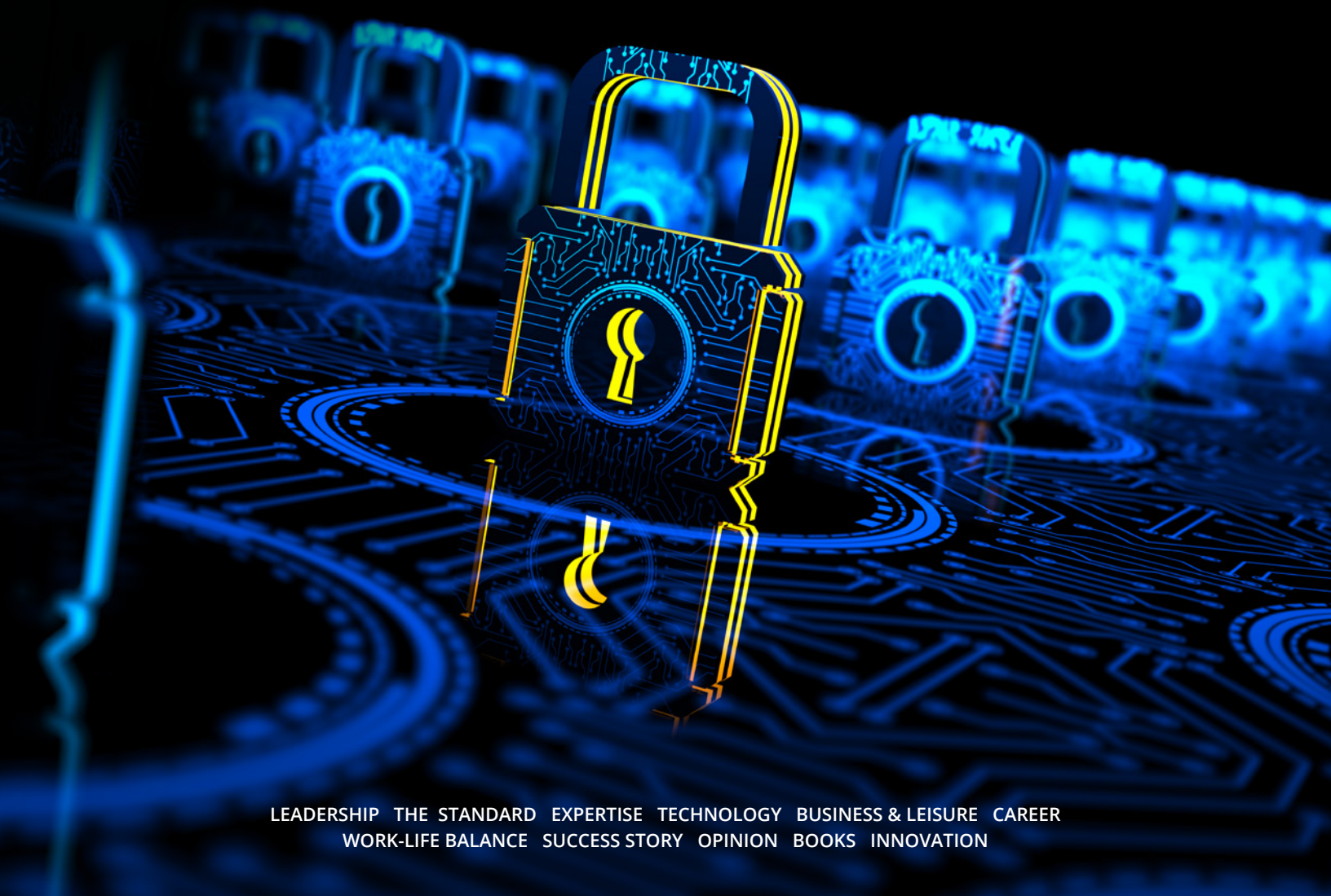
PECB Insights

ISSUE 39 ISO STANDARDS AND BEYOND JULY-AUGUST 2022

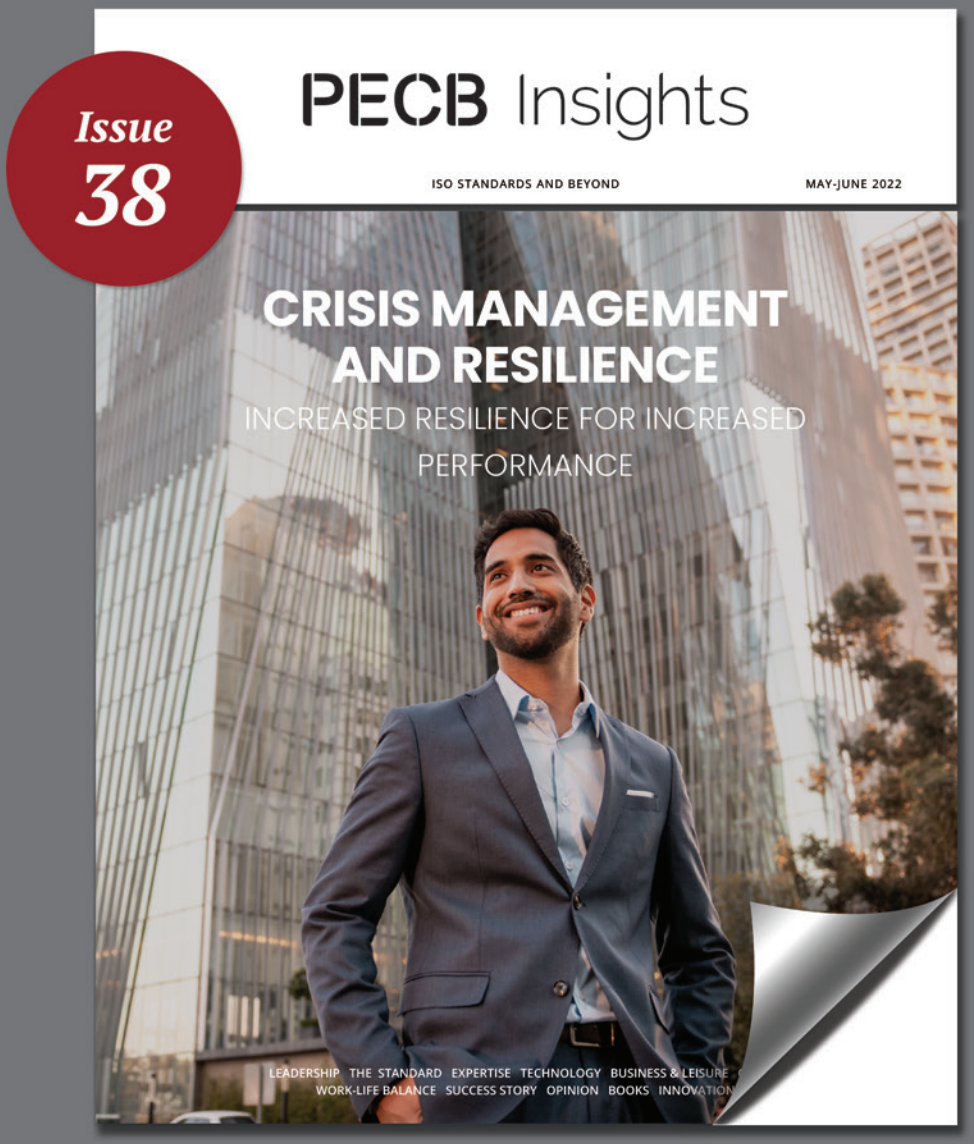
NETWORK SECURITY, ETHICAL HACKING, AND CYBERSECURITY

PROTECT YOUR ONLINE PRESENCE



PECB Insights Magazine

delivered to your mailbox



Subscribe & find out more at

www.insights.pecb.com

In This Issue

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic."

STEPHANE NAPPO
Vice President - Global Chief
Information Security Officer Groupe SEB

WHY METROLOGY MATTERS IN THE DIGITAL ERA

Tomorrow's metrology is the science of measurement for the digital economy.

