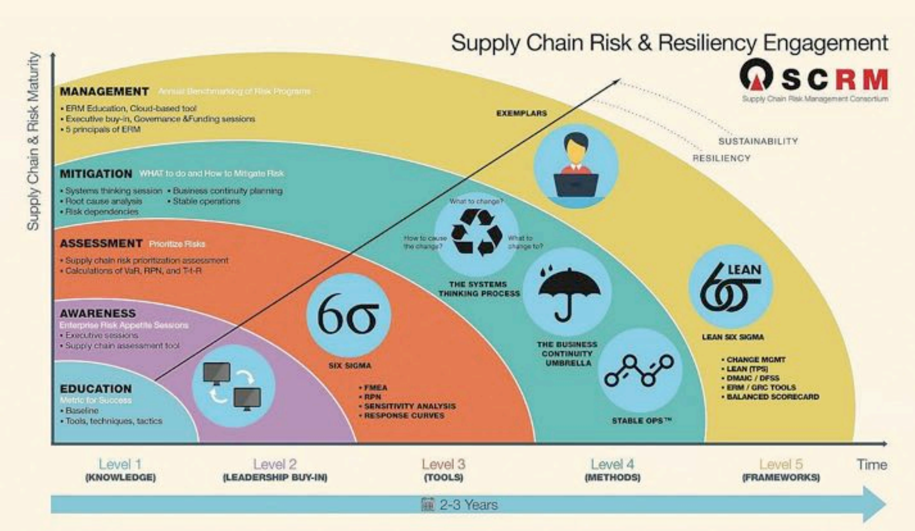
SCRM and Cyber

Increasing digitisation and dependence on suppliers leads to increased cybersecurity risk, and organisations must learn how to manage it and integrate it into the Supply Chain Risk Management program.

Although cybersecurity risks are on the rise and, as we have described, are increasingly associated with increased supply chain integration, these are not yet fully understood by organisations. In an increasingly digital economy, however, identifying and mitigating risk in the supply chain is one of the key features to ensure the resilience of the company's business. The problems in this new scenario are many; suffice to say that suppliers often have credentials and permissions to access corporate networks and applications from which malware can be inoculated. Moreover, as already happened, we could have the case of software providers that can distribute code with malware inside with the consequences that you can only imagine due to a cyber attack.

Companies, therefore, cannot limit themselves to controlling cyber risk only within their perimeter but must extend the approach to risk used in the company to the supply chains as well. The interconnectedness and continuous supply chain process certainly offer many benefits and, however, several risks that must be mitigated.

The importance of adopting a specific supply chain cyber security program to understand the main risks associated with supplying products and services and, above all, to assess the impact of the possibility that suppliers may have extended access to company resources and assets.


Supply Chain Risk & Resiliency Engagement
SCRM
Supply Chain Risk Management Consortium
Supply Chain & Risk Maturity
MANAGEMENT Annual Benchmarking of Risk Programs
• ERM Education, Cloud-based tool
• Executive buy-in, Governance &Funding sessions
• 5 principals of ERM
MITIGATION WHAT to do and How to Mitigate Risk
• Systems thinking session
• Root cause analysis
• Risk dependencies
• Business continuity planning
• Stable operations
ASSESSMENT Prioritize Risks
• Supply chain risk prioritization assessment
• Calculations of VaR, RPN, and T-t-R
AWARENESS
Enterprise Risk Appetite Sessions
• Executive sessions
• Supply chain assessment tool
EDUCATION
Metric for Success
• Baseline
• Tools, techniques, tactics
6σ
SIX SIGMA
• FMEA
• RPN
• SENSITIVITY ANALYSIS
• RESPONSE CURVES
What to change?
How to cause the change?
What to change to?
THE SYSTEMS THINKING PROCESS
THE BUSINESS CONTINUITY UMBRELLA
STABLE OPS™
EXEMPLARS
SUSTAINABILITY
RESILIENCY
LEAN
LEAN SIX SIGMA
• CHANGE MGMT
• LEAN (TPS)
• DMAIC / DFSS
• ERM / GRC TOOLS
• BALANCED SCORECARD
Level 1 (KNOWLEDGE)
Level 2 (LEADERSHIP BUY-IN)
Level 3 (TOOLS)
Level 4 (METHODS)
Level 5 (FRAMEWORKS)
Time
2-3 Years

Conclusion

The supply chain will be a crucial part of the firm's business, and it will be necessary to find ways of meeting the challenges of this new economic recovery. It will be required to undertake actions to increase transparency in these supply chains by identifying, in some cases, alternative sources of supply, also working on the review of the theme of warehouse stocks.

Moreover, we need a careful assessment of the risks related to the impact of cyberattacks. In the last year, attacks have shown how it can hit and target this area, sometimes as a gateway and other times as the primary target. ■

Eliminating the weakest link –

A practical outlook to curbing 3rd party risks.

Authors: Raj Meghani and Marco Essomba

All businesses face and have been increasingly inundated by risks – legal, financial, reputational and the rest. The magic bullet is to move to a 'risk free' future. With the current COVID-19 pandemic challenges, the surge in sophisticated cybercrime now targeting SMEs to the large enterprises has become a pandemic in itself.

Cyberattackers look for weaknesses in a businesses' infrastructure and then go about exploiting those vulnerabilities in a number of different ways. Some are immediate, others more planned and bide their time to cause maximum damage. Complexity is the enemy of security and with this challenge, cybersecurity innovation to protect an organisation's ecosystem and that of its supply chain becomes even more paramount.

In the last edition of this publication, we took a deeper look into nation state attacks and the theft of intellectual property causing wide economic disruptions with devastating effects. It's not just data theft and attacking its integrity that was the prime goal here but the widespread chaos that would erupt as industrial systems were compromised. Added to this was the angle of risk amplified by cyber attackers on targeting 3rd and 4th party supply chains to infiltrate and exploit commercial businesses widening the cyberattack surface yet again. A research study by the Ponemon Institute (Cost of Cybercrime, 2019) highlights that attacks of this nature could account for 23% of the total value at risk for organisations over the next 3 years.

Today more than ever, it is **ESSENTIAL** to have a robust cyber risk management strategy in place. Collaborating with partners in supply chains moves businesses a step closer to protecting their entire *business* ecosystem. Having a security defence in depth layered approach to fight off malicious attacks should form a critical part of every organisation's blueprint – reputational damage is hard to come back from.

The starting point is to understand the current security landscape for the business and evaluate its appetite for risk. Risk is unavoidable – some risks may be deemed acceptable whilst others may be outside of your control. Raising cyber awareness in the workplace through training and development, working with different business areas outside of the IT department, having in place action plans to handle breaches, putting in place preventative measures to stop complex and advanced persistent threats all have a part to play too.

The landscape can be broadly divided into IT infrastructure, applications and people. The latter of these is the weakest link as we see more and more sophisticated cybercrimes involving phishing and insider threats.

Add to that landscape 3rd party supply chain data breaches which may force organisations to respond to incidents that are outside of their operations or introduced from an unknown source. And although the organisation may not directly have to handle the breach (regulatorily), reputational damage due to being tagged 'guilty by association' may occur. Furthermore, this also puts an organisation's customers/consumers at risk of being breached regardless of where the breach originally occurred.

It remains vital on the outset to ensure that suppliers' approach to cyber risk fits with an organisation's approach before engaging with them, as this becomes more challenging to address once onboarded as the service provider. There may also be cost implications as well as time and manpower hours wasted.

So what can be done to mitigate these risks?

Below we list some best practices to gauge whether your suppliers remain within the acceptable risk appetite.

Getting to know your suppliers - The Dos:

Engagement workshops:

As a precursor to any contractual relationship, a capability and operational scoping workshop is a good measure to understand the potential supplier's security aptitude and the wider risk exposure. This helps businesses make learned business risk decisions and understand the service structure including other third-party reliance by the supplier and what measures are needed to put in place to secure against these any additional risks.

Having an overview of associated dependencies to deliver important business services is key to understanding the cyber risks.

Certifications/Accreditation:

Based on the intended work, time and other factors; sometimes asking for relevant recognised standards or certifications is an excellent way to assess a supplier. For example, ISO9001 or ISO27001 certifications to assess quality of information security standards. In certain cases, requesting audit reports or asking what certifications they are working towards can be a good indicator of posture and maturity.

If the purchasing organisation is accredited with a certain certification/ standards, it is also advisable to have a supplier who holds the same certification as this would make a great fit strategically speaking.

Detailed Service Level Agreements (SLAs):

When it comes to putting agreements in place, it is also best to include policies and contingencies related to performance as well as breach of SLAs. This combined with frequent reviews clauses and necessary audits that include all security ownership elements should be ironed out from the outset.

Simulate and test-run cyber incident breach scenarios:

Having and deploying an incident response playbook for addressing 3rd party breaches scenario should be as important as creating standard business direct threat response plans. Just as the SLAs, it should contain elements of training, planning and accountability mapping when it comes to communication to stakeholders or reporting to authorities.

This should be stress-tested using simulated incidents.

Getting to know your suppliers - The Do Nots:

- Rely on a 'one-size-fits-all questionnaire to do the supplier scoping exercise.
- Depend on suppliers who are too commercially or technologically focused - try to find partners that understand a fair balance owing to shared responsibilities when it comes to breaches or incidents.
- Engage with providers where organisations cannot establish a good relationship across the supplier's leadership or senior management - this applies when the work undertaken is across critical and sensitive industries.

Special considerations - The unknown parties:

There are additional risks to consider to the organisation's operations when extended (fourth or fifth) parties are added to the fold. Suppliers may subcontract their operations to minimise resourcing or keep costs down. A lot of these account as hidden risks and are difficult to identify.

One consideration should be to assume and accept that extended parties may be involved and ascertaining this information in the scoping or engagement phase with suppliers and subsequently adding this scenario to the incident response planning playbook.

Final remarks:

As a best practice, it is also critical that the risk profile of each third party should be measured and continually assessed to ensure they remain within risk appetite. The keyword to observe is **'continually'** monitored and reviewed.

Risk assessing and managing 3rd party supply chains is complex and gets more complicated as firms scale up and use additional 3rd parties who may all have different operational modes.

No matter your industry, from the financial to the retail sector, consider the risks of your digital assets moving through vast ecosystems.

When it comes to risk management, firms cannot rely on an all-purpose method but should do so using a dynamic method with a broad outlook. ■

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

Do you know how strong the links are in your supply chain?

Author: Ian Kennedy-Compston

Most businesses rely on some sort of supply chain to deliver goods, services or systems for their customers. Historically, perhaps, the major concern with a supply chain might have been the failure to provide parts in time, interrupting the manufacturing process and affecting supply to customers. Today, that's only one area of concern for any business which relies on suppliers. Modern businesses often outsource many of the services which might have been in-house, such as research and development, marketing, distribution, customer service, finance and recruitment, bringing potential security headaches for business leaders at a time when there are tighter regulations around data protection.

BIO

Ian is CEO and Founder of EnterpriseRed, established in 2013, which provides the full spectrum of solutions and services from a managed SIEM to automated PEN testing and everything in between to SMEs and enterprise customers.

With over 2 decades of specialist IT and Telecommunications experience, Ian is fast becoming a leading trusted advisor in cybersecurity and the driving force to position market leading cybersecurity solutions to the market.

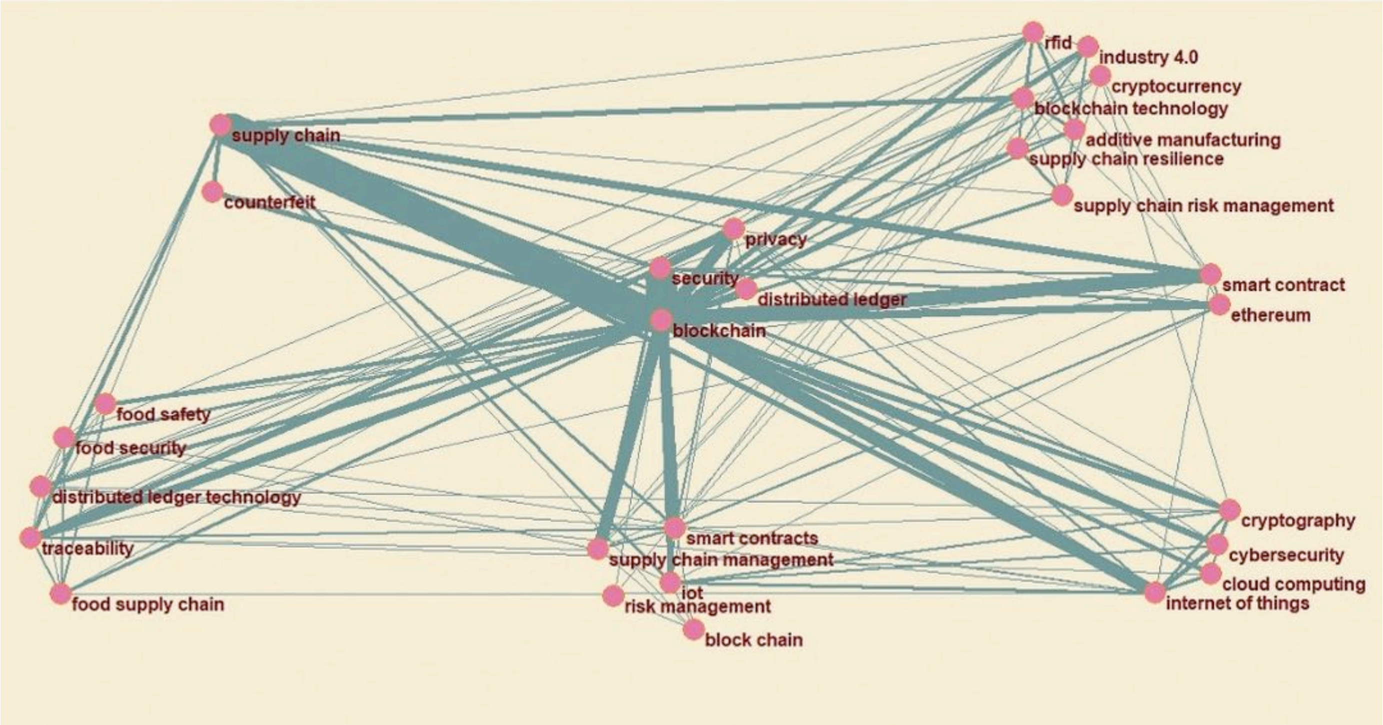
Ian brings clarity to businesses through his collaborative approach supported with the latest cybersecurity emerging technologies.

