TOP CYBER NEWS MAGAZINE

DECEMBER 2022

Chris KUBECKA

CEO of HYPASEC
COO at LION195 AGAINST TRAFFICKING

GEOPOLITICAL CYBERSECURITY LANDSCAPE

HOW CHRIS KUBECKA, THE PEACE, INTEGRITY AND CYBERSECURITY ORACLE, THE WORLD'S LEADING CYBERSECURITY EXPERT, USING HER UNIQUE TECHNICAL AND PEOPLE SKILLS, KEEPS YOU SAFER IN TODAY'S UNPREDICTABLE DIGITAL REALM

Fore *Word*

The world is engulfed in geopolitical debates today. Geopolitical events are scary. Global geopolitical 'tornadoes' create catastrophic destruction and falsification of truth in the mainstream media discussions as well as online and offline forums. Geopolitics is dangerous. Geopolitics is for professionals. Would it be better if we avoided this topic? We cannot.

As the global geopolitical arena becomes increasingly turbulent, and cyber insecurity has become a wide-reaching escalating predicament; governments and businesses across the world ought to function in a greater degree of cybersecurity awareness. Chris Kubecka, the stalwart defender of safety in the digital world, the advocate for cyber diplomacy, the cybersecurity expert who lives geopolitics, shares her expertise and experience on a topic of Geopolitical Cybersecurity Landscape in December edition of Top Cyber News MAGAZINE.

Top Cyber News MAGAZINE Team

Organization Security Enablement

Editorial article by Brad Voris

If you don't take your own company's cyber security seriously, someone else will.

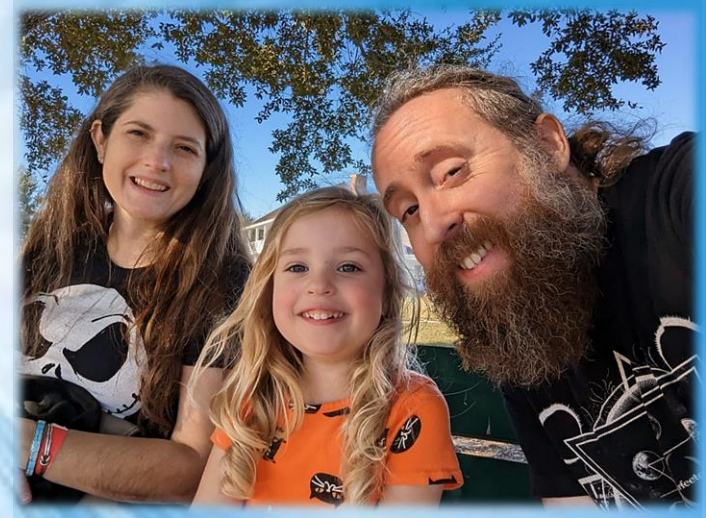
Generally business decisions about cyber security are the lowest on the list. The excuses are always the same: “the cost is too high”, “I have antivirus/firewall”, “we don’t have the in-house expertise”, and/or “we need more compute/storage/networking”…

There are “greater” business needs than cyber security… **That is until someone else takes the company’s cyber security needs more seriously.** A rival business wanting to cut the competition, a careless employee clicking on a link in an email, a disgruntled person with keys to the kingdom, a poorly deployed server with no patches or even that new project over the horizon that promises to simplify the business needs all pose a potential cyber security risk. A malicious person could exploit those risks causing loss. Those risks should be identified, classified and addressed per the business need.

Cyber security threats are everywhere and in everything we do. The potential itself is around every corner with every change to the business or its infrastructure or in a lack of change. **The truth is cyber security threats cost companies billions of dollars a year.** It is not always about the physical loss of equipment or service. Cyber security risks cost the company’s reputation, and its appeal to the general public or its investors. With that kind of damage there is no true way of determining what the potential loss would be. That cost should not come at the expense of the business or its employees. It should be mitigated with security management.

Cyber security management should be working hand in hand with information technology, auditing, marketing, human resources, and business decision makers to help determine best possible outcome for the future of business and its employees.

Cyber security isn’t just about firewalls and antivirus. It is also about people and data. The cost of cyber security is the cost of doing business the right way.



Brad Voris has been working in Information Technology and Cybersecurity for over 22 years. After passing the exam and officially entering the Security field, Brad continued his upward trend through the acquisition of an array of certifications: CISSP, CISM, CCSK, Network+, MCP, MTA, VCA-DCV, NSE1, NSE2, NSE3, ACE, 100W – OPSEC, Trustee, AZ900, and P.I. to name a few.

Continued knowledge and high-level performance has led him to work with a list of enterprise organizations including **United Airlines, Texas Children’s Hospital, and Walmart. Currently he is an Information Security Architect at Walmart.**

Chris Kubecka, Netherlands

Using her unique technical skills, honed starting age six programming and busted hacking into the DOJ at age 10, **Chris Kubecka** is one of the world's most renown cybersecurity experts.

CEO and Founder of HypaSec NL, COO for LION195 Against Traffickin, former Distinguished Chair for the Middle East Institute's Cyber Program, Chris advises the United Nations, multiple governments, militaries, television and documentary technical advisor as a subject matter expert on cyber warfare national defense.

Author of Hack The World With OSINT Open Source Intelligence Gathering; USAF military combat veteran; former military aircrew, and USAF Space Command, Chris Kubecka defends critical infrastructure and handles country level cyber incidents, cyberwarfare, and cyber espionage. Previous to HypaSec, she reconnected Saudi Aramco international business operations & established digital security after the world's most devastating cyberwarfare attack. Chris lives and breathes IT/IOT/ICS SCADA control systems security.

TECH FOR GOOD

by Chris Kubecka

We are surrounded by billions of Internet connected tech. The digital world has permeated our homes, workplaces, public spaces. Winning hearts and minds, forcing change good or bad in our society. We might not be cyborgs, yet. But we depend on bits and bytes for our global economy and survival. Clean water, manufacturing, electricity, railway systems, maritime, aviation and space are almost all digital and much of connected to the internet.

With the embrace of this digital world, there has understandably been a darker side. Crime syndicates have turned various internet frauds and internet of things malicious bots into billions in illicit gains. In 2021, digital theft is now more common than physical theft. The growth of IOT has outstripped the supply of existing cybersecurity professionals. There are little to no regulations on the safety and security of IOT devices, allowing our own technology to be used against us in various cyber grift.

What can be done to turn the tide? Many of the various cybercrimes we don't hear about occur on a smaller scale and not considered newsworthy. Small businesses and NGO's who cannot afford full time tech departments much less basic cyber security are at most risk. They are the backbone of most economies or form part of a social safety net for those in immediate need. Focusing on those easily targeted by both cyber professionals and those trying to gain real world experience in the field can benefit from helping, especially NGO's. The picture doesn't have to be bleak when we consider our digital future and the burden on uncontrolled risk. We as technologists can take a village perspective to provide assistance and give back to our own communities, making the stringer for everyone.

Understanding The Geopolitical Cybersecurity Landscape

by Chris Kubecka

Cybersecurity is a critical component of the geopolitical landscape. Geopolitical cybersecurity risks are those that are related to geopolitical events and tensions. It affects everything from international relations to national security and economic growth. As cyberattacks become more frequent and sophisticated, understanding the geopolitical cyber landscape becomes increasingly important for organizations to measure risk and minimize damage.

This section will explore three topics which are important to understanding the geopolitical cyber landscape:

1. What types of digital devices are at risk?
2. Real world examples of cyber spilling into the physical world?
3. Risks to your organization?

What types of digital devices are at risk?

The definition of a digital system has expanded dramatically in the last decade. Cybersecurity is the protection of information and data on a digital system or network from attack, damage, or unauthorized access.

A digital system can be anything that is connected to other digital systems or the internet. IT assets, IOT, smart devices, industrial digital control systems. I'm not sure who coined the phrase first, but it's become a sort of trademark for me:

The S in IOT stands for Security.

IOT and Industrial IOT (IIOT) devices can found in your home, office, nuclear power plants, aircraft, maritime shipping, and space.

Real world examples of cyber spilling into the physical world

Smartphones and geopolitics

Smartphones, our ultimate pocket sized IOT device. As one Bulgarian MEP said at the EU Commission

"Smartphones are our digital kingdom of connectivity, everyday life and secrets in our pocket."

Our pocket kingdoms are utilized extensively by nation-state level cyber operations, cyber terrorist groups, cyber criminals, hacktivists and patriotic hackers on a regular basis.

In the summer of 2021, I was contacted urgently by a former US Assistant Secretary of State regarding a brand-new US based non-profit. Within two hours of publishing the website Turkish Democracy Project. A distributed denial of service attack launched. The website was so new, google and other search engines hadn't even indexed the website to show in search engine results.

As the story unfolded, the picture was grim. Attempts to shutdown the website, death threats against the organization's board members, a slander campaign in Turkey, the arbitrary arrest of a US citizen who was part of a board member's family, another family member beaten police in Turkey outside their home. A merge of cyber and physical attacks with fears of deadly consequences. All based on a website, published in the United States, by US citizens.

When reviewing the web logs with the development and hosting team. Something stood out. User agent strings, an identifying marker used by devices to show web pages tailored to those devices. For example, a user agent string will say a device is using a certain browser and ask the website to display properly to that browser. Be it Chrome, Firefox on a mobile device. The user agent string can also identify the operating system used by the device.

Most of the user agent strings pointed to particular smartphones and smart appliances. The hosting provider questioned why there were so many old versions of Linux variants in the user agent strings. I knew why instantly, they were IOT smart devices and smartphones. All too frequently smart devices use older and known exploitable versions of Linux and older protocols such as Telnet left wide open for attackers.