Digital technologies such as artificial intelligence, big data and machine learning are increasingly important to the manufacturing industry. Just imagine the implications on metrology – the science of measurement.

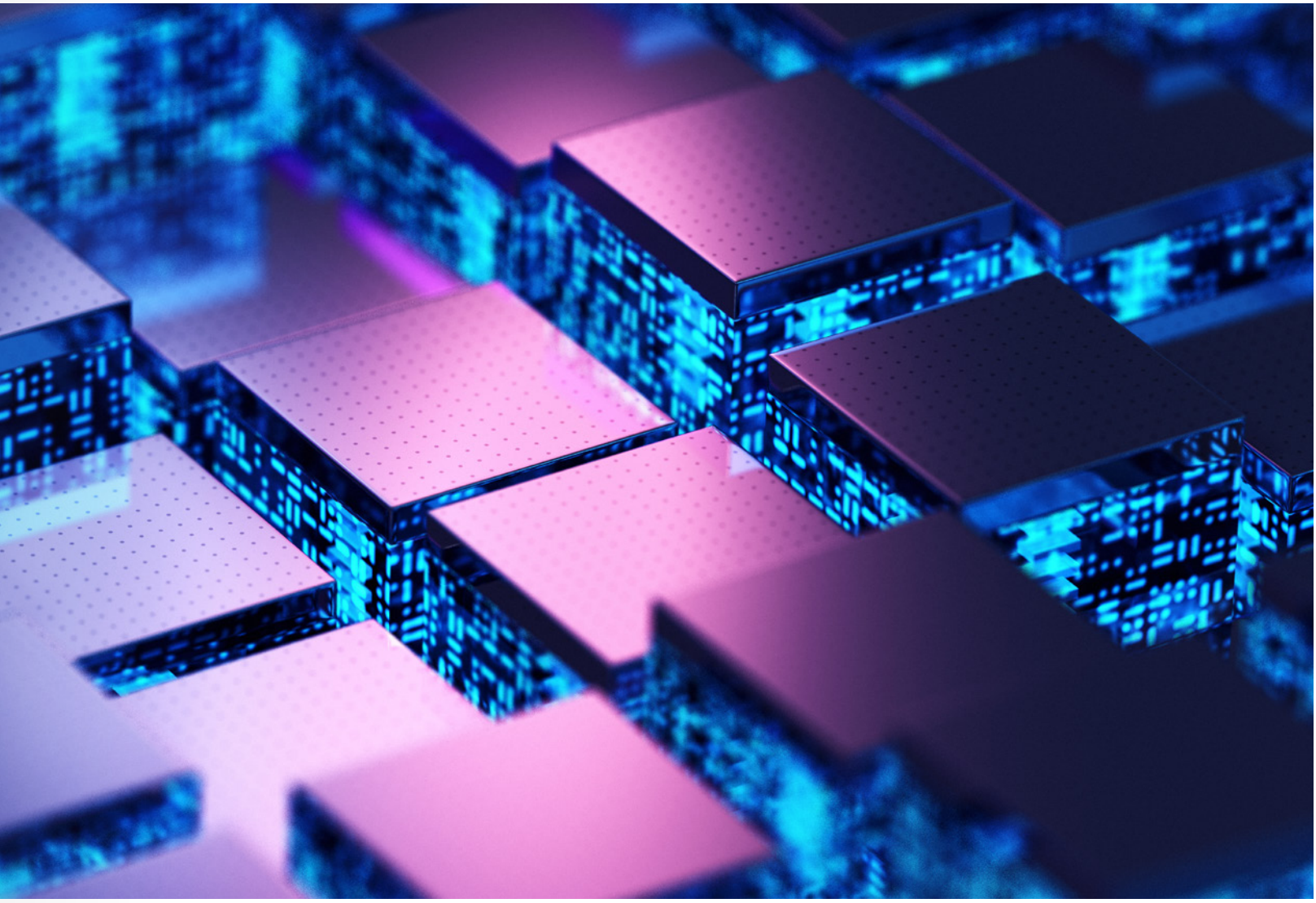
"Metrology in the Digital Era" is the theme of this year's World Metrology Day, celebrated annually on 20 May. The theme was chosen because digital technology is revolutionizing metrology and is one of the most exciting trends in society today. Accurate and fair data is an important cornerstone of the digital development of science and technology. The resulting **high-quality data**, based on measurement standards, is the key to taking our industry to the next level in the digital milestone.