Most of a company's suppliers have suppliers of their own, and those suppliers have theirs, and so on. It's an extended network which would take an almost forensic approach to fully understand and identify. Business leaders simply cannot know all the organisations they're linked to or depend upon in some way or another or have full confidence that those businesses are run in a way which doesn't pose potential hazards to them or others in the chain.

From a cybersecurity perspective, a supply chain of any size can present major risks. Each link in the supply chain can have vulnerabilities which could be exploited or prove unreliable at any point, causing disruption and damage to other members in the chain, potentially catastrophically from a financial or reputational perspective, not to mention the regulatory repercussions arising from responsibilities under the General Data Protection Regulation which came into force in 2018.

A number of high-profile attacks has demonstrated that attackers can, and will, exploit the weakest link in a supply chain. Just last month, it was reported that a Volkswagen marketing partner had suffered a data breach with the auto-maker's Audi business confirming that hackers had obtained personal data involving some 3.3 million current and potential Audi customers across the USA and Canada. It was said that the data, gathered over a five-year period, was in an electronic file that the VW supply chain partner had left unsecured.

This is the latest worldwide household name having had to announce data breach issues not directly caused by their own organisation. Even though the breach was not as a result of a failure of their own IT infrastructure, it has had a significant impact in terms of reputational, as well as financial, damage.



When any business appoints a supplier the procurement due diligence process should cover cybersecurity checks to satisfy companies that all legal and regulatory requirements are at least met if not exceeded. But this shouldn't be a "one and done" process. It's important that suppliers are closely monitored to ensure they use the right tools to predict, prevent and detect cyber vulnerabilities to protect customers and others in the supply chain.

Understanding a supplier's cybersecurity posture is important, especially where customer data is being shared. As a minimum, the initial procurement process should ask for proof of recent penetration testing by suppliers, ideally with the test report shared showing where areas of vulnerability exist and what remedial action is being taken to improve robustness.

But it's not just system vulnerabilities which need to be considered. One of the greatest cybersecurity risks comes from an organisation's people, either through human error causing a breach or allowing hackers to gain access to data. In fact, according to a study by IBM, human error is the main cause of 95% of cybersecurity breaches. In effect, a whopping 19 out of 20 cyber breaches are said to be the result of unintentional actions, or lack of action, by employees which result in either causing or allowing a security breach to take place or spread. Examples include downloading malware-infected attachments in emails to failing to use robust passwords which leaves data vulnerable.

Again, the procurement process should ideally cover what cybersecurity training is provided to employees to gain further confidence in a supplier's robustness. Any company that conducts regular penetration testing and strengthens their team's cybersecurity training and monitoring stands a greater chance of blocking cyberattacks or reducing accidental data breaches, which should provide greater peace of mind to other businesses in the supply chain and regular check-ups through the life-cycle of a supplier contract should be standard practice. ■

Monitoring one's own supply chain.

Author: Massimo Cappelli

Securing your supply chain is not an easy task. By supply chain, in this article, I mean all those suppliers of services or products, external to the company, whose contribution is necessary for the production of value.

According to statistics produced by the Ponemon Institute and Recorded Future, 59% of organisations have suffered a data breach, initiated by their own third parties. Controlling one's own suppliers is not a new issue. Supplier control must follow a life cycle: a real programme that could be divided into three main phases: Entry; Permanence; Exit.

BIO

Massimo is Operations Planning Manager within the 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 with in the Information Protection Department. After economic studies, he obtained PhD in "Geoeconomics, Geopolitics and Geohistory of border regions" focus on Critical Infrastructure Protection Programme and a Master in "Intelligence and Security Studies". In the 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.

1. Entry:

Before embarking on cooperation initiatives, a whole series of checks are usually carried out concerning the soundness and reliability of a company. They check the balance sheet, ownership, any outstanding debts, collaboration with other companies, reputation, etc. etc. From this type of control, with the passing of time, we have moved on to checking the presence of certifications of conformity and quality of the product and service. With regard to information security, ISO2700x certifications are often required.

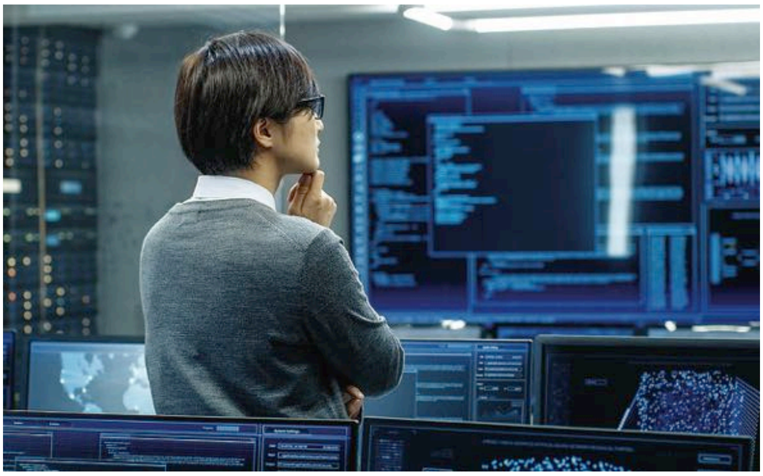
The more forward-looking require the presence of Business Continuity and Disaster Management systems. In some cases, the supplier, if he wants to collaborate with some companies, must also allow very invasive testing of their products and services. This is not always allowed or possible, especially in the technology department. The supplier has to give consent for these tests to be carried out and this is not always the case. In addition, performing these tests, such as dynamic and static analysis of software, are very expensive and require very high technical skills. Further checks must also be made on potential compromises of the provider itself. There may be information on the web about data breaches that have occurred against the supplier and this information must also be taken into account.

2. Permanence:

The next stage is permanence. The company must continue to monitor the supplier and verify that its reliability and robustness is maintained. In terms of information security, if the supplier accesses the company's systems, it must be able to be monitored and controlled. It must have dedicated VPNs. Access logs must be collected and analysed. Who accesses, where they access, what they access, when they access, why they access. The same applies to the platforms that are acquired. You should monitor the activities of the platforms, know all the iterations they perform within the process, what information they process and where they process it (on company data centres, in the cloud, at the supplier's data centre, etc. etc.). All this monitoring should be real-time with alerting systems ready to go in case of anomalies.

If a supplier changes device or geographical region from which it connects, if a platform does not just process the information necessary for its activities, etc. etc. the system must be able to raise an alarm flag for further checks. These analyses require more or less automated data collection and analysis capabilities. They also require high skills. Therefore, it is important to prepare one's own systems for the collection of these data and their processing. This concerns the monitoring of day-to-day activities with the company. It is also necessary to consider the external perimeter of the company and to carry out preventive monitoring of events that impact the supplier and could also impact our company. If a supplier suffers a data breach, the company may be indirectly affected. A web intelligence gathering system, in all its meanings, is useful to keep an eye out and intercept potential signs of compromise. A simple method would be to correlate one's own supplier list with intelligence sources on data breaches in order to automatically alert the company when news about its supplier is published. Obviously the more intelligence sources you have and the more they are profiled to look for information on your supply chain, the more effective the result will be. However, this could be very costly.

The same operation should be carried out on all suppliers and not only on the suppliers of Information Systems. The most strategic information for the company may reside in the computers of the top management and in those of their external collaborators, such as legal consultants, financial advisors and so on. It is advisable to monitor all suppliers and try to categorise them according to the information they manage.



Supplier monitoring requires strong coordination and close collaboration between different functions. This also requires process integration between the business, procurement, administration and control and security functions. Screening time must be kept to a minimum in order not to burden the procurement process.

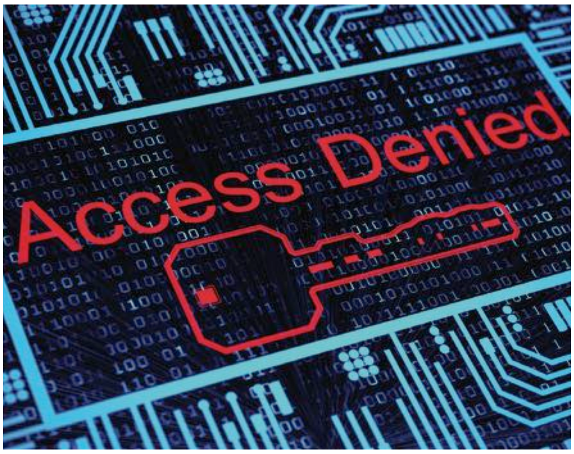
3. Exit:

The final stage is to close the contract. This means blocking access to VPNs and closing any information flows to and from the supplier. This step is very important. It is often prolonged and overlooked, especially if the supplier is not strictly in the IT world where there is a greater awareness of these issues.

So you find access to shared folders, VPN still active and information flows still existing between the company and suppliers that can range from HR to commercial or financial.

The monitoring part obviously cannot be neglected. If the life of the supplier in the company ends in time, it would be precautionary to keep intelligence monitoring for at least one year after the contract has ended. Even if the relationships have ended, there may still be company information around. A year is neither a lot nor a little, it always depends on the monitoring and intelligence gathering capacity a company has.

It is very important that in all three phases there is a strong awareness component for all actors involved. The perimeter of awareness is extended to suppliers and it must be ensured that they have assimilated the company's security policies and that they comply with them. ■



Interview with Paul Delacourt.

Author: Raj Meghani

1. RM: What would you say are the biggest cyber-security trends in the last decade?

PD: Cybersecurity trends race at a speed other trends and threats simply do not, and any list is necessarily incomplete as soon as it is published. Over the last decade, we have seen threats from the exposure of global payment systems, to the potentially catastrophic insider risks posed by Edward Snowden, to the loss of consumer datasets from enormous banks, merchants and retailers. The 2014 Sony Pictures hack exposed the risk to private sector entities from nation state actors, and the Office of Personnel Management breach exposed the same risk to government data. WannaCry and NetPetya attacks only foreshadowed more recent attacks to government and critical infrastructure.

2. RM: How have you seen the FBI transform its operations in light of nation state attacks?

PD: The FBI has seen a generation of FBI employees begin their careers in the aftermath of 9/11. Those same employees are now turning their considerable expertise to the risks of counterintelligence and cybersecurity. The FBI's Cyber Division continues to rapidly evolve to address threats locally, nationally and internationally, through technology, interagency partnership, critical infrastructure protection and outreach and engagement. Emphasising this transformation, during Congressional testimony FBI Director Christopher Wray recently compared ransomware attacks to 9/11.

BIO

Paul Delacourt recently retired from the Federal Bureau of Investigation after 25 years of government service. Paul retired as the Assistant Director of the FBI Strategic Realignment Office, after being the chief executive in both the Los Angeles and Honolulu field offices for six years. Prior to a decade as an executive, Paul developed expertise in criminal and counterterrorism investigations and international operations. Paul joins the Red River Technology managed services division in the Chantilly, VA office, as Director of Programs.

3. RM: What do you currently see as the biggest security challenges facing intelligence and law enforcement agencies?

PD: Cyber operations lower the barriers to entry into the world of counter intelligence and economic espionage for nation state and non-nation state actors alike. Resourcing may always be a challenge for intelligence and law enforcement agencies, while coordination of asset response, threat response and counter-cyber operations continue to improve. Agencies often move beyond the traditional "speed of government," but are sometimes limited by the speed of legislation, or the tyranny of the urgent. Trusted relationships with private sector partners, ahead of a crisis, have dramatically improved. Continuing to develop widespread interagency dialogue with potential victims, sectors, academia and industries remains critical.

4. RM: Can you highlight key areas where you feel there are opportunities to improve in the ways we address cybersecurity challenges?

PD: Cybersecurity must be addressed by a "whole of society." From basic cyber hygiene by the end user, to technology developments, to attribution and accountability for bad actors. There is a healthy friction and debate in our society between privacy and public safety regarding encryption and lawful government access. A cautious and thoughtful way-forward involving technology, negotiated resolutions and legislation will improve cybersecurity, noting that bad-actors and rogue nations will always get a vote.