This saves money on development, most are not security or privacy tested and there are no real regulations requiring testing. Unfortunately, most smart IOT vendors still struggle with basic concepts of secure=re software development lifecycle, i.e. how to patch things so they don't get PWND.

A picture began to emerge, a variant of the Mozi peer to peer botnet was used in the attack. I found several Turkish language social media posts, some tied to a notorious terrorist group called the Grey Wolves who have launched several high-level cyber-attacks.

There were Turkish language calls for action to attack, posted by individuals who associated with the Grey Wolves football team and likely members of the terrorist group.

The devices used by the Mozi botnet ranged from cheaper smartphones to high end smart fridges. All with the same weak security settings wide open for cyber attackers. The initial attack started in Turkey and spread using US devices against the US based organization. An additional external company was called in to investigate with me. based on one founder working for a short time at a US intelligence agency. They had no real-world experience in IOT botnets or the geopolitical issues in the Middle East. The external company fumbled, wrote a low-quality report causing confusion and wasted precious time during a life and death cyber crisis.

At the conclusion of the cyber and physical attacks. A letter was written for the Department of Justice to investigate, and several board members and employees resigned due to ongoing death threats against them and their family members. What happens in cyberspace can spill into the physical world. Turkish Democracy Project (TDP) calls on Justice Department and FBI to investigate cyber-attack and death threats.
https://www.viadiplomacy.gr/turkish-democracy-project-tdp-calls-on-justice-department-and-fbi-to-investigate-cyber-attack-and-death-threats/

- Does your organization remotely patch company smartphones?
- Can your company smartphone be wiped of sensitive data remotely?
- Can they remotely detect unusual activity from company smartphones which could indicate them being used in smartphone bot attacks?
- Have your organization's legal resources reviewed to liability issues if company smartphones are used in botnet attacks and cause damage?
- Does your organization have a real, experienced incident management team on retainer or in-house? Unfortunately, there is a lot of snake oil in the cybersecurity industry. Review proof not words.

Real Embassies, Terrorists, Drones and Weak Passwords. What happens when an embassy is hacked

In 2014 during my time with the Saudi Aramco family as the Head of Information Protection. I was having a rare lunch break, chowing down on some tasty salad. My team handled a great deal of cyber-attacks due to geopolitics and hacktivists involving Saudi and Saudi Aramco . When an imposing gentleman in a well-tailored suit summoned me from the break room. It usually never a good thing if you are summoned from the lunchroom at work.

The Kingdom of Saudi Arabia's embassy in The Hauge had been hacked. I was rushed to the Saudi Embassy with my Dutch top forensic person. Greeted by the embassy's IT person upon arrival. It was the IT person's first week on the job. The Ambassador was not pleased and angry with the new IT person. A common misunderstanding with management and executives is IT is the same as security. It's not whatsoever. IT connects, security protects.

There was a series of suspect emails sent from the Ambassador's secretary. A Saudi citizen had requested citizen services for a visa, unaware there was a recent change, and a 3rd party company was utilized for visas, not the embassy. After requesting visa services, the requestor received an email back the embassy could handle the request if $200 was sent over Money Gram in the name of the then current Saudi Ambassador to the United Kingdom. The requestor initially agreed to the fees and sent her passport and proof of payment via email. After finding the exchange suspect with no visa results, the requestor co reported her suspicions directly to the Ambassador. The Secretary insisted she never saw or sent the email in question.

One of the first steps in an incident is to contain and minimize further damage. Locking down accounts is one strategy if you don't need to surveil an attacker. I asked what the current password for the official Saudi embassy's email account was.

Answer: 123456. I thought the IT person was mistaken, an embassy couldn't possibly have such a weak password. Many of us have expectations that organizations and governments of a certain size and sophistication have stronger security than most of us do at home. This is an incorrect assumption. The password was 123456. According to Tom's Hardware, the worst passwords for 2022 includes 123456. (https://www.tomsguide.com/news/worst-passwords-2022). We can't keep attackers out if the basics aren't covered.

Incidents at an embassy are complicated. The ambassador is fully in charge, the property and information are sovereign territory. Many embassy employees have diplomatic immunity. As observed after the brutal Khashoggi murder in the Saudi embassy in Istanbul, embassy staff are untouchable. The Diplomatic Corp, which operate independently in most countries assist embassies with law enforcement, security, and diplomatic challenges in the host country. However, they typically do not operate without the approval of the ambassador.

My forensics person was able to perform image copies on the secretary's computer. The only internet connected computer on the embassy business network. In addition to a network tap on the business network. We had to tread carefully though. Many embassies have an intelligence collection apparatus. The Saudi embassy had a separate intelligence collection room with analysists on a secured but separate network. A commercial off the shelf malware was found, ISR Hackhound. The incident was looking like a man in the middle attack. However, due to bad relations at the time between Saudi Arabia and the Dutch government due to an extreme Dutch politician who is well-known critic of Islam. Saudi Arabia had recently cancelled all Dutch contracts in the country, costing the economy an estimated 3 billion in contracts. My Dutch forensics person was asked to leave and not to return. I don't hold Dutch citizenship and continued with the investigation.

There were multiple issues with cybersecurity at the embassy. Firstly, there was no basic cybersecurity. They used no certified anti-virus, no patching system, no awareness training, no network monitoring, nothing except a weak password to protect their sensitive business communications. How can an incident be thoroughly investigated without information and digital logs? The systems were locked down as best I could with the Ambassador's approval. Lists of recommendations, purchase of technical equipment, security software etc. Given to the ambassador in executive speak so he could through understand the situation. The ambassador and I thought all the bases were covered and the incident was closed.

Two weeks later the same imposing man summoned me again from the lunchroom. Rushed to the Embassy, there was a graver situation. The attacker using the official business email of the Saudi embassy has sent an extortion letter to all GCC and the Turkish embassy.

Send $25K to save many lives, signed ISIS. In 2014 The United Nations Commission on Human Rights had stated that IS/ISIS/ISIL "seeks to subjugate civilians under its control and dominate every aspect of their lives through terror, indoctrination, and the provision of services to those who obey".

(https://web.archive.org/web/20150204115327/http://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/HRC_CRP_ISIS_14Nov2014.pdf)

ISIS was a well know, brutal terrorist group spreading terror, kidnappings, slavery, beheadings, chemical weapons, suicide bombers, car bombs, selling sanctioned oil to buy weapons and commit more terror. The world is still reeling from ISIS and associated terror groups. The Ambassador was quite concerned. Saudi had also suffered active terrorist attacks by ISIS and the Grand Mufti of Saudi Arabia had condemned the group a few weeks before. The embassies that received the extortion emails were shaken. A top priority was to collect evidence, which is a challenge with embassies. Two embassies gave copies of the original emails so I could review background information called email headers

While knee deep in the investigation phase. The Diplomatic Corp for whatever reason had not contacted the Saudi Ambassador. Instead sent an email over CC, not BCC. To all official email accounts of every embassy in The Hauge. The attacker still had access through a man in the middle attack to the Saudi business email. They responded back to every embassy in The Hauge. Happy to have the direct attention of every embassy and the Diplomatic Corp. They upped the demand and taunted the Diplomatic Corp with all embassies on copy. What started as a $200 scam, to a $25K extortion demand grew to $35 million, then $50 million.

The attackers took the opportunity to threaten a VIP event, National Saudi Day which was held at a national Monument the Kuurhaus Hotel. If the $50 million was not paid. The guests ranging from celebrities, diplomats, ambassadors and Dutch royalty would all be killed. It was assumed the hotel would be blown up in a suicide attack.

Additional challenges arouse. The ambassador gave permission to alert the police and report a hack. However, the local police though hack meant someone had cut a hole into the embassy fence. The seriousness of the incident was not understood by the local police station. The police scheduled an appointment with a detective a week later. When the Saudi government and Aramco lawyers arrived for the appointment, they were greeted by a detective in ripped up clothing, 5 ‘clock shave and general disheveled appearance. Although the detective’s commander said the detective had recently returned from undercover duty. It was taken as a grave insult to the Saudi government and no further cooperation was given. When relations are already shaky, any minor issue or miscommunication can quickly be perceived as an insult.

Due to the terrorist threat, the Dutch Terrorist Police and Diplomatic Corp were permitted by the Ambassador to speak with me. I was chosen as the ambassador’s liaison . However, the ambassador did not trust any aspect of the Dutch government which I conveyed in his words. The Terrorism police were concerned about ISIS and shared a top ten hit/kidnap list had been discovered. I was number two on the list.

During the incident, I still had my regular role at Aramco in our EMEA headquarters. We began having issues with our neighbours, the Yemen embassy. We caught them digging on our property trying to access out fiber connection. An attacker can bend a fiber optic cable in a certain manner to surveil the light traffic. We caught some of their employees trespassing in our lunchroom. Harassing and insulting out female employees on our property. The Yemeni ambassador pulled out in front of m=one of my security employee’s car, halted traffic and yelled at my employee accusing him of following and harassing the ambassador and threatening physical assault.

As I was speaking to my boss in his office, the Yemeni embassy began flying drones to surveil the top floor of our building which was for the IT and security department.

The diplomatic Corps had to become involved, telling the embassy they were only permitted to fly drones over their own property, not our property.It was suspected the Iranian government had funded the purchase of the Yemeni embassy next door. Iran and Saudi do not get along, two years earlier Iran launched the Shamoon attack against Aramco. Almost shutting down the world's oil markets and costing the company billions. Still considered by insiders as the world's costliest cyber-attack.