As the BIPM and BIML directors state in their joint message: "The digital transformation of metrology can bring many benefits to our community. It can expedite time to market for measurement products and services and reduce delays associated with approval processes. In turn, this contributes to innovation, product agility, and sustainability."

ISO has just signed the Joint Statement of Intent on the digital transformation in the international scientific and quality infrastructure. The joint statement provides a platform for the signatory organizations to indicate their support in a way that is appropriate to their particular organization.

This common understanding will help advance the development, implementation, and promotion of the SI Digital Framework as part of a wider digital transformation of the international scientific and quality infrastructure.

> **The digital transformation of metrology can bring many benefits to our community.**



The Joint Statement of Intent is part of an ongoing initiative to develop and establish a worldwide uniform and **secure data exchange format** based on the International System of Units (SI), also known as the SI brochure.

The ISO 80000 series of standards for quantities and units is a vital element of the SI brochure as it provides harmonized terms, definitions, and symbols of quantities and units used in science and engineering, providing a unified language for communicating accurate measurement information between scientists, engineers and anyone involved in measurement.

The SI Digital Framework will enable the implementation of new services that make best use of open data formats, software tools, and services that build upon the SI core representation. Such services will help to produce high-quality data and make it available for analysis in a coherent and consistent form. The outcome will be new digital applications developed and deployed in the broader metrology community and in research disciplines that rely on the SI.

The joint statement had previously been signed by the BIPM, the International Organization of Legal Metrology (OIML), the International Measurement Confederation (IMEKO), the International Science Council (ISC), and its Committee on Data (CODATA). “The addition of ISO further strengthens the collaboration and global reach of the initiative,” reads the BIPM press release.

Celebrated each year on 20 May, World Metrology Day commemorates the day back in 1875 in which the Treaty of the Meter was signed, laying the foundations of a global system for common measurements that are all based on constants of nature. The International Bureau of Weights and Measures (BIPM) and the International Organization of Legal Metrology (OIML), which organize World Metrology Day, actively liaise with a number of ISO technical committees.

What Do Cyber-Attacks Entail?

BY VIJAY KUMAR

The cyber world is growing rapidly. Everyone is involved, either directly or indirectly. Everything is available with a single click or tap on your mobile, tablet, or PC. You can browse websites, listen to or download audio, video, and software, place your order, buy products, book tickets, hotels, buses, taxis, etc. It has been made easy for everyone due to the cyber world or digital world. You can see the very bright side of the cyber world, which you are enjoying in your daily routine, however, there is a dark side to the cyber world that exists in reality, called Cyber Crime or Hacking.

Have you ever heard about cyber crime? It happens due to cyber-attacks.

What is a cyber-attack?

The most valuable asset, nowadays, is data, not only for organizations but also for individual users. If you are able to protect your information or data, you or your organization are stable and secure. Perhaps at first glance, it is difficult to understand the importance, for those not that well-versed with this industry, however, understanding the need to stay protected is of high value today. Cyber-attackers, at all times, are seeking these assets.

If you have data, you may fall victim to a cyber-attack.

We can define cyber-attacks as any type of illegal action by cybercriminals, hackers, or cyber experts attempting unauthorized access against a computer, information system, network, infrastructure or personal computer, or devices including; tablets, mobile phones, smart watches, smart TV, or other smart devices with the help of various methods to steal, alter, breach, modify, or destroy data or information systems.

What are the typical cyber-attacks?

1. Malware

In the cyber world, it has become common knowledge that around 300,000 thousand new pieces of malware are created daily.

Malware is a piece of code (software) that can be installed easily on your server, laptop or desktop, mobile device, tablet, etc., and it is used to leak private information or gain unauthorized access to data, information, or systems.

As stated by Datto, some types of malware are:

- Viruses — These infect applications by attaching themselves to the initialization sequence. The virus replicates itself, infecting other files or code in the computer system. Viruses can also attach themselves to executable code or associate themselves with a file by creating a virus file with the same name but with a .exe extension, thus creating a decoy that carries the virus.
- Trojans — A program hiding inside a helpful program with malicious purposes. It is commonly used to steal information or establish a backdoor to be exploited by attackers.
- Worms — Unlike viruses, they do not attack the host, being self-contained programs that propagate across networks and computers. Worms are often installed through email attachments. They are commonly used to overload an email server and achieve a denial-of-service attack.
- Spyware — These programs are installed on laptops, mobiles, and other devices and are used to collect information about users, their systems, or browsing activities, sending the data to a remote user, the hacker.