5. RM: What do you see as the emerging cybersecurity threats we will face in the next decade?

PD: It seems like ransomware is having its moment. The attacks on Colonial Pipeline and JBS meat company have brought greater public attention to a spate of 2021 cyberattacks. How long this phase lasts is yet to be seen. Emboldened actors in the wake of SolarWInds, engagement of cybersecurity insurance, and payments of ransom complicate the problem, but the greater awareness and related network protection efforts, along with recent law enforcement seizures of proceeds may stem the tide.

Red River Chief Technology Officer Tim Rod recently identified other trends and challenges: the impact of the pandemic and realignment of budgets on digital transformation, particularly as [companies, industries and agencies] shift to remote work. With this transition, and risks to the supply chain, security technologies take the forefront and are being implemented more than ever before.

And finally, the four-way intersection of the Internet of Things, 5G, encryption, and quantum computing over the next decade will lead to trends, risks, challenges, opportunities and advancements that I can't predict!

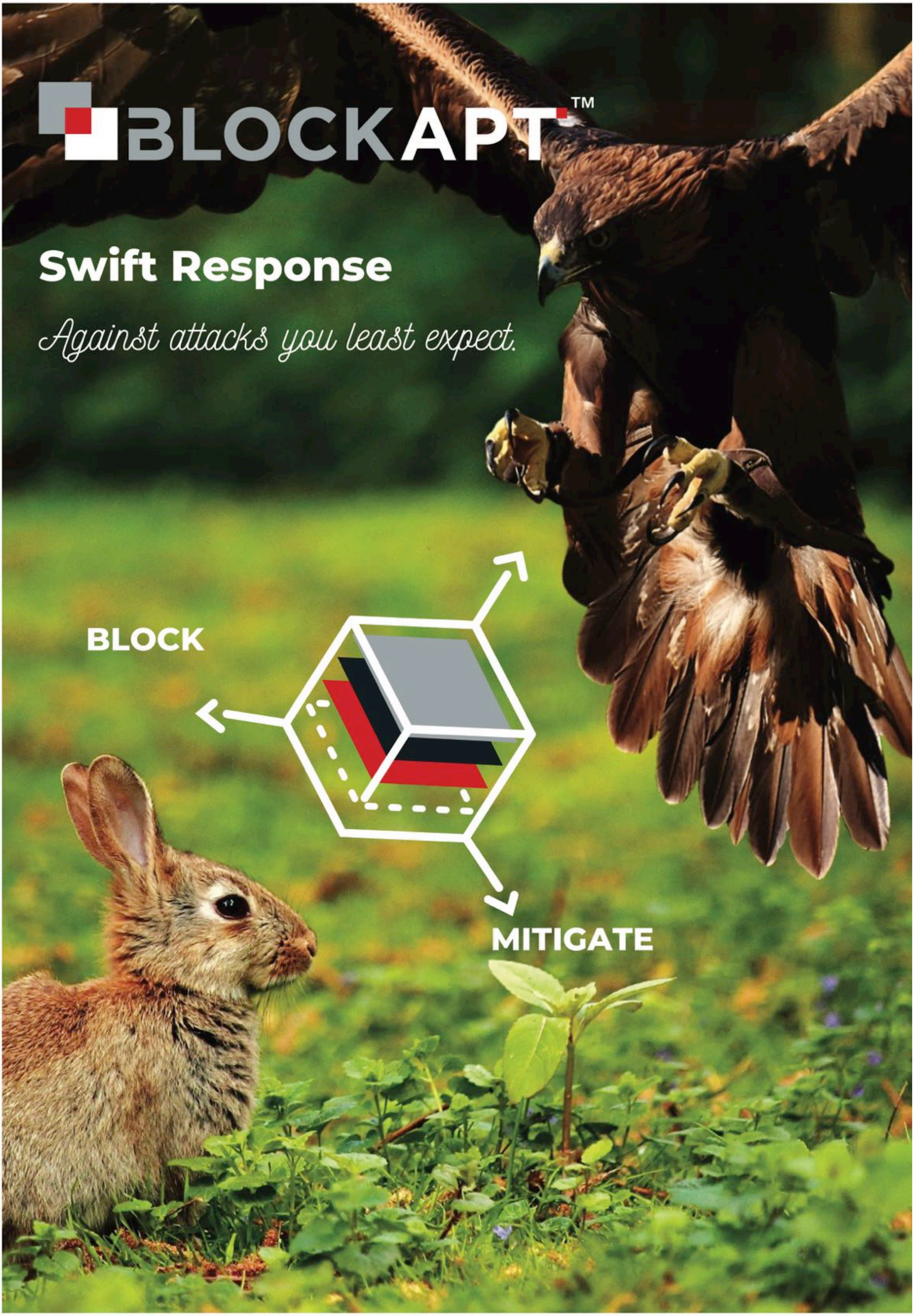
6. RM: What are you looking forward to in your next adventure?

PD: After 25 years in the intelligence and law enforcement communities, I am eager to take lessons, skills and experiences learned over a career, and apply them in a new way, while still protecting people, assets, intellectual property, and driving efficiencies and innovation. Red River will offer me an opportunity to add value for a vast variety of commercial and government clients. ■

BLOCKAPT™

Swift Response

Against attacks you least expect.



A devastating tale of Ransomware in 2021 –

A brief look into the CDPR attack and the ongoing aftermath.

Author: Marco Essomba

As an avid game, I have been following this story closely. But here is a bit of context before I go into the details.

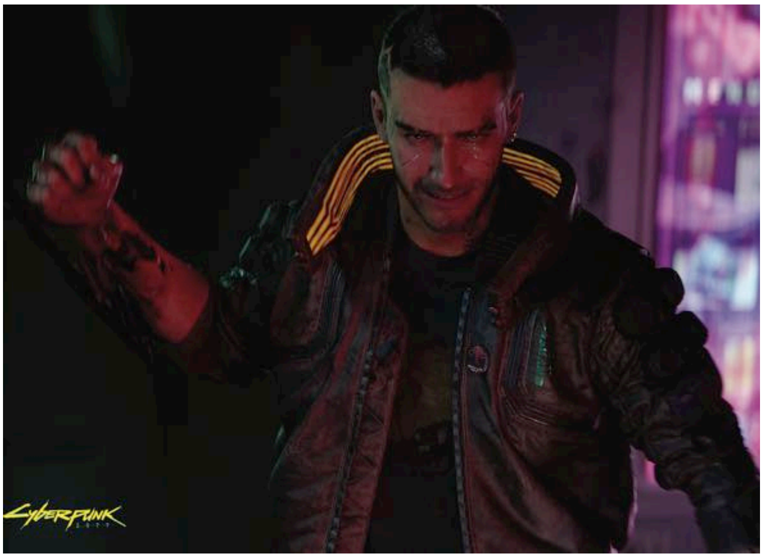
Based out of Poland, CD Projekt Red (CDPR) is the developer of critically acclaimed RPGs like The Witcher franchise and most recently Cyberpunk 2077.

The Witcher 3 RPG is perhaps arguably the most immersive game I have ever played to this date and remains the gold standard in the industry. So when Cyberpunk 2077 was announced in 2012 from the gaming community's beloved studio, the masses were eagerly awaiting the next masterpiece.

A disastrous start:

Upon release, Cyberpunk 2077 was not the Blade Runner-Esque immersive title we were hoping for. The game released a buggy mess, unfinished and riddled with technical glitches as well as frame-rate issues. Subsequently, Sony Playstation (PS) pulled the title from its stores and issued refunds. Media and community outrage aside, stocks plummeted and investigations opened up. Apart from this many factors such as employee crunch-time, board decisions and internal rifts became public. As a result, lawsuits were filed and we also saw key technical leads leave the studio.

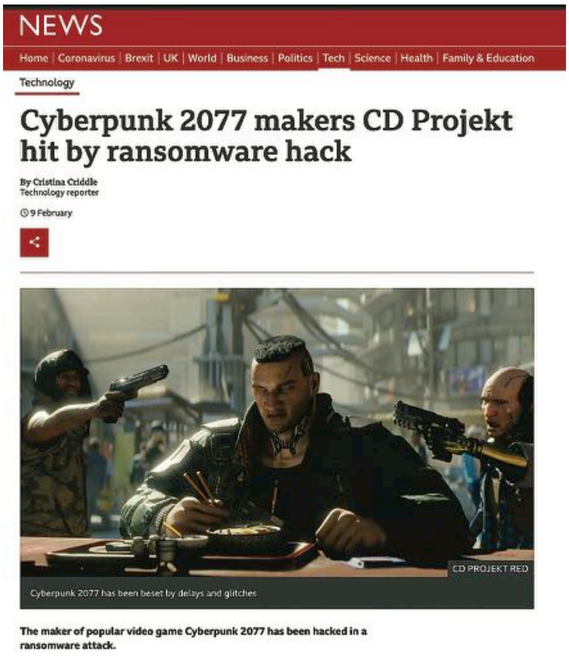
But CDPR finally admitted to the faults and then set out a roadmap and promised to continually fix the game with a dedicated team working on updates (patches). Slowly, it seemed like they were on the right track to redemption as patches began rolling out.



Then the Ransomware happened:

It seems like CDPR just cannot catch a break!

If we roll the clock back a couple of months now, in the first couple of weeks of February 2021, CD Projekt Red was hacked.



NEWS

Home | Coronavirus | Brexit | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Cyberpunk 2077 makers CD Projekt hit by ransomware hack

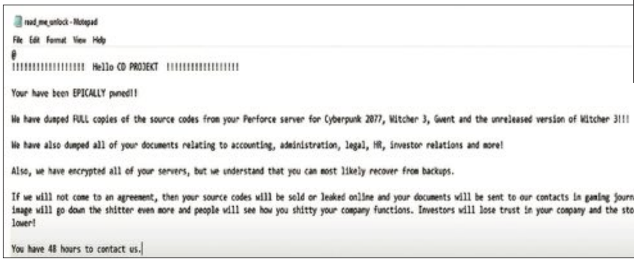
By Cristina Criddle
Technology reporter

9 February

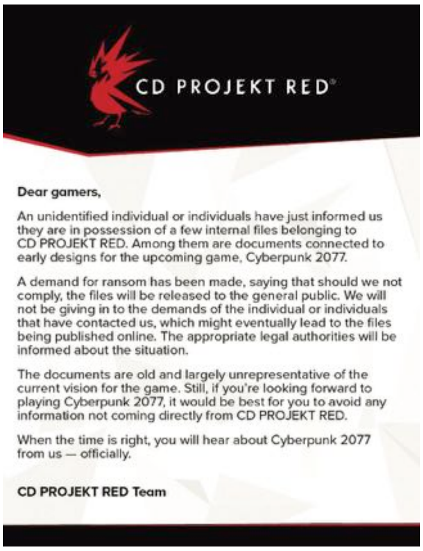
Cyberpunk 2077 has been beset by delays and glitches

The maker of popular video game Cyberpunk 2077 has been hacked in a ransomware attack.

A third-party group got access to a variety of information and published the following text saying that they (CDPR) have been pawned and full copies of source codes for all their digital assets including Cyberpunk 2077 have been dumped online.



```
@
!!!!!!!!!!!!!!!!!! Hello CD PROJEKT !!!!!!!!!!!!!!!!!!

Your have been EPICALLY pwned!!

We have dumped FULL copies of the source codes from your Perforce server for Cyberpunk 2077, Witcher 3, Gwent and the unreleased version of Witcher 3!!!

We have also dumped all of your documents relating to accounting, administration, legal, HR, investor relations and more!

Also, we have encrypted all of your servers, but we understand that you can most likely recover from backups.

If we will not come to an agreement, then your source codes will be sold or leaked online and your documents will be sent to our contacts in gaming journalism. Your public image will go down the shitter even more and people will see how you shitty your company functions. Investors will lose trust in your company and the stock will dive even lower!

You have 48 hours to contact us.
```



CD PROJEKT RED®

Dear gamers,

An unidentified individual or individuals have just informed us they are in possession of a few internal files belonging to CD PROJEKT RED. Among them are documents connected to early designs for the upcoming game, Cyberpunk 2077.

A demand for ransom has been made, saying that should we not comply, the files will be released to the general public. We will not be giving in to the demands of the individual or individuals that have contacted us, which might eventually lead to the files being published online. The appropriate legal authorities will be informed about the situation.

The documents are old and largely unrepresentative of the current vision for the game. Still, if you're looking forward to playing Cyberpunk 2077, it would be best for you to avoid any information not coming directly from CD PROJEKT RED.

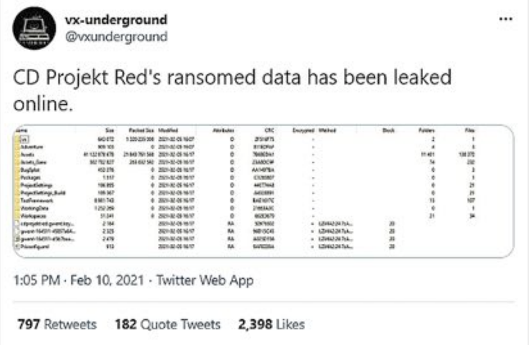
When the time is right, you will hear about Cyberpunk 2077 from us — officially.

CD PROJEKT RED Team

Alarmingly, it also mentioned they have documents relating to accounting, administration, legal, human resources, investor relations and more.

All signs originally pointed to a ransomware attack and the motive was for CDPR to pay out to this group for them not to leak the information. The company released the following official statement to the public and took a bold stance of not giving in to the hackers.

As CDPR did not comply with the ransom attempt, the hacker group ended up going public. This was widely mentioned on Twitter and shortly after all the mentioned content and assets went online for auction.