Political cyber-attacks are those conducted by a state actor against another state actor for the purpose of achieving some political outcome. They can range from denial of service attacks to more advanced techniques such as Stuxnet and WannaCry. Geostrategic cyber-operations are those that have a broader scope than just a single country in mind, but instead focus on one or more regions in the world.

The digital world brings forward visions of transformation, innovation, efficiency. We are absolutely ingrained in bits and bytes and the convenience they bring. Do you even remember the last time you used a paper map to drive somewhere?

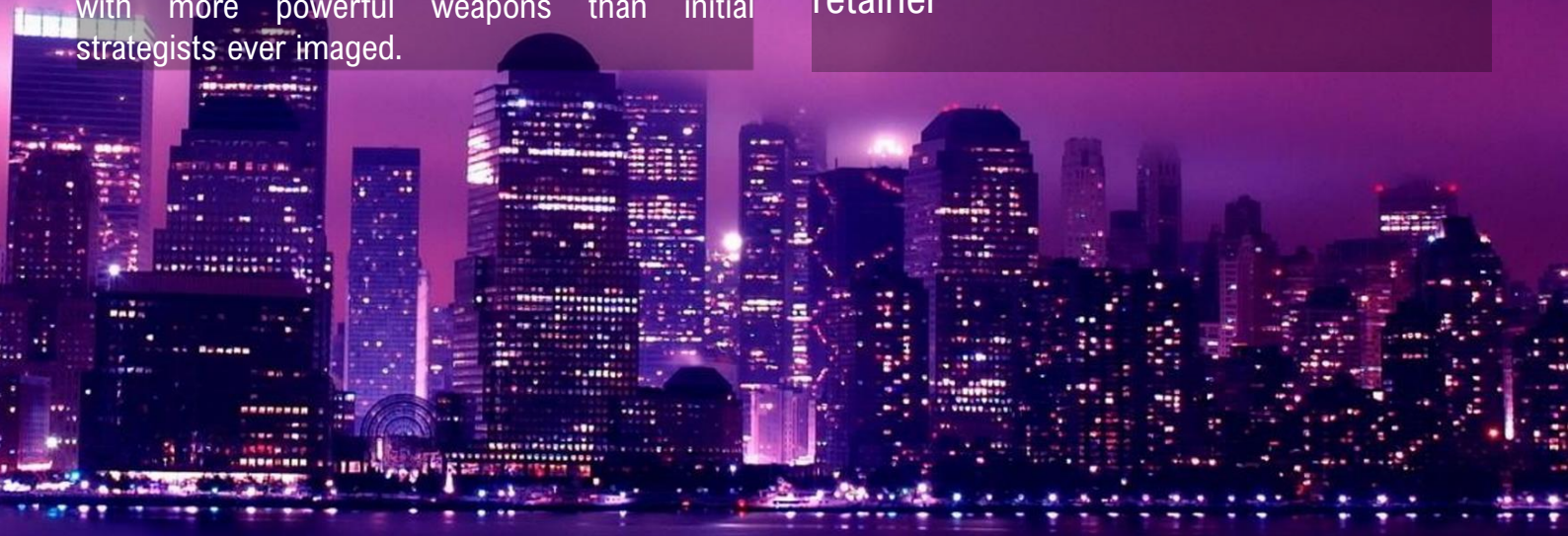
However, behind the scenes is a nefarious game at play. Failures in technology policy and diplomacy plague the industry. The reality of cyber warfare is not entirely new. Previously been clad with a more gigantic body and armed with more powerful weapons than initial strategists ever imaged.

When most people think about the word cyber warfare, visions of exploding items similar to Hollywood movies surfaces most often. However, the reality is much more damaging and insidious.

Focusing on the psychological affects on a population, diminishing trust in government systems whilst turning hearts and minds.

Risks to your organization and Key takeaways

- Proactive Open Source Intelligence against your own organization and key suppliers using tools such as Censys.io or Shodan.io
- Start or maintain a robust responsible disclosure policy
- Contact and foster a relationship with your national level civilian computer emergency response team
- Have an incident management company on retainer
- Have an experienced cyber lawyer on retainer

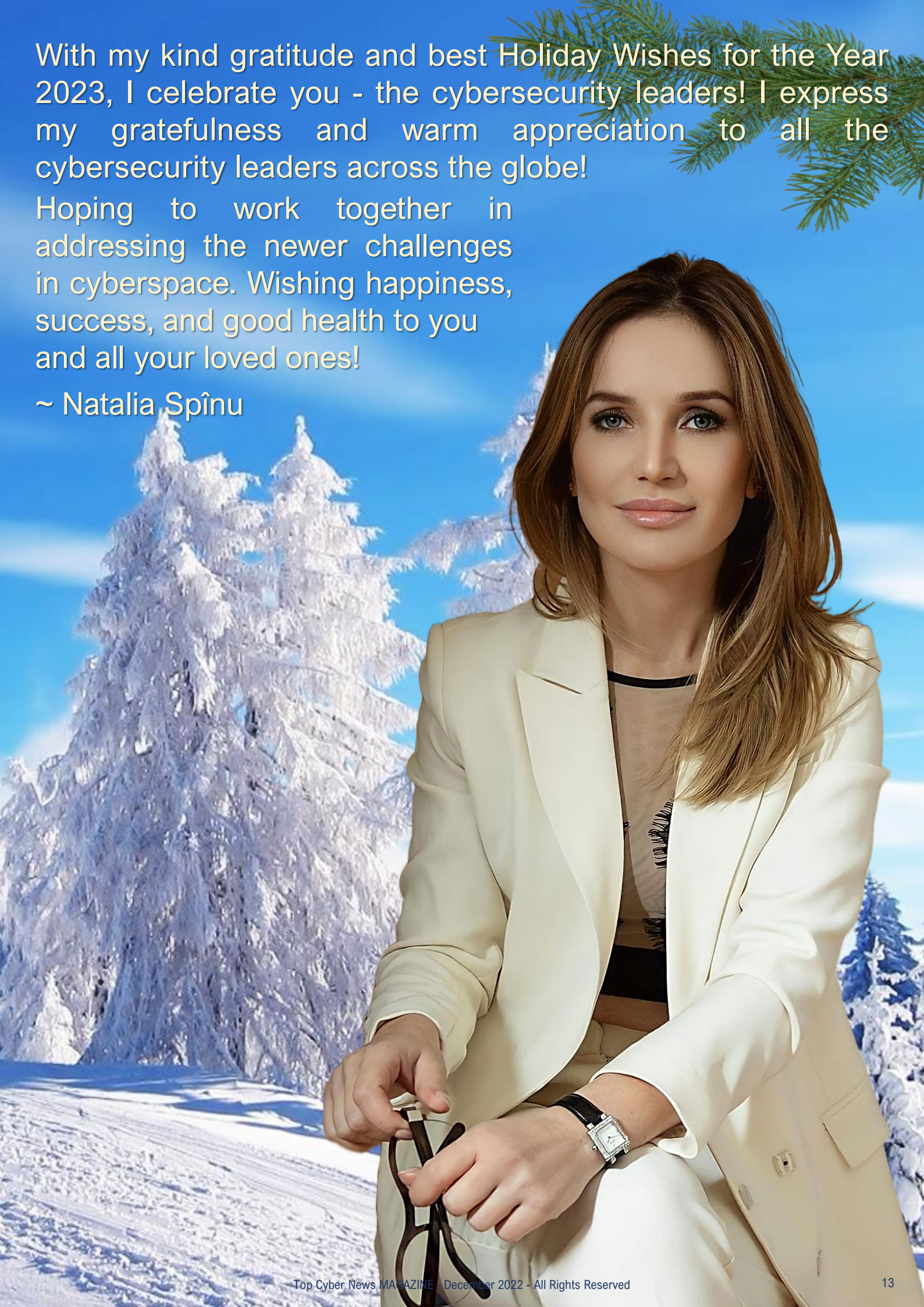


May Your Holiday Season Be Filled With Joy And Happiness! ~ Chris Kubecka

With my kind gratitude and best Holiday Wishes for the Year 2023, I celebrate you - the cybersecurity leaders! I express my gratefulness and warm appreciation to all the cybersecurity leaders across the globe!

Hoping to work together in addressing the newer challenges in cyberspace. Wishing happiness, success, and good health to you and all your loved ones!

~ Natalia Spînu



Data Privacy In The Age Of Digital Transformation

by Hafiz Sheikh Adnan Ahmed

Most of us have been hearing the term "digital transformation" pretty much everywhere for a few years now. It all started migrating business processes to automation, e-services were introduced, with the advent and usage of mobile phones we saw mobile apps for almost every line of business, Entire industries were transformed and moved a great deal of their activity online, embracing technologies like cloud storage, IoT and more. Digital transformation (DX) used to be something that's just good to have. But since COVID-19 disrupted business operations worldwide, many organizations now see DX as a necessary step in preserving their business. The Global Digital Transformation Market is Expected to Grow from USD 469.8 Billion in 2020 to USD 1,009.8 Billion by 2025, at a Compound Annual Growth Rate (CAGR) of 16.5% During the Forecast Period.

According to Finances Online, top benefits of adopting a digital model include improve operational efficiency, meet changing customer expectations, and improve new product quality.

It is also noteworthy to understand what does "digital business" mean to the organizations? It enables worker productivity through tools such as AI-assisted processes, ability to better manage business performance through data availability, and meet customer experience expectations.

With the advent of digital transformation over the last two decades has coined a new statement "data are the new oil", and that holds true from the fact that individuals, organizations, states, and countries across the globe are realizing the importance of data and data privacy. The bad guys are as intelligent as the good guys, and they know what they are after. With the massive migration in the last couple of years to remote working due to COVID-19, making better use of the cloud has exposed more data at risk, and it is still not sure if everybody is aware of that increased risk and how to protect it.