2. Phishing

Approximately 6.4 billion fake emails are sent every day. For this reason, the attacker targets many victims for a phishing attack.

The most common and popular cyber-attack is Phishing, which indicates sending mass quantities of fraudulent emails to unsuspecting users, in a manner that appears as a reliable source.

Phishing attacks can also occur via social media, direct messages, or other online communities targeted by users with hidden intent.

There are multiple types of phishing attacks, as follows:

- Spear Phishing — Specific organizations or individuals are targeted
- Whaling — In an attempt to gain access to classified information, senior directors, stakeholders, or C-Level executives are targeted
- Pharming — Attacker uses Domain Name System (DNS) cache poisoning attack and manipulates DNS entry, to then redirect to a fake landing page to capture user credentials
- Voice Phishing – SMS Phishing – Attackers use phone calls or text messages to manipulate users in order to collect information

3. Ransomware

Ransomware is malware that encrypts critical data of a user or an organization so that they cannot access files, databases, or applications. The attacker decrypts the data and makes it available to the victim only after the ransom is paid. If the victim does not get access to the private key, it is impossible to decrypt those encrypted files that are being held by ransom. According to snap-tech.com, global ransomware damage costs are predicted to exceed $265 billion by 2031.

4. Cryptojacking

Cryptojacking is another form of cyber-attack. It involves the malicious act of the hacker, entirely hidden from the victim, to unauthorized use of the victim's computing resources for mining cryptocurrency.

5. Drive-By Attack

In a drive-by attack, sometimes referred to as a drive-by download, the attacker seeks vulnerabilities in various web browsers, plugins, or apps, to launch the attack. No action from the victim is required to initiate. With the help of this attack, hackers can hijack the device, install malware, keylogger, or spyware to spy on the user's activity in an attempt to steal critical data or personal information.

6.MitM (Man-in-the-Middle) Attack

This is the most common attack and it is performed through public Wi-Fi. The attacker inserts themselves between the public Wi-Fi AP and the visitor’s device and starts intercepting a two-party communication or a transaction. From there, cyber-attackers can steal the password credential and other sensitive information, or potentially manipulate data by intercepting traffic.

7.Session Hijacking

In this attack, the attacker takes over a session between a client and the server, this leads to the victim losing access to their social media accounts.

8. Password Attack

Because passwords are the most basic used mechanism to authenticate users to an information system, obtaining passwords is a common and effective approach to attack. Hacker uses sniffing, social engineering, and other techniques to get access to passwords, to a password database, or outright guessing. The last approach that can be done, in either a random or systematic manner, is brute-force and a dictionary attack.

9. Rootkits

Hackers install rootkits inside legitimate software, therefore, once the victims install this software on their system, it is activated and attackers can gain remote control or administration-level access over a system. Later, the attacker uses it to steal passwords, keys, or other credentials, and retrieve critical data.

10. Internet of Things (IoT) Attacks

Multiple research shows that a large percentage of organizations worldwide have experienced an IoT attack.

Attacks on IoT devices grow rapidly due to gaining popularity and since these devices are given low priority to embed security in their operating systems.

11. Denial-of-Service (DoS) Attack

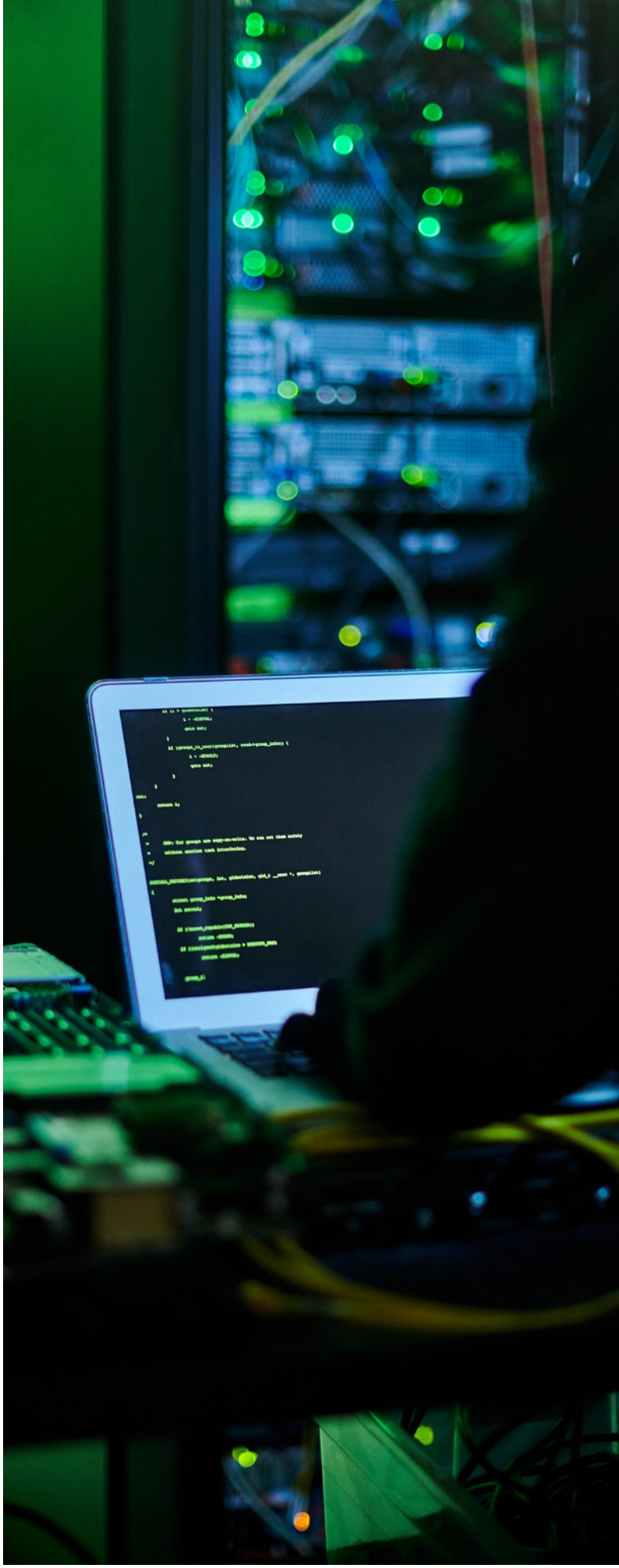
In a DoS attack, attackers work by flooding traffic to systems, servers, or networks, and overload resources and bandwidth. In result, the server or system is unable to process legitimate requests. Another type of denial-of-service (DoS) attacks is distributed denial-of-service (DDoS) attacks.