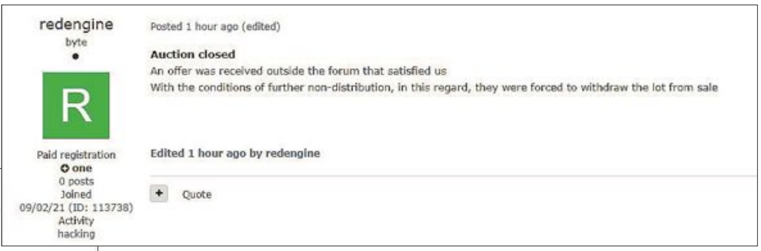
vx-underground
@vxunderground

CD Projekt Red's ransomed data has been leaked online.

1:05 PM · Feb 10, 2021 · Twitter Web App

797 Retweets 182 Quote Tweets 2,398 Likes

The hacking group listed all the hijacked assets for the starting price bid of $1 million dollars and the buyout price of $7 million dollars. Now, it was unclear whether the hacker group received any bids but a few days later the auction was closed with the following message.



redengine
byte

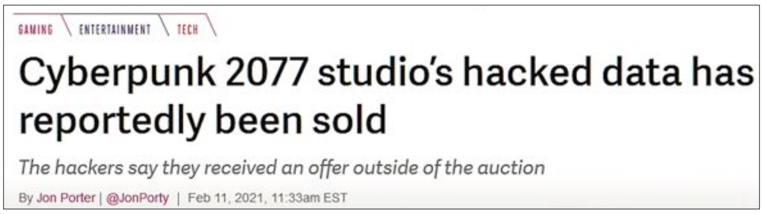
Paid registration
one
0 posts
Joined
09/02/21 (ID: 113738)
Activity
hacking

Posted 1 hour ago (edited)

Auction closed
An offer was received outside the forum that satisfied us
With the conditions of further non-distribution, in this regard, they were forced to withdraw the lot from sale

Edited 1 hour ago by redengine

Now, this almost made it seem like a third-party company either bought this out or maybe the auction did not go as well as they planned so they accepted a bid well below the starting price of a $1 million dollars offer. It is hard to say what really happened.



Cyberpunk 2077 studio's hacked data has reportedly been sold

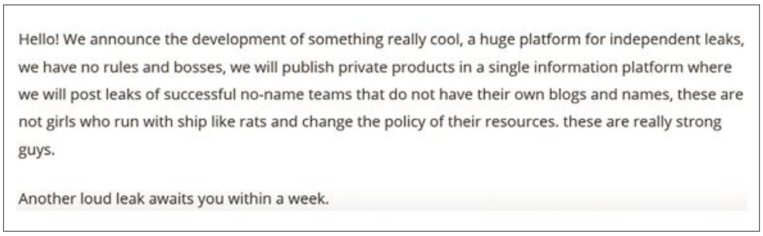
The hackers say they received an offer outside of the auction

By Jon Porter | @JonPorty | Feb 11, 2021, 11:33am EST

All the above happened back in February and since then we haven't heard much about this situation except how it has been impactful in affecting CDPR's release of the much needed (and promised!) patches for Cyberpunk 2077 as well as a lot of employees who had their personal information compromised.

But all in all, it looked like the source code for the games and other assets did not end up leaking, well at least not until recently. At the end of April, a dark-web based hacking website announced some major changes coming to them. They released the following post.

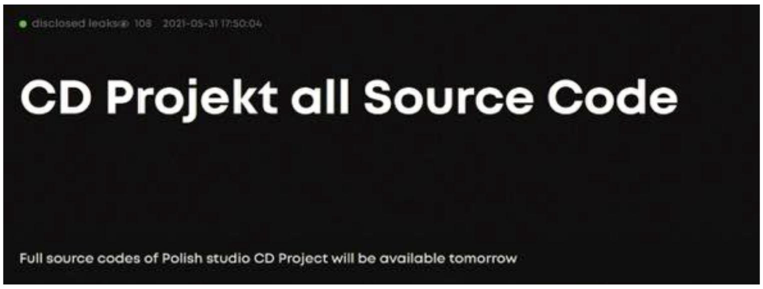
Alarmingly indeed but at the time nobody connected this to CDPR. However, by the end of May, we witnessed what looked like the sources codes from CDPR that were originally hacked back in February had been



Hello! We announce the development of something really cool, a huge platform for independent leaks, we have no rules and bosses, we will publish private products in a single information platform where we will post leaks of successful no-name teams that do not have their own blogs and names, these are not girls who run with ship like rats and change the policy of their resources. these are really strong guys.

Another loud leak awaits you within a week.

now uploaded to this new website with some of the downloads already being available

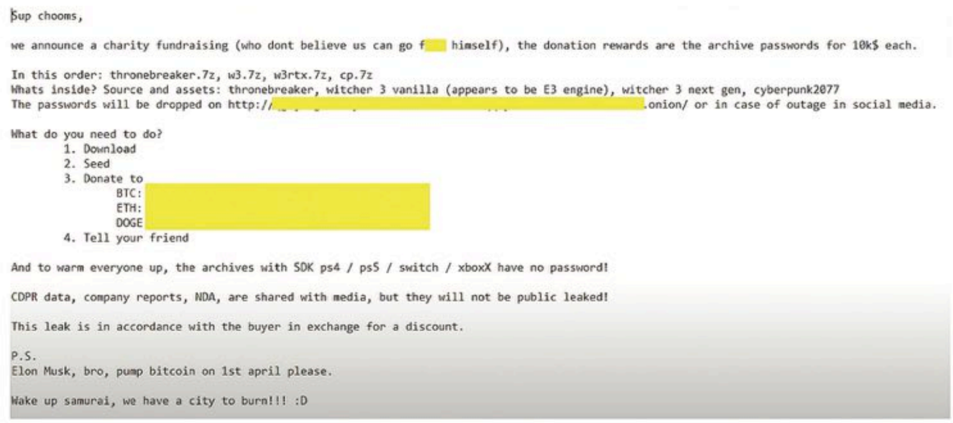


CD Projekt all Source Code

Full source codes of Polish studio CD Project will be available tomorrow

As of now, downloads for the versions of the next-generation upgrade of the hit game Witcher 3, source code for Cyberpunk 2077 game and fully open SDKs for PS4 and PS5 are available. However, those who have downloaded the torrent version of these have found out that the files are password protected and not giving full-on open access to them.

A new note released alongside these downloads read the following.



```
Sup chooms,

we announce a charity fundraising (who dont believe us can go f[redacted] himself), the donation rewards are the archive passwords for 10k$ each.

In this order: thronebreaker.7z, w3.7z, w3rtx.7z, cp.7z
Whats inside? Source and assets: thronebreaker, witcher 3 vanilla (appears to be E3 engine), witcher 3 next gen, cyberpunk2077
The passwords will be dropped on http://[redacted].onion/ or in case of outage in social media.

What do you need to do?
        1. Download
        2. Seed
        3. Donate to
                BTC: [redacted]
                ETH:
                DOGE
        4. Tell your friend

And to warm everyone up, the archives with SDK ps4 / ps5 / switch / xboxX have no password!

CDPR data, company reports, NDA, are shared with media, but they will not be public leaked!

This leak is in accordance with the buyer in exchange for a discount.

P.S.
Elon Musk, bro, pump bitcoin on 1st april please.

Wake up samurai, we have a city to burn!!! :D
```

Apparently, we now know that this (new) leak is in accordance with the buyer's terms from back in February in exchange for a discount on the overall buyout. This seems to be legit as reported by several people who have been able to download this torrent and get a look into the files even though they are password protected for full access. The latter is to be coming in the next few days at the time of recording this event.

The second release of contents being auctioned off to charity indicates some sort of ethics among some hackers about taking money for stolen property. However, this is still very serious as personal information is still at stake. As stated by this group, it will only be shared with the media but at this time it is unclear as to who, when, what or why.

The intellectual property of Cyberpunk 2077 being ousted is absolutely huge as CDPR is already struggling to bring the fixes to the game and this could see frustrated gamers rely on game modders who bring their own iteration of the game to life. This creates an additional mammoth of a task to CDPR, who will have to figure out how to track and shut down the modding community.

We know that large open-world A+++ games have a long-run rate and are designed as such to keep the gaming community invested in a franchise ecosystem. The source codes going public will reveal roadmaps, expansions and future plans.

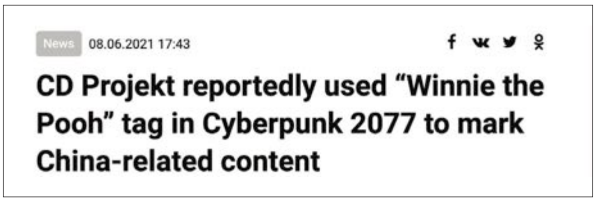
As this story develops, the takeaway is that it is simply not easy to recover from a breach. From reputation, customer base, employee retention to operational efficiency, output, profits and everything in between getting affected. And as evident from this story, a breach can come back to haunt you.

The irony to the hack is that Cyberpunk 2077 is a game that features 'hacking' as a class of character build whereby you can genetically upgrade your peripherals to hack into objects, electronics, and building controls for humans!

But wait.. More to this:

Edit: At the time of writing this I asked the editor if I could squeeze the latest news that was unfolding. We can now confirm that public downloads have indeed full access to the source materials. Apart from being able to dig into the original development roadmap of the game, certain details such as the headline below have already created a controversy.

Now China has very strict rules when it comes to game publishing and has banned companies for much less. This is an interesting development to see if CDPR's presence in China will be affected by this. We can now add 'political' ramifications to data breaches.



08.06.2021 17:43

CD Projekt reportedly used "Winnie the Pooh" tag in Cyberpunk 2077 to mark China-related content

Who would have thought so?

What should have been a redemption story for this game studio has been hampered by one data breach fuelling disruption and they are being continually dragged into the rabbit hole as this spin's out of control and goes public. ■

BLOCKAPT™

We are a finalist for **The UK's Most Innovative Cyber SME 2021** competition held by DCMS & the TechUK.

Attend our virtual session at InfoSecurity Europe:

'Complexity is the enemy of security'

Speaker:
Marco Essomba
Founder & CTO - BlockAPT

E-visit us at Infosecurity Europe event 2021
July 13-15, Virtual, London
Zone: Cyber Innovation Showcase

infosecurity®
EUROPE

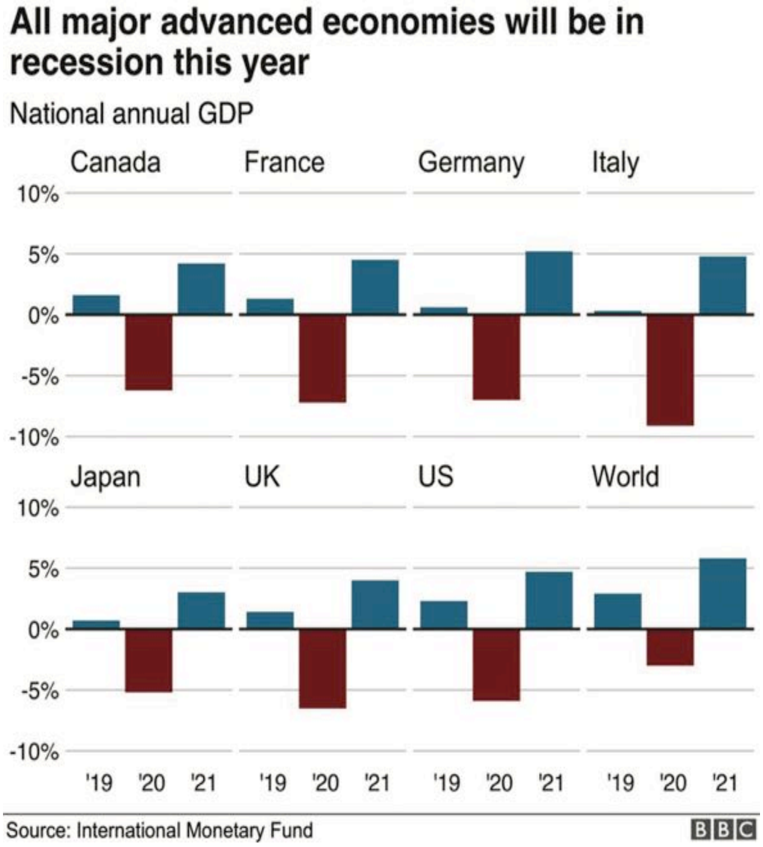
The fight against fraud –

How consumers and businesses will be impacted by the virus crisis.

Author: Simon Foster

These are uncertain times for both consumers and businesses. What is clear is that the UK economy has taken a hit, as has the global economy as a whole. How big a hit is dependent on various factors but the impact is greatly influenced by the current restrictions and peoples' inability to go about their normal working lives.

The International Monetary Fund has warned the virus could push the UK into its deepest slump for a century. In its report, the IMF said it expects the UK economy to shrink by 6.5% in 2020, while the global economy will contract by 3%.



All major advanced economies will be in recession this year

National annual GDP

Source: International Monetary Fund

BIO

Simon has over 25 years working in the IT/Telecom sectors and is Head of Partnerships at Jersey Telecom. His expertise lies in working on international and fraud protection, implementing industry-leading enterprise fraud prevention solutions and anti-money laundering strategies.