After the enforcement of the **EU General Data Protection Regulation (GDPR) in 2018,** which I **consider the mother of all modern data privacy laws and regulations,** states and countries around the globe are either adopting existing data privacy laws or creating their own. According to a 2021 report, 133 jurisdictions around the world have enacted omnibus data privacy laws. Throughout the last several months, many countries have announced and enforced data privacy regulations. For example, **China enacted the Personal Information Protection Law (PIPL), Saudi Arabia approved a personal data protection law that came into effect in March 2022, the United Arab Emirates (UAE) has published the UAE Data protection Law that introduces major changes to data protection in the UAE.**

So, now we are standing at interesting cross-roads. We want things to be done in a blink of eye, our lives are "digitalized", and are connected to devices all-around. Our lives are over-taken by robotics, chatbots, virtual assistants, virtual reality, Artificial intelligence, Machine Learning etc. Data ownership is flawed, on paper it looks to be controlled by one whose data it belongs to, but the reality is different - the data owners themselves are not aware as to how their data is been shared and used. Try looking out for some item on amazon on your phone and then go to any social media site, you will keep seeing the ad to buy that item - did you authorize amazon or those social media apps to do that, may not be, but then you have signed in their data privacy policy which in times is one way entry.

While digital transformation is creating major opportunities for organisations, it is also introducing a new dimension to the traditional view of risk. With industry 4.0, business leaders are making strategic choices on the investment, technology, resourcing levels and the skills needed to operate a digital business, all of which will have an impact on the short-term profitably and long-term viability of the businesses. These strategic choices inevitably involve an element of risk. At the same time, businesses must cope with external threats. For example, as businesses undergo digital transformation and more of their assets become digital, the threats of cybercrimes and risks around data privacy are growing.

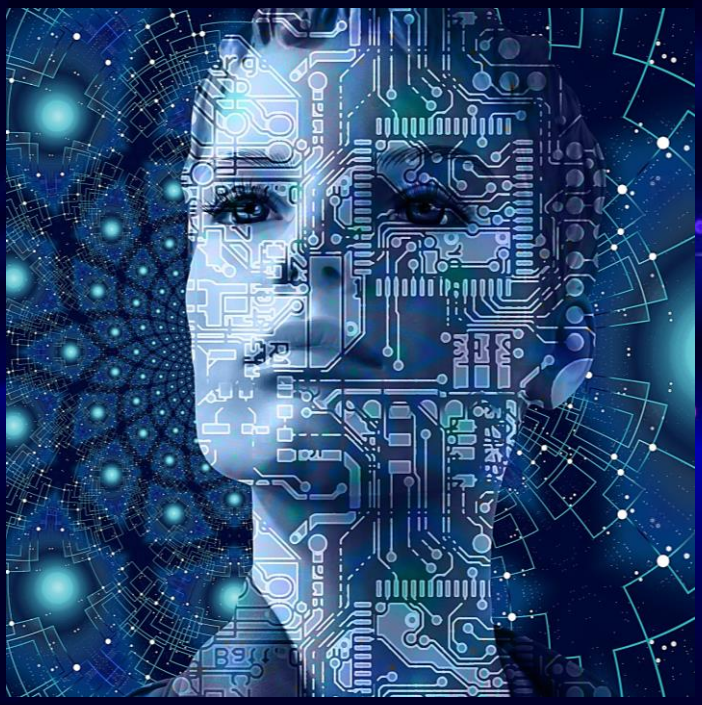
Let's take the example of Artificial Intelligence (AI). Artificial intelligence (AI) has developed rapidly in recent years. Today, AI and its applications are a part of everyday life, from social media newsfeeds to mediating traffic flow in cities to autonomous cars to connected consumer devices such as smart assistants, spam filters, voice recognition systems and search engines.

AI has the potential to revolutionize society, however, there is real risk that the use of new tools by states or enterprises could have a negative impact on human rights. The following are some of the major data privacy risk areas and problems related to AI:

- **Reidentification and deanonymization**—AI applications can be used to identify and track individuals across different devices in their homes, at work and in public spaces. For example, facial recognition, a means by which individuals can be tracked and identified, has the potential to transform expectations of anonymity in public spaces.
- **Discrimination, unfairness, inaccuracies, and bias**—AI-driven identification, profiling and automated decision making can lead to discriminatory or biased outcomes. People can be misclassified, misidentified, or judged negatively, and such errors or biases may disproportionately affect certain demographics.
- **Opacity and secrecy of profiling**—Some applications of AI can be obscure to individuals, regulators or even the designers of the system themselves, making it difficult to challenge or scrutinize outcomes. While there are technical solutions to help improve some systems' interpretability and/or ability to audit, a key challenge remains whenever this is not possible, and the outcome can significantly impact people's lives.
- **Data exploitation**—People are often unable to fully understand what kinds of—and how many—data their devices, networks and platforms generate, process or share. As consumers continue to introduce smart and connected devices into their homes, workplaces, public spaces and even bodies, the need to enforce limits on data exploitation has become increasingly pressing.
- **Prediction**—AI can utilize sophisticated machine-learning algorithms to infer or predict sensitive information from non-sensitive forms of data. For instance, someone's keyboard typing patterns can be analysed to deduce their emotional state, which includes emotions such as nervousness, confidence, sadness, or anxiety. Even more alarming, a person's political views, ethnic identity, sexual orientation, and even overall health status can also be determined based on activity logs, location data and similar metrics.

Let's now talk about IoT or Internet of Things. The Internet of Things (IoT) is a broad term that generally refers to physical devices connected to the internet that collect, share, or use data. This includes personal wearable devices such as watches and glasses, home appliances such as televisions and toasters, features of buildings such as lifts and lights, supply chain and industrial machinery such as forklifts and sprinklers, and urban infrastructure such as traffic lights and rubbish bins. IoT devices and the data they collect can provide convenience, efficiency, and insights into essentially every aspect of our world. For the public sector, the IoT is currently providing many benefits and has the potential to generate even greater public value in the future.

Consumers, governments, and businesses everywhere have been increasingly using IoT devices, and it is widely expected that the use of IoT will continue to expand rapidly. However, rushing into the IoT without proper consideration of privacy can lead to harmful and unexpected consequences. As the IoT grows, the amount of data it generates will naturally increase alongside it. These large collections of data can, in many cases, constitute personal, health and sensitive information, raising many privacy challenges.



Some of the challenges around data protection include, for example:

- **De-identification of IoT data** – The data collected by large IoT ecosystems like smart cities can be valuable for a range of purposes such as research or informing policy decisions. A common way to maximise the value of this data is to make it publicly available online. However, it is generally impermissible for datasets that include personal information to be made publicly available.

The simplest way to ensure personal information is not included in a dataset is to allow individuals to remain anonymous by never collecting information that can identify them. However, data collected by the IoT is often very difficult to de-identify due to its highly granular nature.

- **Transparency** - The passive nature of many IoT devices can make it difficult for individuals to be informed that their personal information is being collected. Devices in public spaces can collect information automatically, sometimes relying on individuals to opt-out if they do not want their information collected.

- **Accountability** - The number of organisations that can be involved in an IoT ecosystem can make it difficult to identify who is, or should be, accountable for what. The nature of IoT devices can make it impossible for an organisation to have control over every aspect of it. For example, organisations often have little or no control over security and privacy risks with communication technologies such as satellite or 5G, as these are usually provided by third party telecommunications companies. This can also be the case for cloud services, which can allow users to have anywhere from no control to high control over the security and privacy settings of services they are using.

• **Interoperability** - The rapid expansion of the IoT in recent years has led to the development of many kinds of devices, Application Programming Interfaces (APIs) infrastructure, data formats, standards, and frameworks. This has caused significant interoperability issues, in that devices, software and data from one vendor often do not work with devices, software and data from other vendors.

Data Privacy Solutions For The Digital Transformation

Privacy laws have never been as important as they are today now that data travel the world through borderless networks. Exciting times ahead for privacy legislations as several notable privacy laws will be enforced. Cross-border transfers are likely to be one of the notable compliance issues tackled by legislative bodies and data protection authorities to ensure the regularization and normalization of data transfers between countries.

Governments around the world are reacting to the increased demand for data protection through different legislations. There is a proliferation of data protection laws during the last few years, which introduced new compliance requirements for organizations. In the case of new regulations, it is vital to achieve a balance between protection and free movement of sensitive data. Global compliance involves safeguarding sensitive data like payment and personal information.

The EU's General Data Protection Regulation (GDPR) is a landmark privacy law and a milestone for the digital age. It has introduced new rights for individuals, such as the Right to be Forgotten and the Right to Portability, as well as made breach notification mandatory.

A consideration business should make is hiring Privacy Architects and protection officers to assess their objectives and the privacy legislation that they will have to comply with. Businesses need to ensure that DPOs (Data Protection Officers) should be expert in both privacy and technology, a rare yet essential combination of expertise. This isn't just a matter of data privacy but compliance as well. While investing in the right security solutions will enhance business' posture against new technology-related risks, organizations need assistance in tackling this challenge from a compliance point of view.

Businesses need to work towards implementing transparent and secure mechanisms. With the right security solutions, companies can achieve the freedom and flexibility they need to succeed in a digital economy with confidence. Businesses need to define data governance strategy and privacy/protection should be at the heart of this strategy. It should include regular training, awareness, and workshops on digital technologies and how to protect personal data while using those digital technologies. Besides external threats like phishing attacks, organisations should keep in mind to guard their sensitive data against insider threats as well. The latter requires a focus on understanding and securing the data itself.