12. SQL Injections

In this attack, an attacker inserts malicious code into a server using a server query language (SQL) forcing the server to deliver protected information. This happens on unprotected or less secure websites.

13. Zero-Day Exploit

A Zero-day Exploit refers to exploiting an unknown vulnerability in an application, system, network, etc. It also refers to exploiting a new and recently announced vulnerability prior to any patch being released or implemented.



14. Cross-Site Scripting

A cross-site scripting attack sends malicious scripts into content from reliable websites (unprotected or less protected). The malicious code serves with the dynamic content to the victim's browser. Usually, this malicious code may have JavaScript code executed in the victim's browser but can include Flash, HTML, and XSS.

Facts about Cyber-attacks:

1. Botnets are responsible for 31% of all cyber-attacks targeting corporate networks.
2. Education and Research was the most targeted sector, which are facing an average of 1,605 weekly attacks.
3. The malicious file type EXE is making up 52%, PDF comprising 20%, and DOCs in 5% of all malicious files.
4. Over 84% of all cyber-attacks were distributed via e-mail in 2021.
5. Cybercriminals can penetrate 93% of company networks.
6. Cyber-attacks are up 50% in 2021 in comparison to 2020, peaking in December, largely due to Log4j exploitations.
7. Software supply chain attacks have increased by 650%, in 2021.
8. The healthcare industry has seen a 51% increase in breaches and leaks since 2019. Furthermore, 70% of surveyed organizations reported healthcare ransomware attacks.
9. By 2025, cryptocurrency crime is predicted to surpass $30 billion, up from $17.5 billion in 2021 according to Cybersecurity Ventures.
10. In a recent phishing attack, $7 million in NFTs were stolen from OpenSea users.
11. In 2021, organizations experienced the highest average cost of a data breach in 17 years at $4.24 million, rising from $3.86 million the previous year.
12. Mobile apps are responsible for 80% of mobile fraud.

Can ethical hacking protect you from cyber-attacks?

Ethical hacking not only protects you from cyber-attacks but also combats the hacker. Hacking is a bunch of skills, methods, and techniques used by a hacker to commit a cyber-attack.

Ethical hacking is the process of hacking in an ethical way, the persons who are involved in this process are called ethical hackers.

Ethical hackers are responsible to:

- Test a system, application, or network for security vulnerabilities to evaluate its performance.
- Test the security of the system and find any weakness they suggest ways to improve it.
- Perform regular pen testing, which helps to improve the security of the system, web app, and network.
- After identifying vulnerabilities in the system, they should create reports and provide feedback after the issue has been resolved.
- Inform the organization of the possible effects on its operations and users.
- Use hacking as a technique to find solutions for the system's exploiting points.

Essential steps to protect yourself from cyber-attacks:

- Install anti-virus and anti-malware software on your devices (PC, mobile).
- You must set up a strong password (combination of number, small and capital letters, symbols, and numbers), gesture, or fingerprint.
- Avoid using most commands and basic passwords. Use different passwords for different websites.
- Always hide or switch off Bluetooth when not in use and disable automatic connection to networks.
- Do not open emails from unknown sources (email addresses) and avoid risky clicks.

Vijay Kumar
Ethical Hacking, VAPT, CEH, CompTIA Security+, CySA, Linux, and Networking Trainer

Vijay Kumar has several years of experience in the field of cybersecurity as a trainer, writer, and consultant. He has experienced in delivering training on Ethical Hacking, VAPT, CompTIA Security +, CompTIA CySA+, CEH, OSCP, Linux System & Server Administrator, Networking Basic and Advanced. He has delivered trainings to individuals, college students, corporates, and Government Bodies. You may reach him through https://cyberpratibha.com/

PECB is Delighted to Receive the "Most Innovative Cybersecurity Training" Award 2022

This award is presented to PECB by the prestigious Global InfoSec Awards 2022, which honors companies that present a unique and valuable scheme for their services and products.

We would like to deeply thank our customers and network for their continual trust and support. Through that, we have been able to accomplish yet another achievement that reinforces our credibility, hard work, and commitment to continuously provide the greatest quality services to our clients.