Simon matches rich data attributes from global mobile operators to specific fraud engine requests in his drive to protect customers with innovative technology solutions.

Impact on consumer spending and the impact on the retail market

Growth in household spending in 2021 is predicted to be at its slowest since 2011, as the effect of Coronavirus temporarily weakens consumer demand. European retailers are expected to lose over $4bn due to disruption caused by the health emergency, according to data gathered by LearnBonds. Statistics show Germany is forecast to suffer the most with over $913m lost in retail sales.

Through social distancing rules, consumers have been spending less as they are forced to stay at home. Many household incomes will be negatively affected and coupled with uncertainty about the future people will be more cautious about unnecessary spending. Non essential items such as clothing and footwear brands have suffered the most, but the UK food and grocery market is forecast to grow higher than previous forecasted annual spend.

As millions of Europeans remain to stay at home many of them have opted for online orders – sometimes for the first time. This has seen an increase in cashless payments and the opening of more digital accounts. An Ipsos survey reveals that more than 30% of Italian consumers increased how often they shopped online compared to the previous month. The UK came next with 18% followed closely by France, and Germany.

With the virus encouraging consumers to remain at home, sales of quality food purchases as well as health and luxury items are rising while the leisure and tourism industry is still uncertain, hotel, holiday and travel bookings are starting to recover.

- Sports equipment – 28% decrease
- Travel sites – 20% increase (double bookings home and abroad)
- Hotel bookings – 8% increase (double bookings home and abroad)
- Healthcare items – 27% increase
- Online grocery shopping – 20% increase
- Adult (luxury) items – 35% increase

As consumers look for ways to amuse themselves indoors, the large subscription giants such as Netflix are bound to be the winners in this crisis – 16 million new sign ups reported recently thanks to lock down. As traditional grocers come under pressure to fulfil online orders, traditional wholesale businesses and smaller, niche companies will be able to fill the gap by being more flexible and providing choice to the market.

Reports are showing an increase of online transactions, in card not present activity due to flurry of financial activity — selling stocks, sending money to relatives, buying items they'd never considered before and accessing sites they have not tried before.

Impact on fraud

The increase in card not present activity and the spike of transaction volumes has resulted in a surge of fraud cases. New accounts are being opened at greater levels as millions of people are signing up for food delivery and other services, or recurring subscriptions, or using online services for the first time. As such it is just as important as ever that companies carry out identity verification checks.

Criminals are using the coronavirus outbreak as an opportunity to try to steal money. Google has revealed that its servers are currently blocking around 18 million scam emails per day and one fifth of those relate to COVID-19. Fraudsters are posing as organisations such as banks and pretending to provide financial advice to people who are genuinely fearful about the months ahead. They'll then try to trick consumers into giving personal or financial information. As a result, these stolen credentials are used to take over customer accounts.

With households effectively on lockdown across the world, some banks said customers had already been caught out by fraudsters posing as banks, government and even health service providers to persuade victims to hand over passwords or other sensitive data. Online merchants also need to err

on the side of caution with every new customer registering or existing customers showing a dramatic change in shopping habits.

Requirement for strong customer authentication checks

As more people are staying at home, spending and financial activity is changing. More people are accessing online services and opening up new accounts to access new services. Due to this and the continued rise of fraudsters taking advantage of the situation, the banks and online merchants need to employ strong customer authentication checks to ensure that unusual spending activity is in fact down to the change in consumer buying activity and not the result of fraudsters taking over peoples' accounts. In addition, the regulations enforced by the European Banking Authority are starting to come into effect making it obligatory for banks and merchants to implement SCA with certain purchases. Card issuers will also have to employ step up verification checks if they see unusual behaviour associated with the new minimum spend levels for contactless payments.

The FCA is indicating that for banks and other UK Payment Service Providers (PSPs), the deadlines that have been set for implementing 'Strong Customer Authentication' (SCA) standards for e-commerce could be pushed back in light of the coronavirus crisis. The FCA is supportive of contactless payments and welcomes the industry's initiative to increase the contactless limit but is recommending fraud monitoring tools and systems are in place.

At this time when retail businesses are under more pressure than ever before, the focus has to be on providing a satisfactory service and retaining loyal customers. The key concerns are fraud; friction and false declines.

Nielson sets the cost of card fraud at $28B and the revenue lost to false declines could be worth 10 times that amount. Without robust customer authentication checks, retailers could see customer churn unless the fraud; friction and false decline concerns are dealt with. Only those organisations who are putting the customer first and ensuring they are not compromised security wise in any way will come out of this with intact reputations and perhaps with a new group of satisfied customers that will reward with loyalty even when this virus shadow has lifted.

JT Fraud Protection Services

JT currently works with BlockAPT to provide powerful sources of data linking a consumer to their mobile device. Just simple background checks utilising Mobile Network Operator data can make the difference in determining whether a transaction can be approved with the utmost confidence. For instance, a live check to determine if a mobile account has been recently transferred to a new sim and when, can raise an alarm that a device may have been compromised in some way. This is a vital check to carry out before sending an SMS OTP and doesn't interrupt the consumer experience or increase latency.

As a mobile network operator, JT is able to aggregate cross operator data services and provide real time network checks that proves to be effective in the fight against fraud. ■

Current Cyber Insurance and Ransomware Challenges.

Author: Sarb Sembhi

Ahead of some Insurers, has Elon Musk single-handedly become the cause of fast rising demands made by ransomware?

Ransomware gangs are not only charging more each time than they did a few years ago, they are also growing more aggressive in their approach to ensure that they get paid. What has led to these increases and aggressive nature and what will businesses have to do to protect their livelihoods? Some may argue that cyber insurers have contributed to the growth of this criminal sector by offering policy cover which pay out ransomware demands.

Others may argue that the existence, use and nature of crypto payments have facilitated the monetisation aspects of ransomware. However, whatever factors any wants to attribute as the single cause of the current situation, the fact is that there have been several factors contributing to where we are today and the challenges the cybersecurity industry will face in its future responses to ransomware.

Let's take a look at cyber insurance, ransomware and how we got to the rise in digital extortion, starting with cyber insurance.

BIO

Sarb speaks, writes and contributes to global security events and publications. He was the Workstream Lead for Thought Leadership of the UK Cyber Security Council Formation Project and is the Co-Vice Chair of the Smart Buildings Working Group of the IoT Security Foundation. He advises and sits on several start-up boards and is a Mentor on the Cylon accelerator programme. Sarb was shortlisted 5th in the IFSEC Global 2020 "20 Most Influential People in Cyber Security" and included in "2018 Tyto Tech 500 Power List" of influencers in the UK's technology sector.

Cyber Insurance meeting growing needs:

I first came across Cyber Insurance way back in 2012 and later worked on establishing the early stages of a consulting service to insurers, brokers and customers, during that that time so much has changed. For the purposes of this discussion, some of the changes include:

- There's more data available for underwriting – unlike other areas of insurance like death, health, shipping, business, fire, homes, etc. cyber is relatively new, with more data available each year, there is a better understanding for underwriting purposes – to some extent, see below for limitation.
- Cyber Insurance is not only in its infancy as a product, for many insurers it is still one of their biggest potential growth areas for the future. This means that there is and will continue to be experiments or tweaks made to cover, types of cover, exclusions, etc. for many years to come before insurers accept that the market share they have, is what they are happy with.
- Cyber-crime like cybersecurity is fast changing – as more traditional crime has been taking advantage of the internet, connected devices, etc. they have all had an impact on every aspect of cybersecurity responses and consequently cyber insurance.
- The basics of insurance remain the same – the overall number or value of claims that may need to be paid out versus the revenue from premium cover remains relatively as straight forward as it's always been. How is this a change,

when it's still the same? Essentially, there are several layers of underwriting insurance that have developed over centuries. Although this statement is true at the lowest level and ensures that the insurance industry doesn't take a complete nosedive resulting from any single event, at the higher customer facing product and premium levels of underwriting things have changed. The changes have been around responding to what customers want and are willing to pay for, especially when there is scepticism around insurers paying out. There are cases of insurers paying out in situations that they wouldn't normally pay out due to having had no other claims, and that they want to demonstrate that they are paying out on claims.

- In the early days of cyber insurance where the policies wouldn't pay out if a director or employee was responsible or cause of damage or an incident (where insurers just didn't get the idea of the insider threat) or where (when I asked one insurer) "is there anything that anyone purchasing cover can do to reduce the premium they have to pay" and the answer was a very definite "No!" Although this was only eight or nine years ago, in cyber terms it was a very long time ago and can and cannot be covered and how customers can reduce premiums has changed a lot.
- The provision of cover for ransomware payments is one such change – although not every insurer offers this cover, it does exist, and many customers around the world have already benefited from this it.
- Better data for cheaper more scientifically produced cyber insurance cover may still not exit – although there is a growing volume of data every year. The interplay of the changing impacts of cyber-crime, the growing volume of breaches, the proliferation of adopting vulnerable apps and new devices and technologies creating ever greater opportunities for cyber crime doesn't make for consistent data from one year to the next.
- In terms of pay-out by an insurer, it may only happen when the cost of the pay-out is likely to be cheaper than any other option to get the organisation up and running again. Also, although insurers have begun to request additional assurances for ransomware cover, the assurances requested may not actually be the controls that are circumvented which leads to the installation of the ransomware.
- But we must not forget that the percentage of business which hold cyber insurance compared to the percentage that do is very big, and even then, the percentage those with cyber insurance having ransomware cover is even smaller.

Many other changes have taken place in cyber insurance but are too numerous and not directly related to this discussion on ransomware.

Ransomware grows up:

Before looking at the effects of cyber insurance on ransomware, let's just take a quick look at some of the changes ransomware itself has undergone since the early days:

- Although the first public example of ransomware was back in 1989, and there have been regular advances by cyber criminals using it, it has not been a growing type of malware until more recently.
- Several factors have contributed to its growth, including its evolution in improved encryption, cyber-criminals creating easier monetisation with "ransomware-as-a-service", and the opportunity to revenue-share by any non-technical criminal in criminal marketplaces.
- The facilitation of payment services and customer service by the criminal groups – a few years ago along with a message to pay a ransom, messages began to appear on how to pay and even who to call to ensure that you get your data back. This was all to evidence signs of goodwill that if you pay, you get your data back.
- In the past, malware relied on data sharing on portable media, the reduced need for portable media has meant an increased reliance on email and browsers to infect users. Further, malware relied on vulnerabilities in applications and operating systems not being patched to be successful. This can be exampled by hospitals and other public sector organisations being the target of some ransomware campaigns, armed with the knowledge that systems in certain sectors are unlikely to be on the latest versions of software.

Again, I've painted a simplistic picture of the changes, but it's good enough to provide a basic appreciation to move the discussion on.

The simmering events leading to the boiling-point:

The third critical factor in the rising demands made by ransomware today apart from cyber insurance and Elon Musk, is the rise in data protection regimes around the world. So, let's get back to cyber insurance and Elon Musk's role by looking at recent events to question the future challenges.

- The provision of ransomware cover by some insurers has led some cyber-criminals to assume that since victims will recover any pay out demands from insurers, they are more willing and likely to pay quickly.
- The EU's General Data Protection Regulation set a minimum standard and minimum fine structure to be copied by others around the world.

▸ Ransomware developers have adapted from just encrypting data, (whereby if there was a backup, the victim may decide not to pay up), to where exfiltrating the data first, explore it and then determining what price the victim should have to pay based on the GDPR fine the victim would have to pay. So that even if the victim has a backup, they cannot choose not to pay, because if they do so, the exfiltrated data is then released to the public and the victim will be subjected to a fine larger than the ransom demand.

▸ The use of crypto currencies as the only form of acceptable payment has been a recent development in preference to card payments which were more easily traceable, and those services could be more easily withdrawn by the payment industry.

▸ While the trend of crypto currencies has been slightly volatile, the trend seemed to be an upward one, which meant that the criminals were getting paid in assets that could be worth more in a few weeks, months or years' time compared to being paid in cash.

These are probably just a set of knock-on effects of different events on each other which have contributed to where we are today.

The unfolding of boiling-point events:

Our story doesn't finish there due to the events over the last few months.

▸ The ransomware attacks to a vital oil pipeline and a meat processing plant are examples of the above summary in action.

▸ One insurer (Axa) which has provided cover for ransomware demands, reduced the cover for future policies in response to charges that it is contributing to an increase in ransomware demands. Very soon afterwards this insurer reported it had suffered a ransomware attack.

▸ Several countries have started to indicate a clamping down of crypto currencies or that they won't be accepting them; thus, impacting the value of currency.

▸ Over the first six months of 2021, Elon Musk's tweets not only raised the value of crypto currencies, but also later reduced their value considerably. One crypto currency billionaire donated $1.4B, but his actual donation was left being valued at $900M.

▸ Some of the breakaway ransomware gangs have recently been more aggressive in making demands as reported in the press in June 2021.

▸ Crypto currency is volatile! This means that a demand for $1M, could end up being valued at anything from $0.5-2M. How can any self-respecting business criminal accept such uncertainty? Therefore, they have to demand more to ensure that the worst-case minimum scenario is still acceptable, and anything above that is a bonus.

▸ A report from anti-malware vendor Trend Micro in mid-June 2021 suggesting that to maximise their earnings, ransomware groups are starting to focus their attention on businesses that have over $1milliion in revenue. However, since the total percentage of such business is less than just a few percent, those criminals not part of ransomware gangs will still continue to target the low-hanging targets, which are small businesses – because they are unlikely to just drop their source of revenue in favour of bigger gangs.