Businesses also need to employ data security governance principles by focusing on sensitive data protection and privacy, conducting, deleting unnecessary data, and consolidating data silos, whether they are on-premises or in the cloud, to ensure project alignment with business objectives.

The Final Verdict

Despite its potential pitfalls, digital transformation remains an extremely exciting venture for businesses of all shapes and sizes. The prospect of leveraging cutting-edge technology to accelerate their business' processes and thereby making themselves more competitive is certainly attractive. However, data privacy should always be a foundation of any digital transformation project, as without it, the whole house will start to fall.

At the end of the day, companies that incorporate transparent privacy policies into the building blocks of their companies are the ones that will see increased brand loyalty moving forward. They're the ones who are actively pursuing ways to incorporate blockchain into the processes—who are actively working to not just meet but exceed the guidelines of the General Data Protection Regulation. They're the ones who actively empower their customers to offer them information, knowing it will be used to enhance their user experience—no more, no less. But **in the next 3 to 5 years, I anticipate privacy will become a game-changer for the companies that do it right. It will bolster trust—and ultimately sales. And customers will, thankfully, be all the wiser for it.**

About the Author

Hafiz Sheikh Adnan Ahmed's journey started back in 2005 as a Quality Assurance Engineer and over the years, he shaped his career in the areas of information and communications technology (ICT) governance, Information and Cybersecurity, business continuity and organizational resilience, data privacy and protection, risk management, enterprise excellence and innovation, and digital and strategic transformation.

Hafiz is an analytical thinker, writer, certified trainer, global mentor, and advisor with proven leadership and organizational skills in empowering high-performing technology teams. He is a certified data protection officer and won chief information security officer (CISO) of the Year awards in 2021 and 2022 by GCC Security Symposium Middle East and Cyber Sentinels Middle East, respectively.

Hafiz is a public speaker and conducts regular training, workshops, and webinars on the latest trends and technologies in the fields of digital transformation, information and cybersecurity, and data privacy. He is an ISO Lead Auditor and ISO Management Systems Auditor for ISO 9001, ISO 20000, ISO 22301, ISO 27001, and ISO 27701 Management Systems. He volunteers at the global level of ISACA® in different working groups and forums.

He is the Co-Founder and CIO of AZAAN Cybertech Consulting, and his role is to drive and align business strategies of the company's esteemed clients towards Information and Cybersecurity centric and to oversee the people, processes, and technologies within the organizations to ensure they deliver outcomes that support the goals of the business. To know more about AZAAN Cybertech consulting, log on to: https://azaan.net.au

Hafiz can be contacted through email at hafiz.ahmed@azaanbiservices.com


A new year. A fresh, clean start! It's like having a big white sheet of paper to draw on! A day full of possibilities! A year full of cyberattack free! Sending you all warmest wishes as you enjoy the holidays. May you feel renewed to embrace the possibilities that 2023 has to offer.
~ Hafiz Sheikh Adnan Ahmed


In 2023, the conversations, knowledge sharing and true collaboration among global experts will be the key to a stronger defense. Let the New Year 2023 be prosperous, healthy and filled with global peace for all! ~ Carmen Marsh

Cyber Security Trends That Need Great Focus In 2023

by Sourish DATTA

Organizations are struggling to be as good as the emboldened adversaries in the cyber space who have access to seemingly endless intelligence, compute power and tools, sometimes along with state sponsorship. The threat that organizations face is not only limited to their systems and data; they extend to the value of their brand and trusted relationships in marketplace.

In recent years we have seen the topic of cyber security move from being a technology problem to the board room and hence here's a look at some of the key cyber security trends for organizations and the board members to focus in 2023:

IoT Devices Possess A New Cybersecurity Threat Paradigm

As the IoT devices are becoming an integral part of our digital lifestyle and workplace (IT and OT), the need to focus on cybersecurity is essential. **As per recent analysis, 69% of IoT devices are vulnerable to cyber threats.** In coming years, several initiatives around the world will be triggered aimed to increase security of connected devices and networks that tie them together. This includes a labelling system for IoT devices to provide consumers with information on possible security threats posed by these devices and consumers should consider the inherent risk profile of these devices before introducing them in their ecosystem.

Adoption Of Zero Trust Is A Must For Organisations

Zero Trust is not a technology but is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating a digital interaction / transaction by adopting the principle of “never trust and always verify”.

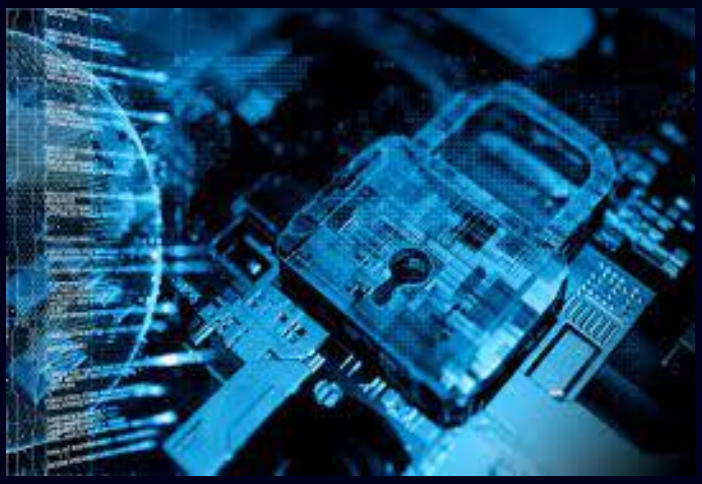
It helps in securing an organizations infrastructure and data in the digital era by requiring all users (internal or external), to be authenticated, authorized, and continuously validated before being granted or assess ongoing access to systems, applications, and data. Zero Trust is enabled by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying fine-grained “least privileges and least access” policies.

Edge Computing And Data At The Edge Presents New Threat

One of the growing concerns for organisations is the increased attack surface that comes with distributing data and processing power to the edge. Securing data at the edge also can be difficult due to the remote location of edge devices. Organizations must consider these challenges and implement adequate security measures when planning their edge computing strategy.

Couple Biometric Authentication With Continuous Contextualized Authentication

Biometric authentication is rising as organizations attempt to bolster their access control measures. This identification method uses physical or behavioural characteristics to verify someone's identity. Is Authenticating once enough? Continuous Contextualized Authentication based on behavioural patterns or other attributes will make it more difficult to spoof than other methods. Additionally, it can provide a higher level of assurance that the user accessing a system is who they claim to be.



Quantum Computing Threats Are Looming Large

As we are moving rapidly towards a digitalized world, quantum computing threats are becoming a reality. The unprecedented processing power of quantum computers will enable it to rapidly decrypt information, potentially making national or business secrets accessible to adversaries. Another threat posed by quantum computing is denial-of-service attacks by flooding a system with requests in a short time. This attack could have severe outcomes for entities that rely on their online systems availability.

Secure Access Service Edge (SASE) Is Emerging

With digital transformations driving adoption of Cloud and SaaS platforms, the attack surface has grown manifolds. The SASE approach to cybersecurity plays a crucial role in protecting today's distributed information systems. The SASE framework enables remote work and the use of cloud-based services by shifting the security policy enforcement point away from the corporate network and applying it wherever users are located. SASE adoption brings cloud native security technologies like CASB, SWG, ZTNA, SD-WAN and NGFWs together and ensures speed, and ease of maintenance across multiple applications and platforms for organisations.

5G Led Data Breaches Are Becoming A Reality

Data breaches are becoming more common as we increasingly rely on technology. 5G is promising faster speeds and more connectivity than ever; but with this increase in speed and connectivity comes an increased risk of data breaches. There are several ways that 5G data breaches can occur - 5G networks are often unencrypted, meaning anyone within range can access them. It makes it easy for malicious actors to intercept data transmitted over the web.

Focus On Nation State Actors Targeting Critical Infrastructure

Nation-states frequently take part in cyber-espionage and sabotage to undermine unfriendly or competing governments, impact availability of critical infrastructure, financial benefits or to access secrets. Currently, however, it's increasingly likely that organizations with national significance will find themselves targeted by state actors. Organisations (especially with critical infrastructure) hence should be aiming at appointing a cyber defence team focused on nation-state, and task that team with reviewing all information sources on a regular basis and summarizing the potential impact for the organization and hold periodic meetings with other security teams to ensure they have adequate counter measures to mitigate nation-state cybersecurity risks.

Cognitive Artificial Intelligence (CAI) To Play A Prominent Role In Cybersecurity

As cyberattacks become more advanced, organizations are turning to AI to help them detect and respond to threats. Machine learning algorithms can examine the vast amount of data moving across networks in real-time far more effectively than humans can and learn to recognize patterns that indicate a threat. The use AI and automation to detect and respond to data breaches can save an organization's system, data and reputation.

Cloud Security Needs More Attention

As the world increasingly moves toward a cloud-based systems to support their digital lifestyle, cybersecurity becomes a top priority. A successful attack can lead to availability issues, data loss, financial damage, and reputational damage.

There are several counter measures that organisations can take to improve their cloud security posture which include implementing access controls, strong authentication measures, encrypting data in transit & rest, and using intrusion detection and prevention systems.

Threat Intel Sharing Is Necessary For Contextualisation

As threat actors become progressively more sophisticated, it is increasingly essential for organizations to share threat intel and leverage the industry's collective knowledge to improve their security posture and implementation of adequate protective measures in a timely manner. With detailed and contextualized threat intel, organizations can better anticipate and identify malicious activity and utilize intelligence to fast-track detection and prevent attacks.