FIND OUT MORE ▶

Ethical Hacking vs Penetration Testing

BY BASSEM LAMOUCHI

During the last decade, we have faced the grim reality that is cyber-attacks in their most sophisticated forms. Incidents orchestrated by malicious actors that tested many companies' cybersecurity practices, and even brought other companies to bankruptcy.

The goals for such attacks often vary, depending on the actor, malicious actors do it for financial gain, activists operate for a multitude of reasons, fun, profit, and to advocate change, and state-aligned actors attack each other as a new form of warfare.

These attacks have been getting more and more sophisticated as time goes by; there are many examples, such as the most prolific ransomware group, Conti, which managed to gain $180 million from its victims last year through various cyber-attacks, or the Netwalker ransomware attack executed on Equinix, one of the largest data center provider companies in the world, demanding $4.5 million.

As these attacks evolve, the defending side also adapts and develops in order to be able to protect and secure public and private infrastructure from these devastating attacks, often using new, innovative, and clever ways, since the ancient ways of simple cybersecurity and compliance audits are no longer sufficient all by themselves.

This is the difference or gap created by modern, sophisticated cyber-attacks. Two decades ago, a crude but thorough cybersecurity and compliance audit was necessary since most corporates infrastructure was relatively small compared to the modern, federated, decentralized, cloud, and microservice-based infrastructure.

Securing, auditing, and maintaining massive modern networks requires considerable time and effort with a specific competence not easily found among most network engineers and other IT professionals.

Many new approaches and strategies have been invented to deal with this issue, so far, the most commonly utilized strategy is the employment of a wide set of practices under the term "ethical hacking."

What is ethical hacking exactly, and what does it constitute?

In simple terms, ethical hacking is an authorized, simulated attack against a computer, network, or organization to identify existing cybersecurity vulnerabilities and system misconfigurations, gauge the risks, and protect them from real threat actors (malicious hackers).

It is possibly one of the most effective, time and cost-efficient ways to enhance an organization's cybersecurity posture due to its flexible nature and realistic practices.

Are such practices legal?

The target organization explicitly authorizes these operations in order to assess their security posture and fix any weaknesses that exist within.

In fact, these operations are often ordered by the higher-ups of the organization, sometimes without the knowledge of the subordinates in order to simulate an actual attack, but this is not always the case, as the scope and goals always vary from one operation to another.

Who executes ethical hacking operations?

Authorized attacks are often carried out by professional cybersecurity experts known as "white hats or white hat hackers." Regarding technical proficiency, white hats must present a thorough, top-to-bottom expertise in networks, operating systems, databases, web servers, web applications, mobile applications, and other concepts, such as Cloud Computing and IoT.

As for trade proficiency, white hats must have a grasp of the legalities surrounding the operation and the industry as a whole, the principles of information security, and the compliance involved.

What does ethical hacking consist of?

Ethical hacking is a very broad term that helps companies to evaluate the risks of cyber-attacks and can encapsulate many operational concepts depending on the customer goals and his desired scope of simulation, but the four most relevant ones are; vulnerability assessments, penetration testing, red teaming, and bug bounties programs. These different operations vary in size, scope, rules of engagement, and goals.

A. Vulnerability Assessment

Usually considered an audit against a target or a list of targets that vary in nature (networks, computers, or applications) and attempts to find all known vulnerabilities.

Vulnerability assessments attempt to discover a very wide area of vulnerabilities, misconfigurations, and non-compliances that developers and system administrators usually cannot catch, a vulnerability assessment must be thorough, enforcing, and methodical.

Vulnerability assessment follows a very specific four step lifecycle:

1. Asset discovery
2. Asset prioritization and target configuration
3. Vulnerability scanning
4. Result analysis and actions

1. Asset discovery

First, the operator needs to make sense of the target infrastructure and understand the big picture; this usually is a tricky phase since the operator has no guarantees that the target will be fully visible, and even if it is, it is even tougher organizing their digital footprints.

2. Asset prioritization and target configuration

This part of the assessment is completed by organizing the assets into clearly ordered priorities and organized attack metrics, this is not necessary if the customer can afford a full scan on each and every single one of its assets, but most cannot afford it, so they resort to scanning their most critical assets, which are usually public internet facing web applications, servers, or internal critical infrastructure, such as a domain controller, some targets require finer tuning than others depending on their nature, criticality, and robustness.

3. Vulnerability scanning

The most important step of the process, using a massive database of publicly known vulnerabilities and the ability to scan, probe, and attempt to check the target's service vulnerabilities. It is only a matter of time until the vulnerabilities are identified and the report is generated based on a predefined baseline. At this stage, the pentester team must well configure the vulnerability scanners to reduce the number of false positives.

4. Result analysis and actions

Vulnerability scanners, no matter how advanced, are still tools; they may generate false positive, and they may identify a vulnerability that does not really exist or bump up the severity rating on a relatively harmless bug, therefore, human bug triaging and analysis is instrumental to a successful assessment, the operators will check and recheck for the existence and severity of identified bugs, as well as vulnerabilities in an attempt to patch them in a suitable manner.

B. Penetration Testing

Often like a red teaming exercise, penetration testers use their experience in order to attempt to attack all possible angles of the organizational structure.

Penetration tests also consist, usually, of a five step comprehensive lifecycle:

1. Planning and Reconnaissance
2. Scanning
3. Gaining System Access
4. Persistent Access and Housekeeping
5. Analysis and Reporting

1. Planning and Reconnaissance

This phase covers describing and defining the scope as well as limits of the test and a preliminary, (often automated) information gathering mission in order to understand the infrastructure and topology of the target entity. By the end of this step, the pentester team will have as much information as possible to map the attack surface.