So, there we have it, cyber insurance cover for ransomware may or may not have contributed to the rise in ransomware, but once identified by criminals, the unintended consequences of both data protection laws and Elon Musk's tweets have increased the price being demanded from victims.

Challenges ahead:

The challenges for governments and the cybersecurity and insurance industries include:

▸ The data protection regulators need to look at the impact of what has happened in consider how they should treat blackmail attacks to extort money from businesses which have been targeted specifically for extortion; regardless of whether it is ransomware or any other type of criminal activity.

▸ How can the different types of cyber insurance cover be provided so that it does not end up being abused to become a source of income by criminals?

▸ Exploring alternatives to current data access models and practices, where access is all or nothing; so that even if an organisation has unsupported or vulnerable systems, the ability to bounce from it to access immediate, recent, past and archive data is not possible.

▸ How can smaller organisations be protected better? Although awareness may be growing, it is nowhere near the levels it needs to be to safeguard peoples' livelihoods. ■

Success driven Digital Transformation strategy.

Author: Kaustubh Mehdi

For some organisations, the digital journey is about exploring newer avenues of growth or optimising costs, while for some others, it is about keeping their heads above water in the face of an onslaught from the competition. Regardless of the drivers, leaders often highlight "risk taking strategy" as a key tenet for a successful transformation. Risk taking involves backing initiatives that encourage experimentation with new business models or collaboration with new partners without the fear of failure or admonishment. This approach is supplemented with flexibility and freedom to innovate without the burden of bureaucratic organisational processes or legacy technology.

BIO

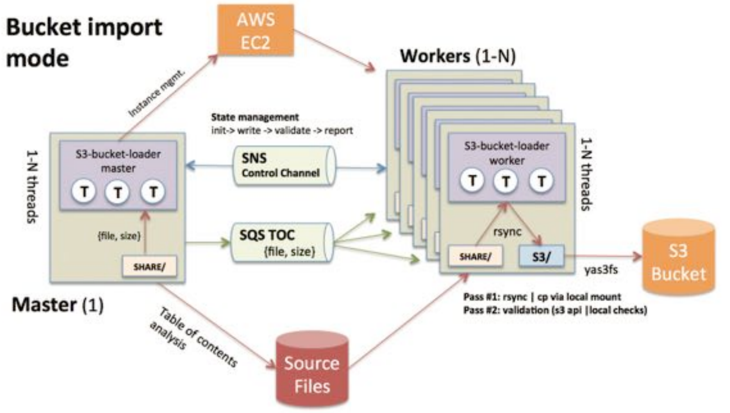
Kaustubh is an accomplished risk management professional with nearly two decades of experience in information security consulting, audit and operations. Kaustubh currently leads the Cyber Defence Center Operations at Reliance Industries where he focusses on Threat Intelligence, Security Analytics and automation. In his previous avatar, he has successfully led the cyber security practice at global managed security service providers such as Happiest Minds and Paladion. Kaustubh has authored several articles on security and risk management and has featured as a speaker at the RSA Security Conference and the Gartner Security and Risk Management summit. He actively shares his views and ideas on LinkedIn and can be reached at kaustubh.medhe@gmail.com.

Keeping with the spirit of this philosophy, business leaders unleash several programs that comprise of adoption of open source/ greenfield technologies for building custom applications or co-creation of solutions with relatively new/ niche technology vendors. Almost invariably, these pilot programs are bolstered with unbridled approval for the use of third- party cloud service providers, integration of on-premise databases or migration of customer/ business process data to cloud-based analytics platforms, third-party API integration for data exchange and the freedom to test and use custom/ open source hardware and software within the corporate network, as long as the "work gets done".

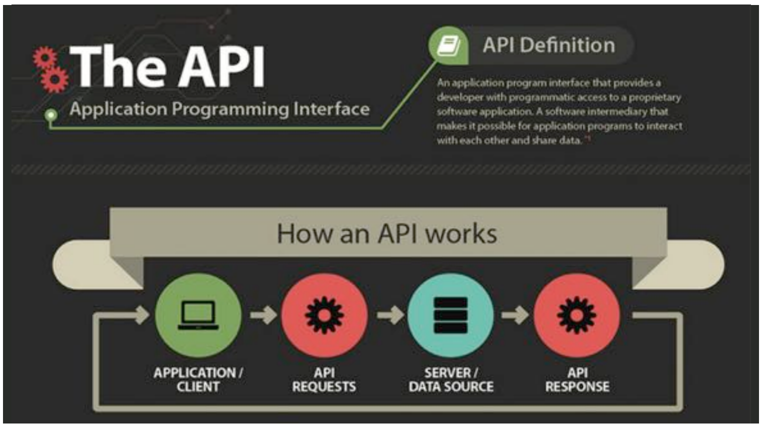
This agile and "learn as you go" approach has significant upside, allowing the IT organisation to quickly ship a MVP (minimum viable product), while leaving the door open for a course correction if the initiative doesn't yield promising results. However, unbeknownst to the management, every digital initiative (big or small) expands the threat surface for the organisation, introduces vulnerabilities and leads to the accumulation of a digital risk portfolio, which if not managed properly, can unravel all the gains.

For a few unlucky companies, some of these digital risk scenarios manifest in the following situations:

1. A misconfigured S3 bucket in the cloud exposes database credentials, application passwords, API access tokens or encryption keys for accessing the organisation's critical internet-based applications that are later used to carry out a hacking attack on the organisation.



2. An insecure API allows unauthenticated rogue endpoints to download excessive or personal sensitive financial or health related data of customers causing a huge media uproar and a regulatory enquiry for the data privacy violation.



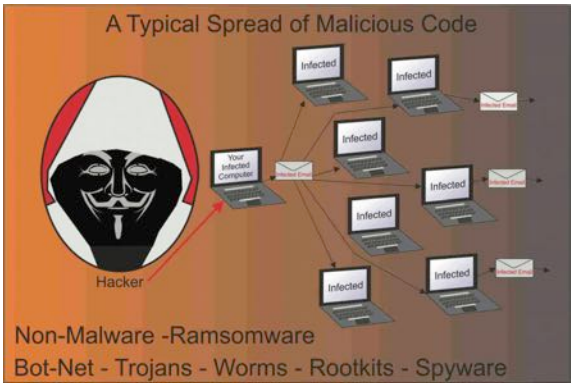
An application program interface that provides a developer with programmatic access to a proprietary software application. A software intermediary that makes it possible for application programs to interact with each other and share data.[1]

3. A third-party developer uploads the entire source code of the company's much anticipated mobile app to a public code repository.

4. An attacker targets an unpatched vulnerability in an obscure open source component used in the newly launched internet portal to download and execute crypto mining software.

5. A third-party SaaS vendor's multi-tenant platform hosting the organisation's e-commerce applications comes under a DDoS attack taking it offline and resulting in revenue loss.

6. To save time and meet a sprint deadline, a software developer intern downloads and installs a nifty software utility on the test server from a public code repository that contains malicious code. The mal code is designed to silently monitor keystrokes and exfiltrate sensitive data from the victim machine to an attacker-controlled server and maintain persistence on the victim machine that is later used to carry out a ransomware attack on the organisation.



7. An operational technology team opens multiple ports on the internet firewall to test an IoT enabled cloud-based real time process monitoring software for their chemical plant and then forgets to shut them, after the proof of concept is over. Advanced attackers discover and abuse the weak network security settings to implant ransomware on the OT systems and force the company to halt production.

8. A bank is penalised for bias when a regulatory audit reveals that their newly launched machine learning and AI enabled credit appraisal system rejects customer applications from a particular locality and community.

In most digital transformation programs, agility, performance and user experience always trump security and compliance. The typical mindset is "Security is very important…as long as it doesn't get in the way". Only when things go wrong, the security and risk teams are abruptly scrambled to launch a response and salvage the situation.

With so many new, un-proven and dynamic technology components being deployed as part of a digital transformation initiative, security teams routinely grapple with a lack of requisite technical skills to properly assess the risk and impact of the change. This problem gets compounded further, when they get engaged (or are deliberately involved) only towards the end of the project. In many of these cases, it may be too costly or too late in the project life cycle to first understand and then incorporate some of the essential security controls for risk mitigation.

There are a few things that organisations can do to reduce the likelihood of such disasters and secure their digital transformation journey.

Cybersecurity and Risk Oversight by the Board:

The Board can play a pivotal role in setting the right tone by requiring that security and privacy imperatives be baked into the digital transformation blueprint. This will automatically lead to involving security and risk teams early in the inception and design stages of the program. Secondly, the Board should call for and then sanction necessary budgetary provisions for security and privacy controls as part of the overall investment budget. Additionally, they should seek periodic risk assurance from the CISO or the CRO on the transformation initiative so that any critical concerns can be surfaced and addressed at an early stage.

Reforming the Cybersecurity, Privacy and Risk Management Function:

While the Board can do its bit, the risk management leaders (CISO, CRO) must strive to acquire situational awareness by engaging closely with the business and IT stakeholders and anticipating the security needs of the transformation program. This will allow them to acquire, build, re-train and retain the right set of diverse skills and competencies to support the dynamic needs. They also shoulder the responsibility of ensuring that the security and risk management practice "reforms" as the business digitally "transforms".

They can achieve this by:

- Doing away with bureaucratic and time-consuming manual approval processes and archaic security testing and auditing methodologies that could hinder the progress of the project.
- Evolving "agile dev-sec-ops" practices by embedding automated security workflows in software development life cycle processes.
- Prioritising technologies that enable continuous vulnerability assessment, threat monitoring, incident response and remediation.

Implementing security by design and default and continuous close engagement and collaboration between IT, business and security stakeholders goes a long way in ensuring the success of a digital transformation program. ■

The Cloud –

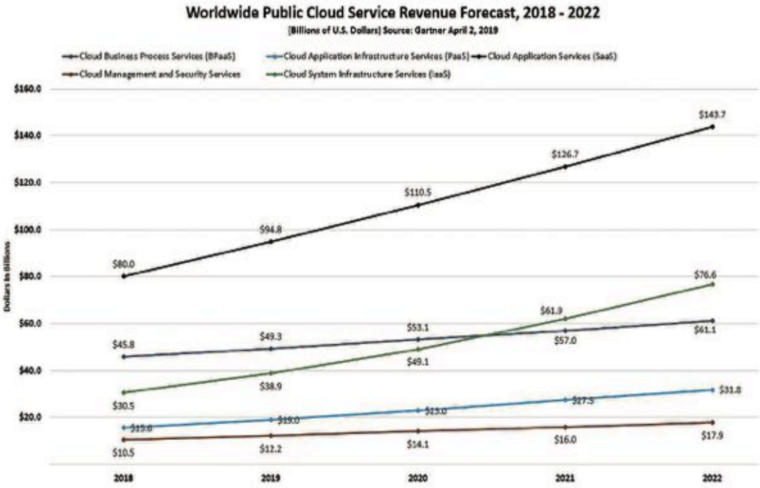
The power of technology. Now.

Author: Raj Meghani

The inception of the modern-day cloud was launched almost 2 decades ago.

2 years ago I spoke with someone and asked him what the top barriers to cloud adoption were. Security was the common denominator – data security and general security risks. At that time, Gartner was predicting that 50% of all global enterprises who were using the cloud would have an 'all-in-cloud' strategy by the end of 2021.

Fast forward to today. The COVID-19 pandemic with its remote workforce has meant businesses of all sizes have opened their eyes as to how a cloud infrastructure could offer them a scalable, flexible, cost-effective solution. By the end of 2021, Forbes predicts that 83% of a company's workload will be stored on the cloud (Public, Private & Hybrid). Gartner predicts revenue from the public cloud sector to jump by 21% from $175 billion in 2018 to $331 billion by 2022.



The numbers are staggering and the opportunities for providers such as Microsoft Azure, AWS and Google are on an upwards trend as cloud technology gets assimilated into business infrastructure and becomes their modus operandi.

So why are so many organisations still struggling to overcome some of the barriers? What are they and how can some of these myths be debunked?

1. I have already invested in my own data centres and my security is sufficient.

Whether your infrastructure is on premise or on the cloud or a mixture of the two, many organisations fail to detect and identify the source of the increasing number of cyberattacks. Having sufficient security controls is paramount to ensure scalability and business continuity.

Cloud service providers have invested billions in ensuring they have the right cybersecurity methodologies and tools to enhance security for their customers and continue to do so. Although, on premise applications may be secure, reliable and allow businesses to maintain a certain level of control, the sheer effort and cost of managing and maintaining hardware, software licenses, integration capabilities, incident response management not to mention keeping hold of skilled staff and training increases the organisation's risk exposure and could be a barrier itself on the scalability front.

2. Moving to the cloud will automatically save me money.

Not always the case. It's a fairly simple concept as you only pay for what you use on the cloud. No sunken costs on hardware or replenishment, power usage, space, etc.

For example, In the case of a server, once you've reached the storage space limit, you are faced with purchasing a new server to increase bandwidth. Businesses with a seasonal trend on customer flows with an on premise solution may not find it as cost-effective when traffic flows resume to normal levels and their server sits there with a high under utilisation rate.

According to IDC, the most prominent industries who will be spending the most on cloud computing this year are those which deal with the most data yield – i.e. retrieving vast amounts of sensitive information from several different locations are Manufacturing ($20 billion), Professional Services ($18 billion) and Banking ($16 billion).