Build A Robust Incident Response Capability

A rapid and effective response, as well as supporting playbooks for specific attack scenarios, can lower costs, minimize disruption and damage, mitigate harm to an organization's reputation besides restoring normal operations as quickly as possible after a security incident, malware attack or data breach. The first stage of uplifting the maturity is to document a robust incident response plan and testing the processes in a simulated environment on a periodic basis.

Security Of Remote Workforce Is At The Focal Point Post Pandemic

A recent cybersecurity priority for many organizations has been to secure the millions of devices that are being used for home and remote working, since the start of the pandemic. In 2023 and beyond, when workers are more likely to use personal devices to remotely connect to work networks, a new set of challenges has emerged; connecting to networks with non-secured devices or connecting devices to unsecured networks can lead to employees falling victim to a magnitude of attacks which puts the employer at risk.

The risk of this also increases in remote working conditions, where it is more likely that devices may be left unattended.

Build A Strong Security-Aware Culture

The most important step that can be taken by any organization is to ensure that it is working towards initiating and fostering a culture of awareness around cybersecurity issues. Today, it is no longer enough to simply think of cybersecurity as an issue for the IT department to resolve. Developing an awareness of the threats and taking basic precautions to ensure safety should be a fundamental part of every employee's responsibility in 2023.

Build Cyber Insurance Needs To Be Done Right With ALE Considerations

Adequate cyber insurance should cover the cost of replacing damaged infrastructure, lost data as well as the labour costs to investigate the incident, rebuild systems and restore data. Organisations should also start considering insurance for productivity loss resulting from a major system failure or catastrophic event. Cyber insurance value hence should be calculated based on an organisations cybersecurity risk using the concept of annual loss expectancy (ALE).

Sourish DATTA, Australia

Sourish Datta is a strategic, result-oriented Security & Risk Management leader with almost two decades of global experience in leading security transformation for organizations by providing thought leadership, influence, and collaboration to drive enterprise level change. Mr. Datta has a proven track record of leading cyber resilience strategy and security service delivery for organizations aimed to deliver best-in-breed security capabilities to protect against cyber threats. Mr. Datta specializes in setting enterprise security vision which has a demonstrable result of improving the ROI besides driving value & consistency of security outcomes across the business domains.

Sourish is also entrusted by organizations to lead governance, compliance and audit programs which includes working with industry & government regulatory bodies to inform them about the organization's adoption of regulatory requirements, obligations, risk posture and remediation / maturity uplift roadmap besides periodically reporting on any breaches, risks, and incidents on critical infrastructure.

We are on the verge of a new era where the real world and virtual world of Digital Twins melt into a new universe - Metaverse and Web3 that will transform society over the next 10 years.

However, data security problems will be similar, even much more worse than today's cyber security challenges.

Now is the time to think of newer cyber security challenges. In the year 2023, let's gear up our cyber security posture and stay cyber safe. Have a wonderful Christmas and a Happy New Year 2023!

~ Gurleen Barara & Col (Dr) Inderjeet Singh

When A Robot Gives Better Estimates Than A Human

by Bo THYGESEN

For organizations with many (several hundred) systems quantitative IT risk management can be likened to a window cleaner being asked to clean the United Nations headquarters in New York. He will never finish before the first couple of windows need cleaning again. The process of quantitative risk assessment, which involves many systems and respondents, can be close to impossible to execute. The challenge means that one either fails to do the experiment or goes to qualitative methods, which are probably fast but problematic for the reasons we have mentioned in several posts.

Imagine the following situation:

- Your organization has 100 IT-systems
- Each system is estimated to be exposed to 10 threats
- Each asset-threat combination has 3 possible consequences with individual loss distributions

This situation gives 3,000 scenarios (100 x 10 x 3), which must be estimated and calculated in a quantitative assessment. A qualitative approach would mean asking the respondents to place each scenario in a 5x5 heatmap. If we estimate that every scenario requires 5 min. of work, we have a 250-hour project in front of us. It requires resources, and the result is a useless analysis placebo.

What can we do?

Imagine that we could develop an estimation robot that we can influence with a series of basic assumptions and data points about each IT system, after which the robot calculates the risk picture. Imagine further that it can do it with such high quality and speed that you can use the result as decision support in real-time.

Using a robot to determine probability and loss

Using statistical regression analysis (it sounds difficult but is a standard function in Microsoft Excel) is effective for analyzes where the uncertainty and the number of estimates is large. In an analysis with many systems, each with individual security settings, all of which can be affected by several types of events, we can advantageously prepare an estimation robot (LENS model developed by Egon Brunswik and described by Douglas Hubbard and Richard Seiersen in "How to Measure Anything in Cybersecurity Risk").

The purpose is to let the respondents, who previously have been dragged through painful estimation processes, alone determine the settings for their systems. They typically do this with much less uncertainty than if they are asked about the probability or consequence of several scenarios. For example, we ask whether the system has implemented multi-factor authentication (also known as MFA). The system owner will know this, making the data point high in quality.

Based on a system where we know the system's properties, the model can estimate the probability and the loss in different scenarios. A positive side effect is that the modelled estimates are better than the estimates the individual system owners would provide.

This is because the model can remove the inconsistency that respondents typically impose on the risk assessment. Inconsistency in experts' answers is well described by, among others, David Kahneman in his book "Thinking Fast and Slow".

The construction of an estimation robot follows the following overall phases:

1. Identification and calibration of the relatively few experts who must participate in providing reliable estimates
2. Identifying the characteristics relevant to assessing the probability and loss of cyber incidents targeting the systems
3. Selection of risk scenarios for the individual systems based on an assessment of their properties
4. The estimation phase where the experts estimate the probability and the loss for the selected scenarios.
5. The analysis phase where logistic regression analysis is carried out using the average of expert estimates as the dependent variable and input to the experts as the independent variable. Here we remove the noise of human inconsistency.
6. The result phase where the most suitable formula is extracted as the logistic regression for both probability and loss.

Can you picture it? We get a small group of selected and calibrated experts to provide estimates that depend on the characteristics of the systems. These estimates are of good quality when we have removed the noise that typically occurs in connection with all human judgments. Now we can scale to many individual systems with different characteristics.

Blown away

ACI had the pleasure of working with this model with a very large Danish organization in the financial sector. We were, to say the least, rather excited to see the model in action. The system owners submitted their answers to the systems' security settings, and we pushed the button and got a data set that could be included in a simulation. With the simulation, we were able to present key figures that the steering group could relate to immediately. Due to the use of the LENS model, we were able to proceed with adjustment and validation many weeks earlier than would otherwise have been possible.

Another notable result was the response rate among the system owners that had increased significantly due to a more accessible and faster completed questionnaire survey.

All models are wrong – some are useful

We naturally remember that "all models are wrong, but some are useful". If we continuously calibrate our model against reality. Registration of incidents with sufficient details to create feedback to the estimates and assumptions allows us to improve the model. We might find that certain assumptions in our model must be adjusted. Perfect – we adjust and make the model better. The absolute worth thing to do is to just lean on the model without feed-back.

Meteorologists and bridge players are among those who can give the best forecasts. Do you know why? They practice. They constantly get feedback on their predictions. They continuously calibrate themselves and become more cautious for the next predictions. If we also, do it with the predictions that our estimation robot produces, we end up with a model that is capable of prediction or forecasting. In this way, we will be able to intervene in advance. This is worth a lot of money.

We do not doubt that these models are the future of risk assessment in multi-system environments.

Bo THYGESEN, Denmark

Bo Thygesen was born 1967. He holds a BSc. in IT-software development and a project management degree from University of Washington. He is certified in Governance of Enterprise IT, and Information Security Management. He was a CIO for 10 years and saw the limitations of classic qualitative IT-risk management methods firsthand.

“In many cases risk management was something we did for the sake of compliance. A lot of effort without adding any value” he says. IT is extremely important today and he believes we should use methods for risk management that are based on sufficient evidence. Methods that have been used since the 50s for the construction of bridges and high-rise buildings, the aircraft industry, financial instruments, etc. He founded ACI A/S in 2009 and has since then dedicated his professional life to help companies to develop IT-risk management to the highest standards. “We want to enable our clients to get real forecasts from their risk management activities” - Bo says

To all Cybersecurity leaders across the globe, I appreciate everything you do to continue to keep cyberspace safe. I look forward to contributing and working together in 2023 and beyond to address our relentless challenges in cyberspace. May you and your loved ones enjoy a Safe and Joyful Holiday Season and a Fruitful New Year ahead! ~ Dr. Vivian Lyon

Understanding the ICS-OT Cyber Security Risks is Mandatory for Cyber Defense

BY DANIEL EHRENREICH, CONSULTANT AND LECTURER, SCCE

In recent years, industry experts have been exposed to new vulnerabilities detected in Programmable Logic Controllers (PLC) supplied by a range of well-known vendors. This exposure leads to growing concerns about possible cyber-attacks against Industrial Control Systems (ICS) / Operation technology (OT) systems. Among the published internally and externally generated cyber security incidents, you find attacks that may directly or indirectly affect the industrial process and cause operation outage, damage, and risks to lives.

To protect industrial and utility plants, you must deploy a range of SRP (Safety, Reliability, Productivity) triad-related measures. In some cases, these solutions must also satisfy the CIA (Confidentiality, Integrity Availability) triad-related requirements. This paper aims to help the readers to understand how to perform risks assessment for ICS-OT systems and select suitable cyber defense solutions.

Cyber Security Risks Analysis

The following paragraphs will guide you through scenarios that describe various ICS-OT-related cyber security risks. The charts and the descriptions below will help you to correctly understand the risk factors and select the most suitable, practical, effective, and cost-effective cyber defense.