2. Scanning

This phase, based on the information acquired from phase one, attempts and gets not only a complete top-to-bottom granular technical overview of the target entity's technology stacks (services, defensive measures, etc.), but also a list of vulnerabilities that can be exploited.

3. Gaining System Access

The penetration testers parse all the information they have acquired throughout phase one and phase two and look for misconfigurations and exploitable vulnerabilities that will allow them to gain network or system access belonging to the target then run the payload to exploit the target.

4. Persistent Access and Housekeeping

Once one or more systems have been successfully attacked, the penetration testers try to understand how far they can go inside the target system by trying to infect more machines, intruding on more networks, escalating their privileges, packaging, and exfiltrating as much valuable data as possible. The testers must not forget that housekeeping is essential; any modifications to the target systems must be reverted and rolled back; in other words, the target system must be exactly what it was like before starting the penetration test.

5. Analysis and Reporting

The penetration testers compile the results and findings of their operation into a report, findings such as the vulnerabilities exploited, a list of machines successfully infected, and weaknesses found in security systems.

This report will be sent to the target organization for analysis. In the meantime, the penetration testers will work with the corresponding team to fix any weaknesses they find. It is pivotal that organizations running critical infrastructure conduct, regularly and often, penetration tests to get the most accurate and complete overview of their security posture.

C. Red Teaming

Attempts to simulate a real threat, actor's attack against the target organization, trying to gain access and reach the goals by any means necessary.

Most members in the organization should have no idea that a red teaming operation is taking place. Otherwise, it defeats the purpose.

Operators will use tactics that emulate known adversaries (criminals, state actors), as well as develop their own tactics.

Red teaming follows an attack lifecycle very similar to penetration tests, but unlike penetration tests, where the target is to map out and exploit every attack vector possible, the red team's target is to reach a well-defined objective, such as access to a server, access to a network, creating a successful data breach, or acquire domain controller admin account. Usually, red teaming operations follows the MITRE ATT&CK framework and mostly deliver the attack using social engineering.

D. Bug Bounties

A method of loose cooperation between corporations and paid volunteers in the form of a bounty program, bug bounties are essentially companies giving ethical hackers the permission to attempt and exploit their applications and infrastructure, as long as the ethical hacker responsibly cooperates in vulnerability disclosure and the payoffs are often massive.

Many large corporations such as FAANG (Facebook, Amazon, Apple, Netflix, and Google) or even government organizations, such as the US Department of Defense (DoD) implement their own bug bounty programs.

This kind of program will help companies to fix new vulnerabilities, assign them a unique ID called CVE (Common Vulnerabilities and Exposures) and then add them to the database of publicly known vulnerabilities which is used by vulnerability scanners.

Each of these methodologies and operations employs ethical hacking and is essential to maintaining a sufficiently advanced cybersecurity posture to protect organizations and their subsidiaries and assets from harm caused by all sorts of malicious actors in cyberspace.

Neither of these methodologies is enough on its own, and they all must be combined and carried out regularly or risk asset loss through cyber-attacks.

Bassem Lamouchi
EC-Council and PECB Trainer | Third Party Auditor | CISSP | SOC Analyst | CEH MASTER | CHFI | ECIH

Bassem is a cybersecurity and Cloud Computing professional with highly valuable technical skills. He has successfully led many security audits, incident handling, and forensics projects in the private sector and particularly in the banking and financial services sector. Bassem has gained valuable international experience which includes working in Ivory Coast, Mali, Niger, Togo, Senegal, Benin, France, Canada, Guinea, Burundi, Kenya, Madagascar, and Ghana. In addition to consulting, he is a certified PECB trainer teaching courses such as ISO/IEC 27001, ISO 22301, ISO 21001, ISO/IEC 27032, Lead Ethical Hacking, and Lead Cloud Security Manager.

My Success Story
Jan Carroll

In May 2021, Ireland suffered its most catastrophic cybersecurity attack to date. Our Health Service Executive, which manages our national health service of 4,000 locations, 54 acute hospitals, and over 70,000 devices, suffered a Conti ransomware attack from the Russia-based Wizard Spider group.

Almost immediately, the IT systems were shut down and internet access was removed. The HSE is the largest employer in the state with over 130,000 staff, all of whom reverted to using pen and paper with no access to patient records. As it was a 'double extortion' attack the attackers had also stolen patient data which they were threatening to release, some of which was published online.

This had a huge impact on patient care as thousands of appointments were canceled. The group demanded €16.5 million in ransom which was not paid but in a surprising turn of events, the gang released the decryption key. The clean-up operation took months and reports of costing up to €500 million, the effects of this attack are still being experienced.

Other opportunistic criminals took advantage of this event and the leaked data, as a pretext for vishing scams. Calling individuals to threaten the release of their medical information and demand money. This attack had an immediate impact on thousands of patients but then rippled to impact other individuals and organizations by forcing them to review their preparedness for such an attack. Suddenly, everyone in the country knew what cybersecurity was.

Ireland is home to the European headquarters of the largest tech companies in the world and has a thriving tech workforce. We are suffering the same cyber skills gap as the rest of the world with nearly half of cyber and infosec roles remaining unfilled. On top of this, many organizations lack a 'security culture' and continue to think that cybersecurity is an IT problem rather than everyone's problem to tackle.

Personally, this attack impacted those close to me by restricting their access to medical services and I received numerous vishing phone calls.

Professionally, I had recently taken on a role as a lecturer to create a Professional Diploma in Cybersecurity with UCD Professional Academy. Due to the attack, the demand for this course was overwhelming as managers scrambled to get guidance on the threats they faced. I am grateful that I can give my students the knowledge and tools for them to improve their organization's security posture by putting the correct incident responses in place so they can reduce the impact and recover quickly from such an attack.