But *caveat emptor* - the cloud offers a long list of services, tools and options all of which can escalate costs for a business quickly if it is unprepared on its requirements. Most of them offer tools to help manage billing and costs but the onus is on the organisation to get the cloud optimised to meet their specific requirements in the first place.

3. If it ain't broke, then don't fix it right?

Wrong - unless there are strict regulatory, legal constraints on managing data. On premise, tried and tested legacy systems, applications, hardware, etc are not as agile as a cloud solution. If your business is looking to grow, scale up then the need to ensure your IT infrastructure can scale too is key. Add to this attractive cost savings and increased security levels wrapped into the service and it's only a matter of time before a digital transformation starts to show results.

4. Having my data on premise is safer than having it on the cloud.

Hmm. With only 1 in 10 organisation's apparently being able to analyse over 75% of their security events both on premise and in the cloud, the concerns around cloud security, data loss and data privacy still remain a big challenge for businesses of all sizes.

SMEs are not just looking to survive in these challenging times but save as much money as possible without compromising the security of their customer data. Often lacking in the relevant security expertise and knowledge, 40% of them have found it more cost-effective to employ third-party cloud platforms than maintaining an in-house system.

Of all the cloud services, studies show that management tools and security services are expected to be the fastest-growing segments with a 28.4% improvement.

With the traditional on premise set up, the onus is on the business to mitigate against cyberthreats. Staying on top of patches, security certificates, etc can often be missed. Cloud providers with their deep pockets are seen to be on top of their game with security policies, compliance adherence, etc. In most cases, more so than what the traditional organisation has in place. Automation plays a key role here – intelligent collaboration and integration with change control processes across different devices, firewalls with robust threat intelligence, vulnerability management and incident response capability all boost the security ecosystem.

Interestingly, most public cloud breaches have been driven by an enterprise customer's insecure configurations. Gartner predicts that through 2025, 99% of cloud security failures will be the customer's fault NOT the security providers.

No business is guaranteed against cyberattacks – whether on cloud or on premise they are facing the same threats and risk exposure. The difference here is to do with responsibility and accountability.

5. Migrating to a cloud environment is going to be painful and disruptive.

Not always the case as it depends on the current state of a company's infrastructure. The business in the main has complete control over its software, policies and data. The flexibility to scale up or down on cloud usage is cost effective and provides economies of scale.

Treat the cloud migration as any other digital transformation project – with careful planning, a clear cloud strategy and implementation plan. Deployment compared to an on premise solution is often quicker and less disruptive to the business. The key is in the planning. Plan. Plan. And plan again.

So the benefits of cloud adoption are clear: According to IDG's report, 71% of companies look for speed improvements and 63% want greater flexibility. Other benefits include:

- Operational cost savings – no physical hardware investments, no trained staff to manage hardware, better space utilisation, pay per use, etc.
- Competitive strategic advantage – access to latest applications, innovation, analytics, etc to better manage your business and generate additional revenue.
- Security & Reliability – real time response to changes with controlled backup and restore.
- Speed – deploy your offering faster with fewer clicks.
- Ease of use – automation enables resources to effectively manage time consuming tasks.
- Collaboration – across geographies and teams in a secure way.
- Rapid deployment – minimal disruption to the business.

Cloud adoption is here to stay but it's the way in which we need to look at it that makes a difference.

Paul Maritz summarises this well – "Cloud is about how you do computing, not where you do computing". ■

Five most common mistakes to avoid when securing against cyber-attacks.

Author: Saurabh Gupta, President, HFS Research

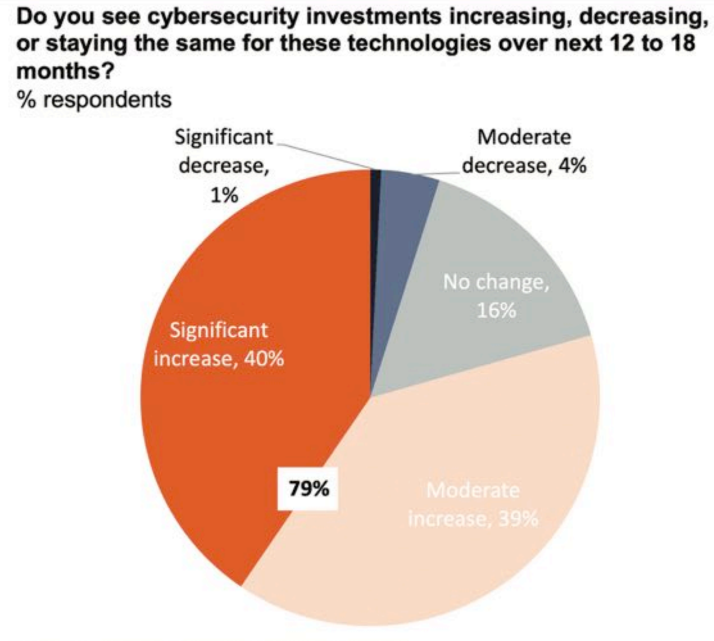
COVID-19 shone the spotlight on cybersecurity. Nearly 80% of Global 2000 executives expect increased investments in cybersecurity in the next 12-18 months (exhibit 1). According to Risk Based Security, the number of records compromised by cyber-attacks in 2020 exceeded 37 billion, a 141% increase compared to 2019.

BIO

Saurabh Gupta is President of Research and Business Operations at HFS. He oversees HFS' global research function managing the global team of analysts and operations across US, Europe, and Asia-Pac and is a recognised thought leader and passionate problem solver in the global services industry. With 15+ years of experience across client, provider, advisory, and analyst roles, he brings a uniquely realistic and wide-ranging perspective to industry's challenges and opportunities.

Saurabh has authored over 125 research reports, is a frequent speaker, and is regularly quoted in industry publications. He is well-known for spotting disruptive trends like As-a-Service, Cloud, Analytics, Robotics and predicting their implications for different stakeholders.

Ransomware attacks in 2020 nearly doubled. The explosion in the work-from-home and virtual workforce gave hackers more opportunity to inflict damage.



Sample: 800 executives across the global 2000 enterprises
Source: HFS OneOffice Pulse Study, H1 2021

Exhibit 1. Nearly 80% of Global 2000 executives expect increased investments in cybersecurity in the next 12-18 months

Despite the evident and stated importance of cybersecurity, only 40% of executives surveyed feel confident that their enterprises are adequately protected from cybersecurity threats. While organisations can never be 100% secure, HFS has distilled the five most common mistakes to avoid when securing your enterprise from cyber-attacks.

1. The security lip service. Limited support from C-level executives and the Board and lack of security, training and staffing budget are the biggest inhibitors to enterprise security readiness. Many CISOs are often subject matter experts who struggle to communicate the business value of security to the Board. On the “flip side”, the Board is not versed in cybersecurity. The result is a communication divide with the Board often unable to effectively assess the security team’s success in protecting the business. Lack of buy-in is the key behind surface-level cybersecurity initiatives. Cybersecurity is a C-level conversation.

2. Security as “Check in the box” exercise. Security policy development should not be a one-time check-the-box activity for compliance. Our data suggests that only 20% review their security policy every quarter. It is more important than ever to regularly review and update your security policy to consider the macro-economic environment, changing technologies, business practices, and the increasingly virtual world.

3. Paranoid about the new but protecting the old. Enterprises understand the risks with more recent technologies – such as the cloud – but show little appetite for tackling security gaps in areas of the business that are likely to be running on older technology. As a result of businesses’ desire for the new and exciting, they extend their budgets to accommodate security services and products, and the risks are better known. Also, the information in circulation about risks in newer technologies is more prevalent, while risks inherent in older technologies only come to light after a breach.

4. Security as an afterthought. Cybersecurity needs to be part of a larger value framework that includes both risk management and the development of digital trust. Enterprises should consider a shift in how cybersecurity funding is viewed, away from treating security costs as overhead. A holistic approach should be followed, including the cost of securing data and allowing it to be used—as part of overall business initiative financial requirements.

5. Security as a barrier to technology innovation. Enterprises are aggressively implementing new technologies and initiatives to survive and thrive in the post-pandemic virtual economy. Over 80% of executives across Global 2000 companies expect to increase investments in emerging technologies over the next 12-18 months. Companies need to realise the substantial risk of damage to their corporate brand should they experience a significant data breach or interruption in service delivery and build security as an integral part of the innovation process.

The Bottom Line. Cybersecurity is an integral part of the digital underbelly that every organisation requires to reach their transformation goals.

COVID-19 flipped the endemic, decades-old, corporate mindset of resisting change to one of demanding change overnight. Business resiliency became the lifeline in the quicksand of just focusing on cheaper/ faster efficiency. We are the dawn of the OneOffice organisation (exhibit 2) with the advent of connected, global talent and the infinite possibilities of intelligent, automated processes and data running in the cloud. Cybersecurity needs to be built into the digital infrastructure of the OneOffice organisation, not added-on! ■

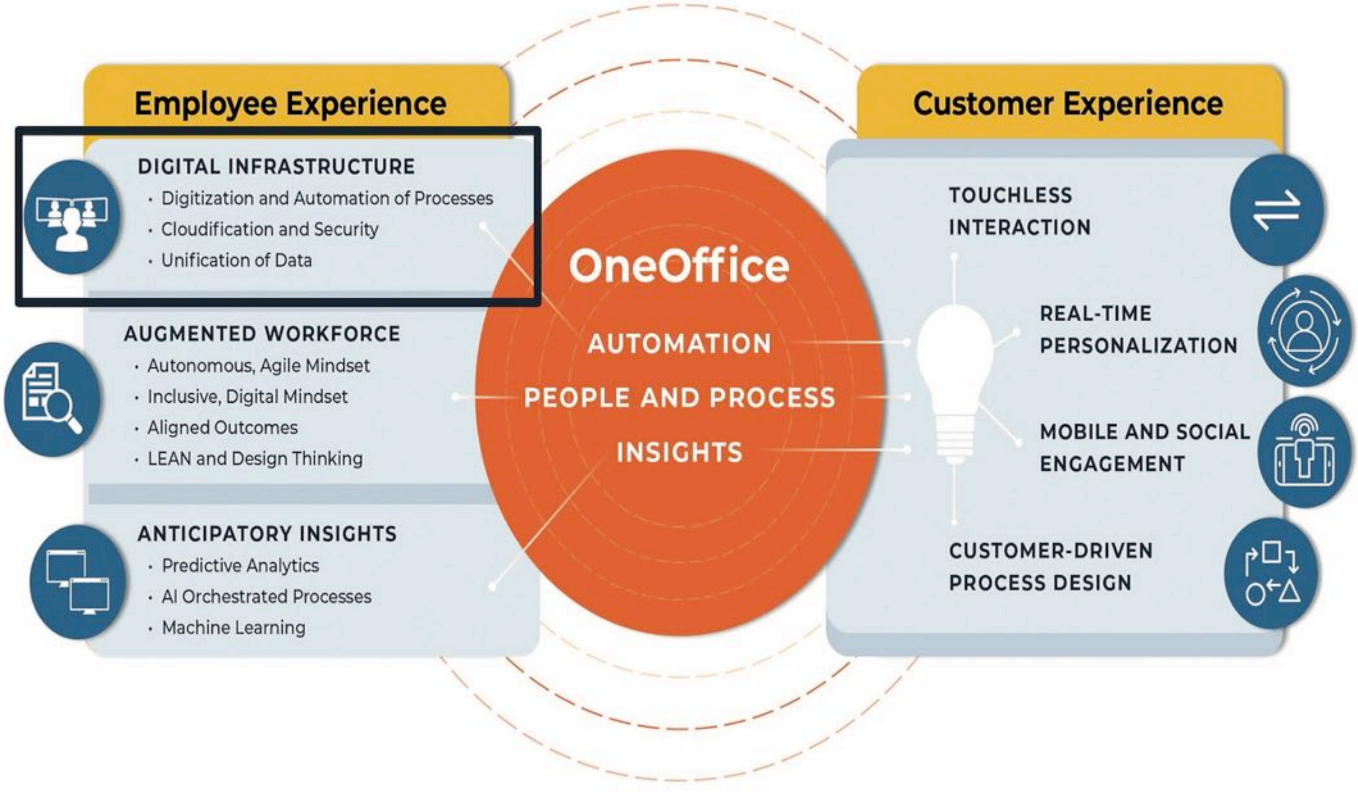

Employee Experience
DIGITAL INFRASTRUCTURE
· Digitization and Automation of Processes
· Cloudification and Security
· Unification of Data
AUGMENTED WORKFORCE
· Autonomous, Agile Mindset
· Inclusive, Digital Mindset
· Aligned Outcomes
· LEAN and Design Thinking
ANTICIPATORY INSIGHTS
· Predictive Analytics
· AI Orchestrated Processes
· Machine Learning
OneOffice
AUTOMATION
PEOPLE AND PROCESS
INSIGHTS
Customer Experience
TOUCHLESS INTERACTION
REAL-TIME PERSONALIZATION
MOBILE AND SOCIAL ENGAGEMENT
CUSTOMER-DRIVEN PROCESS DESIGN

Exhibit 2. Security is an integral part of the digital infrastructure for the HFS OneOffice organisation
Source: HFS Research, 2021

How to Ensure Diversity in Security Teams.