1) How do cyber incidents happen?

Here we must differentiate between failures created by hardware products or software bugs, incorrect actions of authorized personnel, and cyber-attacks, which can be internally or externally- generated or supply-chain related. The three suggested attack factors below may be associated with multiple possibilities.

Analyzing the security level (SL1 to SL-4 factors according to ISA/IEC 62443) will help you understand who or what organization might initiate the attack, the level of their expertise, and how much resources they have are willing to allocate. Upon analyzing Figure 1 below, your organization may select the industrial facility's most suitable defense or risk mitigation solution.

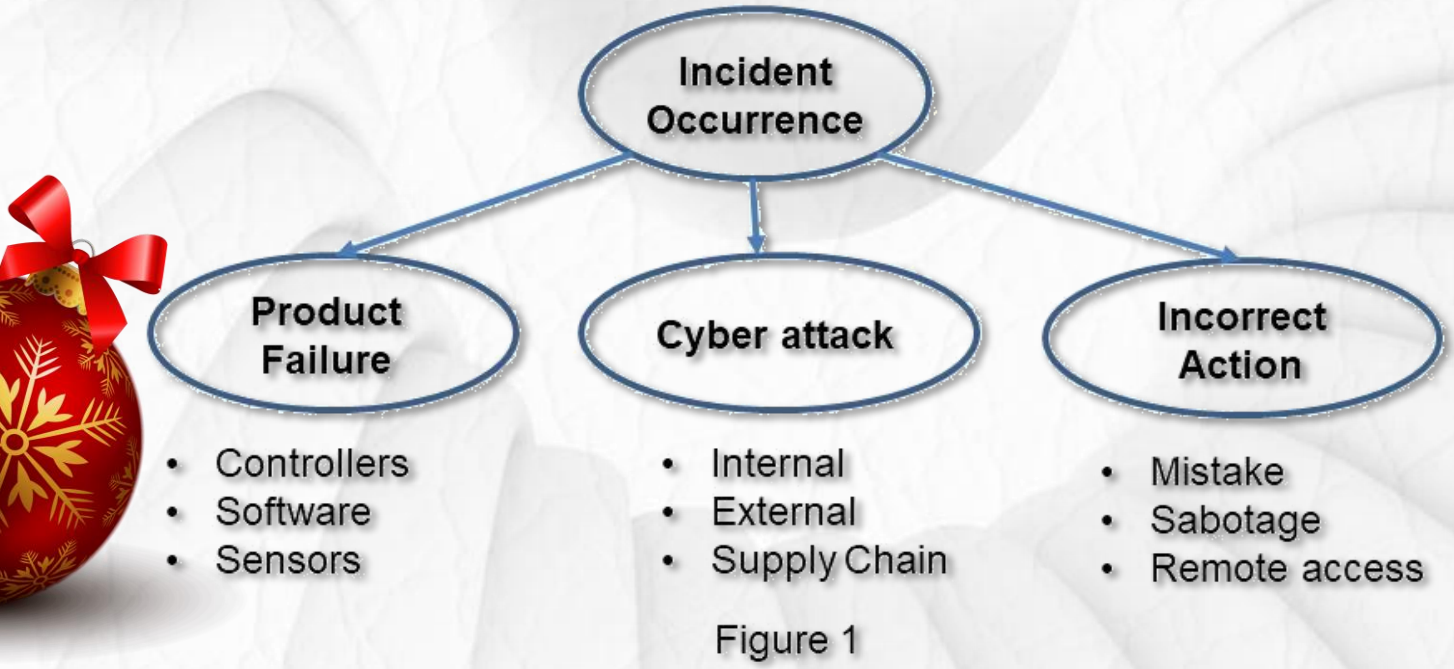


Figure 1

2) Which factors might lead to a cyber-attack?

Cyber security incidents are initiated following the combination of three factors. According described in Figure 2 below, a) the ICS-OT architecture might have one or more unsolved vulnerabilities caused by hardware, software, physical security, or poorly structured application program, b) someone or an organization must have a light or strong motivation, and c) the attackers must have the confidence that the planned attack process is possible.

Understanding the "driving factors, based on the SL1 to SL-4 elements defined at ISA/IEC 62443, the organization may select the most suitable defense or risk mitigation solution. It can be achieved by strengthening the end-point protection, perimeter security, or another defense measure.

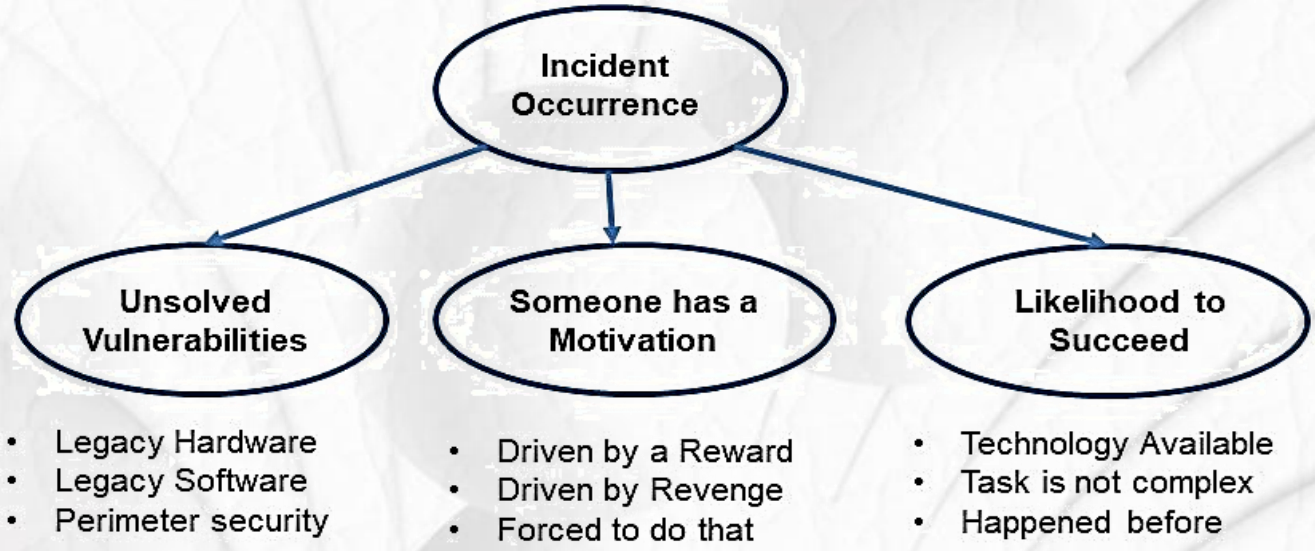


Figure 2

3) Differentiating among the cyber-attack vectors.

The essential activity conducted by defenders is to differentiate among the possible attack vectors and attack paths. The Lockheed Martin Cyber Kill Chain and the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) are suitable tools for this evaluation and for reaching conclusions related to cyber defense.

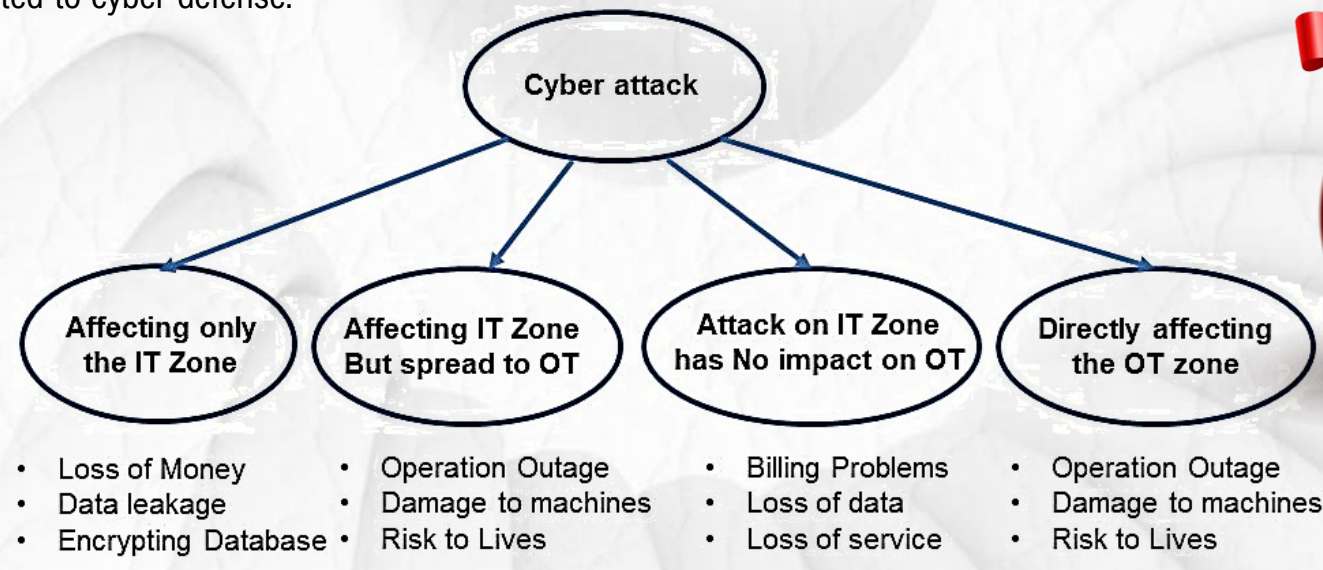


Figure 3

In Figure 3, you see an illustration of these possibilities. An attack might start directly in the ICS-OT zone (usually an internally generated) or the IT Zone (usually an externally generated action). The initiated attack might directly or indirectly affect the SRP-related requirements at the industrial plant or utility operation.

4) Consequences of a cyber-attack against an industrial plant

When analyzing the possible impact on an industrial facility, it is essential to realize the amplitude or the severity of that incident. The lowest impact may be a short operation outage (minutes or hours), or a lengthy outage (weeks up to months) caused by the harming factors described below. A higher level of impact might lead to repairable or even non-repairable damage.

In the worst case, the result of a cyber-attack may hurt the lives of a few or many people. Figure 4 below illustrates these possibilities and may help the organizations' experts to combine multiple layers of defense to select the most suitable and effective defense solution.

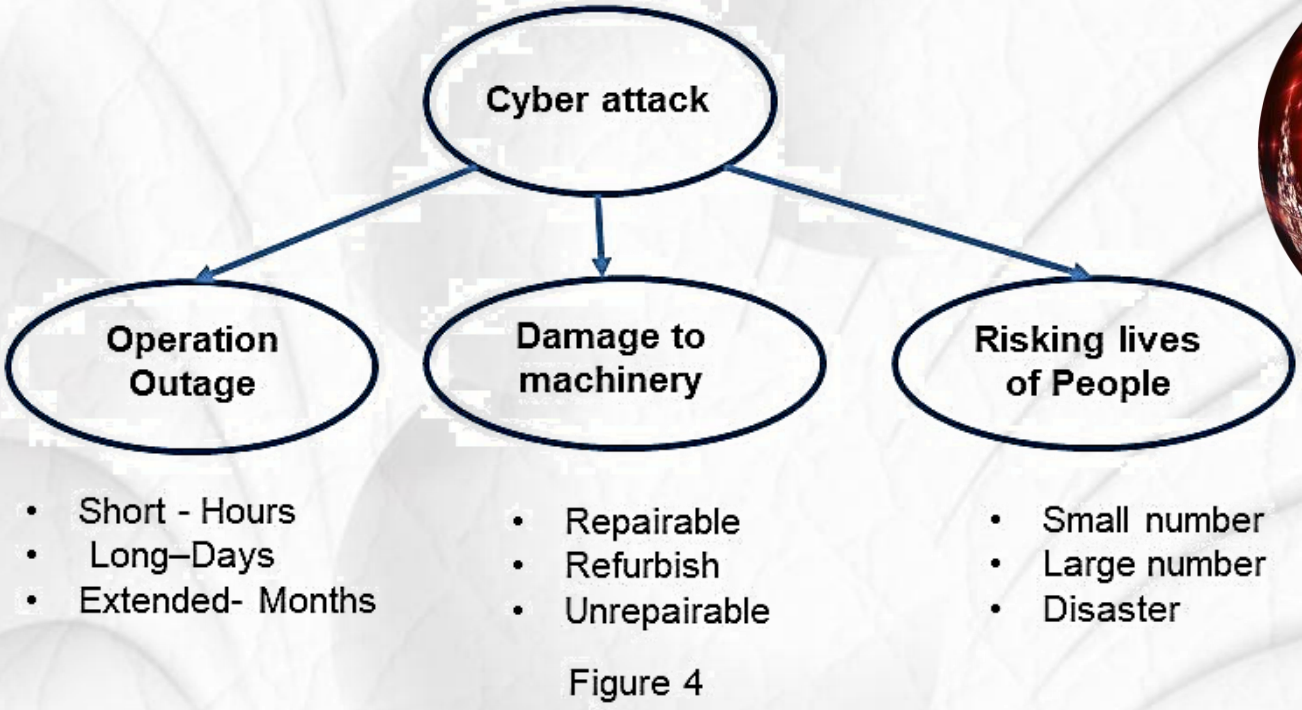


Figure 4

5) Factors allowing the cyber security incident

When analyzing the possible factors that might lead to a cyber security incident, that process might be pointing to a) poor physical/perimeter or endpoint security, b) incorrectly designed Applications Program, and c) lack of attention to critical factors described by the PPT (People-Processes - Technologies) Triad. Organizations must pay attention to physical processes which must be conducted at the plant according to "Security by Design" principles.

The PPT Triad focuses on the training of employees and subcontractors working in the facility, the existence of correctly defined procedures, and the consistent process aimed to retrofit legacy-type hardware and software. Substantial mentioning here is that organizations that do not conduct at least one annual assessment might be exposed to cyber-attacks for the reasons described above.

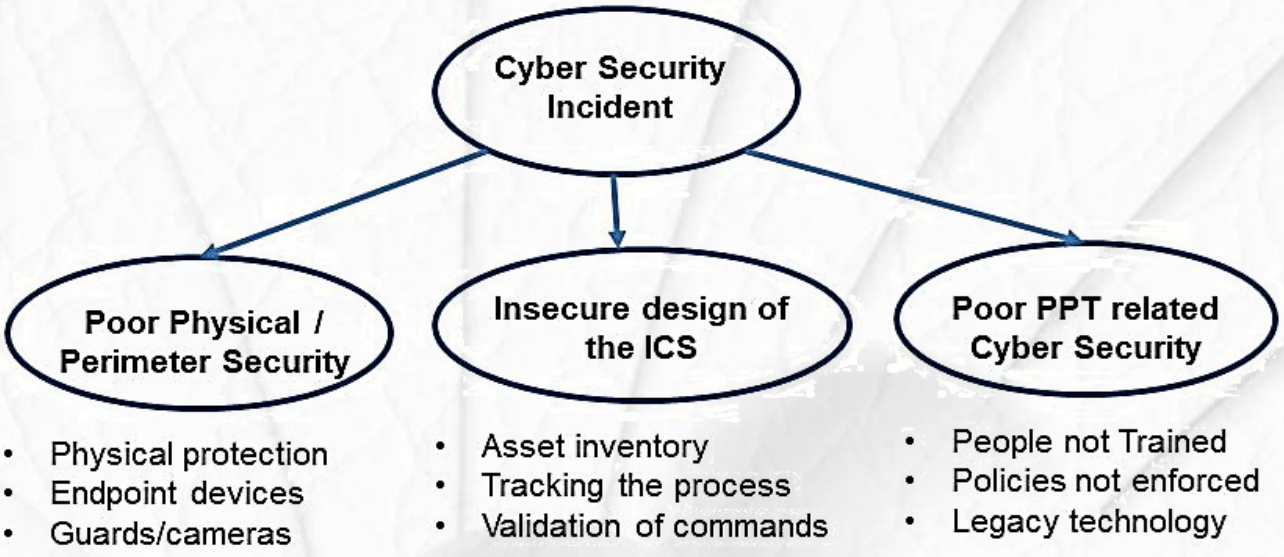


Figure 5

Summary and Conclusions

Important to mention in the summary section, that investment in education for employees on cyber security risks and defenses has the highest Return on Investment (RoI) among all PPT actions.

ICS-OT cyber security experts know well that to select the most suitable, effective, and cost-effective cyber defense, their team, must understand the plant's physical process, the control architecture, and the operation of the ICS-OT system. Once these learning processes are completed and confirmed, the local teams can start to analyze the sources of malfunctions, sources of cyber-attacks, evaluation of people or organizations who might initiate the attack, etc. Experts must accurately evaluate the possible attack vectors (using practical tools mentioned above) and assess the possibility of conducting a direct attack on the ICS-OT zone of the attack that might start by compromising the IT-related architecture.

Consequently, essential to strengthen here that strong perimeter/physical defense is a mandatory precondition to cyber security, and robust cyber security and network segregation are mandatory preconditions to operating safety. Finally, IT and ICS-OT experts must collaborate toward selecting and deploying correctly designed cyber defense.

The role of the management at industrial and utility-related facilities is to allocate the needed resources to be at least one step ahead of hostile attackers.

Daniel EHRENREICH, Israel

Daniel Ehrenreich, BSc. is a leading Industrial Control System (ICS) expert and acting as consultant and lecturer at Secure Communications and Control Experts (SCCE) consulting entity, based in Israel. Periodically conducting workshop sessions via Internet and in person for educating international participants on ICS cyber security risks and defense measures for a broad range of ICS verticals.

Studied CISSP in 2014 and is certified as a Lead Auditor for the ISO 27001-2013 standard by the Israeli Institute of Standards. Daniel has over 30 years of engineering experience with ICS for: electricity, water, oil and gas and power plants as part of his activities at: Tadiran Electronics, Motorola Solutions, Siemens and Waterfall Security.

TOP CYBER NEWS MAGAZINE

Human Centered Communication Of Technology, Innovation, and Cybersecurity

AN AWARD-WINNING DIGITAL MAGAZINE

ABOUT PEOPLE, BY PEOPLE, FOR PEOPLE

Ludmila Morozova-Buss

Editor-In-Chief

Doctoral Student at

Capitol Technology University

As we move into 2023, the world faces many challenges, not the least of which is growing cybercrime. We are optimistic that with collaboration and an understanding that cyber security is everyone's accountability, we can work together to build strong cyber security cultures for the benefit of current and future generations. Merry Christmas and Happy New Year 2023!

~ Christiane Wuillamie OBE and John R Childress

We are all dependent of the Internet and security and privacy should be part of our personal and corporate DNA. Create alliances, work together, share best practice, develop and innovate responsible and with security, privacy and integrity in mind. Start prevention early and realise it is a long lasting effort. Humanity Will Survive The Internet. It will be a bumpy road. We better buckle up and get started. ~ Troels Oerting

TOP CYBER NEWS MAGAZINE

BRING TECHNOLOGY TO THE FRONT OF THE BUSINESS

Human Centered Communication Of Technology, Innovation, and Cybersecurity