Author: Lisa Ventura

In many security organisations, conversations around the pressing issue of diversity in the industry are tending to be overlooked. Not only is the world of cybersecurity made up of a highly homogenous group of people at the top, the lack of diversity in the industry creates hurdles and makes the process of securing organisations much harder than it needs to be.

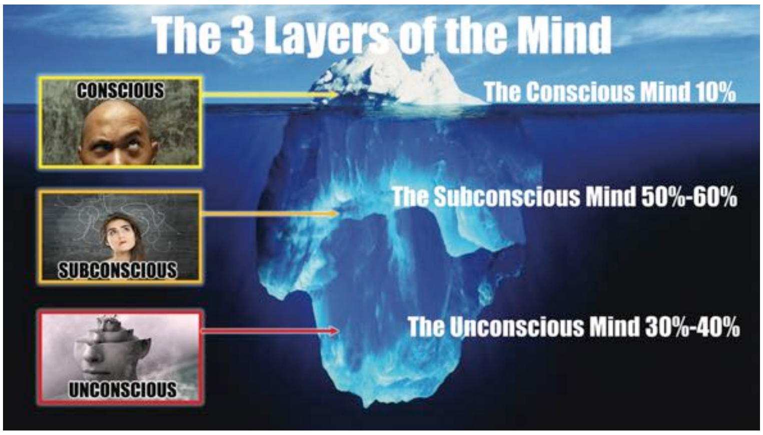
So, how do you increase diversity within your security team? Here are some tips:

1. The retention of diverse staff is as important as the recruitment of them:

Much of the conversation around diversity in cybersecurity often focuses on hiring staff, but if you want to create more diverse security teams, you need to also focus on retaining your diverse staff. While it is important to dramatically increase the number of non-binary, women and people of colour, it is just as important to improve your internal processes to help retain them.

Studies show that up to 52% of women leave security careers, as do those with non-traditional backgrounds, and this is nearly double the percentage of men who leave cybersecurity careers. Some say this is because women don't enjoy their careers in security, but 80%+ of women in the industry say that they love their work. This implies that many from diverse backgrounds leave the industry due to culture.

2. Don't let conscious or unconscious bias affect your picture of someone:



Too often, we have a mental picture of what a security person is supposed to look like which does not reflect reality. The famous picture of Einstein shows him with tongue out and his hair all over the place, and if you did not know that he was one of the greatest intellectual minds in the world, you might assume that he was not very bright based on how he looked. As this shows, appearances can be very deceptive.

We often do not realise that we have fallen victim to unconscious bias. Acknowledge that your biases may not be explicit or intentional and learn to recognise that they do exist. Listen to what people say, evaluate the work they produce and observe how they collaborate with others – these are all indicators of the value they bring to the organisation.

Also, keep in mind that those who have been conditioned to believe that security is not a valid career path for them, or those who are neurodiverse, may not exhibit a level of confidence with their work. It does not mean that they cannot do it, it just means they may need a little more encouragement in their working lives.

3. **Nurture those who think uniquely:**

Security organisations often think that they want people to shake things up by thinking uniquely, but in practice many are uncomfortable with being challenged and presented with new ways of doing things. When original thinkers do not feel as if they are valued, they are more likely to move elsewhere.

Building a culture of inclusion where everyone has a chance to share their ideas can help hugely when it comes to improving diversity within security organisations. Not every idea will be a great one, but all ideas and opinions should be shared and listened to.

4. **Instil a culture of remote and flexible working where possible:**

In March 2020, a mass move to get everyone working from home quickly was undertaken when the COVID-19 global pandemic hit. Due to this, many organisations realised that their employees could be just as productive working from home as they could be by working in an office. In addition, those who are neurodiverse often get stressed when a deadline is approaching and undertake their work as far as possible in advance, while others find that they need the adrenaline rush that comes when waiting until (almost) the last minute to deliver a project.

BIO

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

Supporting flexible working hours, a flexible working location, job sharing or three weeks on/one week off enables people to set their own hours and location where they feel at their most productive, while still delivering on deadlines and projects. Trust that people can be productive even if they don't work in the same way or at the same time as others.

Inclusion from a personal perspective:

The cybersecurity industry is very male dominated, but I didn't let that put me off when I transitioned into it from the entertainment industry in 2009. Luckily, I had the support of some amazing pioneers and leaders in the industry, but I saw quite early on how off putting cybersecurity could be as an industry to newcomers and to women who were looking to join it. I resolved to help and support as many women as I could to help

them make the transition and to put them in touch with relevant mentors.

Ironically, I have had nothing but support from men in the cybersecurity industry for what I do with the UK Cyber Security Association. They have all been helpful and some have bent over backwards to help me and introduce me to contacts who could help me take the UK Cyber Security Association forward. Chris Windley, my Head of Business Development has been particularly supportive of me and the work that I do.

I have experienced animosity and bullying from other women in the cybersecurity industry. One in particular approached me at Infosecurity in 2019 and said she had heard all about me and that the UK Cyber Security Association was a ridiculous idea that wouldn't amount to anything. She got quite close to me in a threatening way, and as it was someone who I looked up to and admired in the industry. The experience left me feeling very shaken indeed. Since that experience I felt that I had to work harder to prove myself in the industry and to establish myself as a credible thought leader.

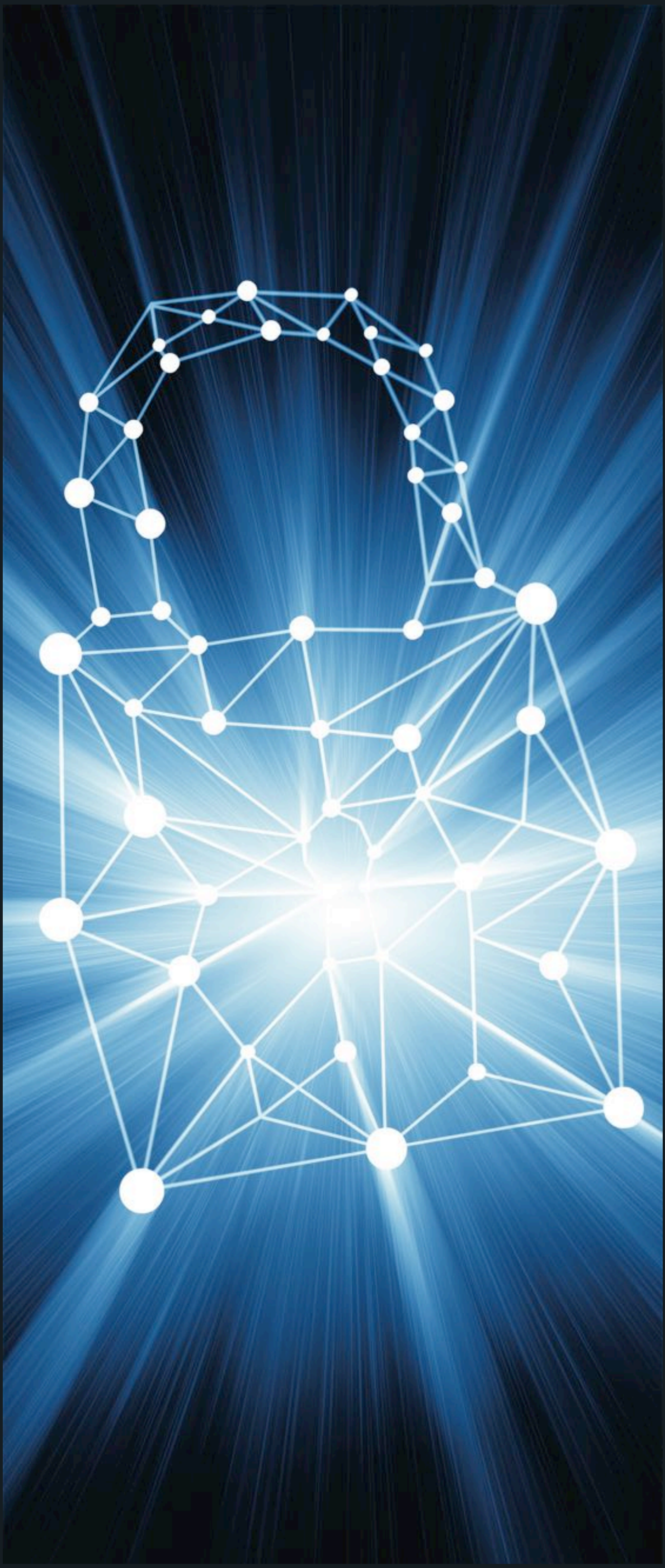
This is just my own experience, and one of the best pieces of advice that I give to others looking to enter the industry is to make sure that you have a tough skin and can deflect any bullying and abuse that is aimed at you. There are those in the industry that will do all they can to belittle you, but do NOT let them win. They should never win. You have much to give and contribute in cybersecurity, and the industry needs you.

Final thoughts:

To build a strong and diverse security team, you need to build an environment that supports and accepts differences of all kinds. Do not let unconscious bias about gender, the hours someone works, the location that someone works, or their appearance get in the way of nurturing all the great security talent available within organisations.

Organisations need to focus on creating cybersecurity teams that mirror the make-up of their wider workforce. Only then do they stand a chance of warding off the growing number of cyber threats. ■

Cybersecurity Trends



A publication

web for your business
swiss webacademy

edited by:

BLOCKAPT™

Copyright:
Copyright © 2021
Swiss WebAcademy and BlockAPT.
All rights reserved.

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

For the UK edition:
Raj Meghani

Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

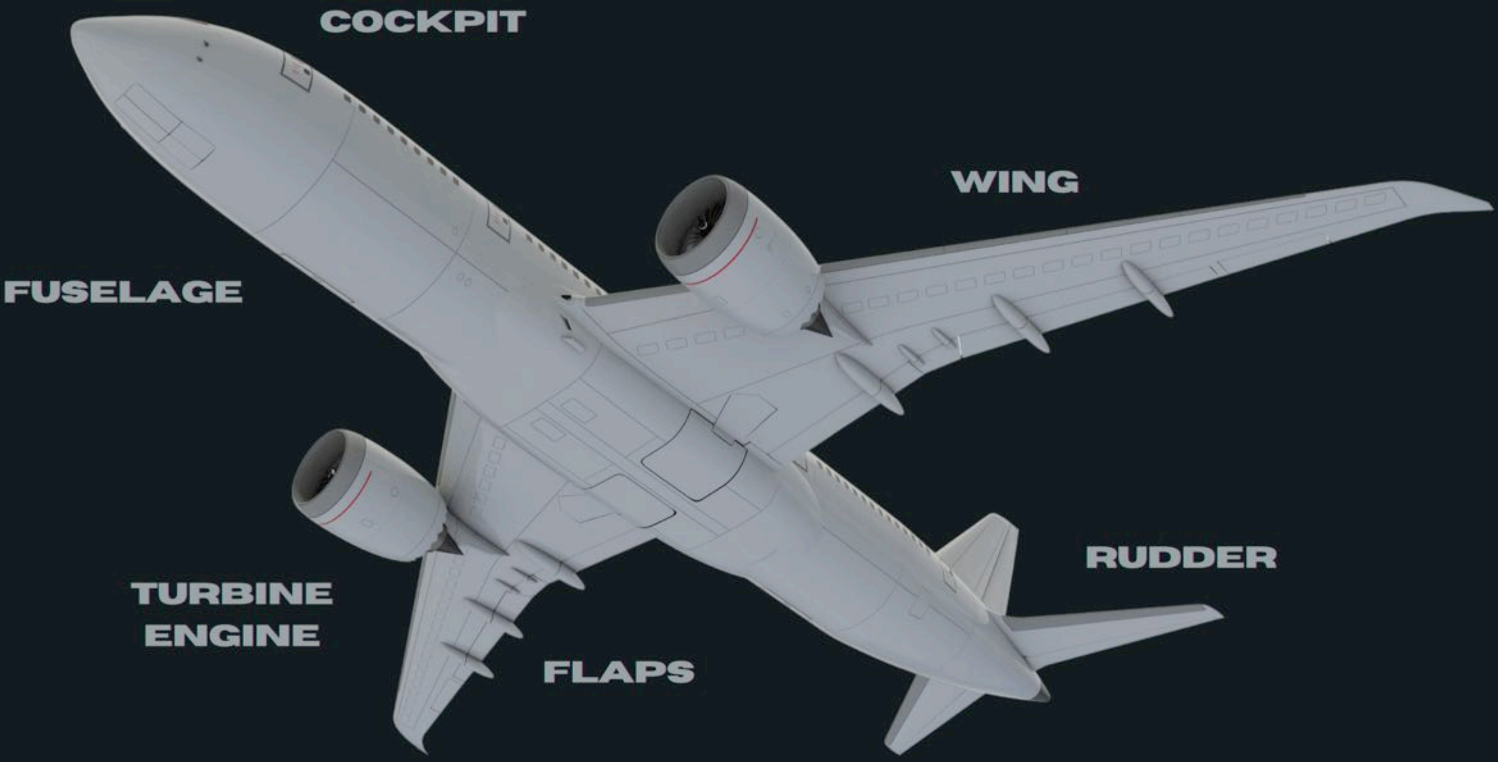
Addresses:
Swiss Webacademy - Str. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

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

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

BLOCKAPT™

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



We bring together essential engineering to make your security SOAR.

All controlled by our MMAR* technology.

Monitor - Manage - Automate - Respond*

blockapt.com

@blockapt