Early Days

I left school in the early 90s but going to college was not an option then. Most young Irish people went straight to work or failing that, emigrated. I took a different path by training to be an electrician, a very unpopular choice for young women at the time and still is. I adored the work and working on building sites and after a few years, I decided to go to college, to study electronic engineering, as a mature student. I have been a lifelong learner ever since.

I love learning and I am constantly taking certifications and training. I still strive for equal opportunities for women in trades and STEM.

After graduating I worked as an IC layout technician and Electronics Technician in a college. At this point, I had just had my third child and we faced a common dilemma for young families with spiraling childcare costs. Our solution was also common, as I decided to take some time out to care for my children.

After a couple of years, I returned to work. I sought a role that would work with my family, and I went into IT teaching. This was an excellent fit and I went on to study for a Master's in Adult Education and took more tech qualifications.

This was a hugely rewarding role as it was 'second-chance' education for adults who missed out on their education when they were young. Many students progressed to work or college, to pursue their dream roles.

Moving into Cybersecurity

One time in a class we were discussing progression and the opportunities available to young people now, when I was asked if I had my time again, what career would I choose? I did not hesitate and chose cybersecurity. It was a lightbulb moment and by the end of the day, I had enrolled in a Master's in Applied Cybersecurity at Technological University Dublin, the same college I had worked in earlier in my career. The program ran for over two years, and I enjoyed every part of it, the pen testing, the secure networks, the programming, all of it.

I learned a huge amount and made fantastic connections. The next year I gave up teaching and started working with small businesses helping them prepare for the impending GDPR. I enjoyed this role and wanted more experience as a practitioner and auditor in the industry, so over the next few years, I got the opportunity to work in some of the top infosec and cybersecurity firms in Ireland. I was very content with my role and did not regret making a career change in my forties. Life was good, then Covid-19 hit.

COVID-19 Hit

When COVID-19 hit, I became part of the 'great resignation' which was when many of us took the opportunity to take stock and reevaluate our life paths and make a change. Ireland was under lockdown which meant working from home, children home-schooling, and parents needing extra support. While it was a temporary situation, I made some permanent changes by resigning from a role I loved, but it was for the right reasons. I missed teaching and I wanted to build something, a company that would close the cyber skills gap by offering training to professionals to upskill or move into information security and cybersecurity. This is how Fortify Institute came to be. The mission of Fortify Institute is to provide quality cybersecurity, information security, and physical security training to professionals. As a woman and someone who moved into cybersecurity in my 40s, I wanted to offer these training opportunities to women and older people too.

If I could offer advice to anyone considering a career change is to look to cybersecurity and information security. There are so many opportunities and many skills we have acquired by that stage of our lives that are transferable. Other skills can be learned via accessible, affordable training. Often our age, experience, and confidence are a great advantage. Get involved in your local cyber community, it is a brilliant and fun way to grow your network and learn. One of my proudest accomplishments in my cyber career was to deliver a talk on cyber learning opportunities at BSides Dublin 2022, which is a wonderfully, community-focused organization.

My Journey with PECB

When I created Fortify Institute, I looked at the certification bodies out there whom I could reach out to, to gain certification, and deliver certification and education as a trainer. PECB has been a fantastic support to me and Fortify Institute. Through PECB I am a Certified ISO/IEC Lead Implementer, and I became a PECB Certified Trainer which has opened so many opportunities for me.

I enjoy being part of the PECB community to write articles, such as 'The Role of the Human Factor: Social Engineering', and contributing to whitepapers, such as 'Ethical Hacking Whitepaper' and 'ISO/IEC 27002:2022 Whitepaper'.

As an SME business owner, this type of industry validation is invaluable and helps me stand out in a crowded marketplace. The PECB community is a fantastic source of support and opportunities. PECB shares my values around inclusivity and reducing barriers to education and training.

Volunteer Work

One of the benefits of working for myself is that I can give my time to causes close to my heart, such as organizations that promote the industry to young women, career changers, returners, and other underrepresented groups. Volunteering is an opportunity to meet like-minded people who share your vision and see value in the experience, not just financial goals.

As a member of the committee of Cyber Women Ireland, we work to increase girls' and women's entry, retention, and return to the cybersecurity industry. Returners are close to my heart as often women have left their successful careers due to overwhelming childcare costs. They make this decision for their families at the time but when their children have grown or their relationships have broken down, they need the support that the dedicated returner program provides to return to work.

As a member of The National Cyber Awareness Task Force, our mission is to create learning resources for frontline workers to support women suffering from tech-facilitated abuse such as cyberstalking. This will take the form of online training for police, health care workers, teachers, etc. ENISA, the European Cyber Agency, do fantastic work in researching cybersecurity trends and I am a member of the ENISA Ad-hoc working group for Cybersecurity Markets. ENISA often seeks security experts to join their working groups and it is a wonderful opportunity to contribute to the community and connect with international experts. I mentor those who enter cybersecurity but do not know where to start. It is tough as many do not yet know where they want to specialize.

So, I encourage them to immerse themselves in cyber.

Do some short free courses, listen to podcasts, read the books, watch YouTube classes, sign up for national alerts but most importantly, get involved with the community, network, and volunteer. The rest will come.

What the Future Holds

When I began writing this piece, I questioned whether I was successful. I am extremely fortunate; I am happy and healthy with wonderfully supportive family and friends. Success is subjective and I consider it from a work-life balance perspective.

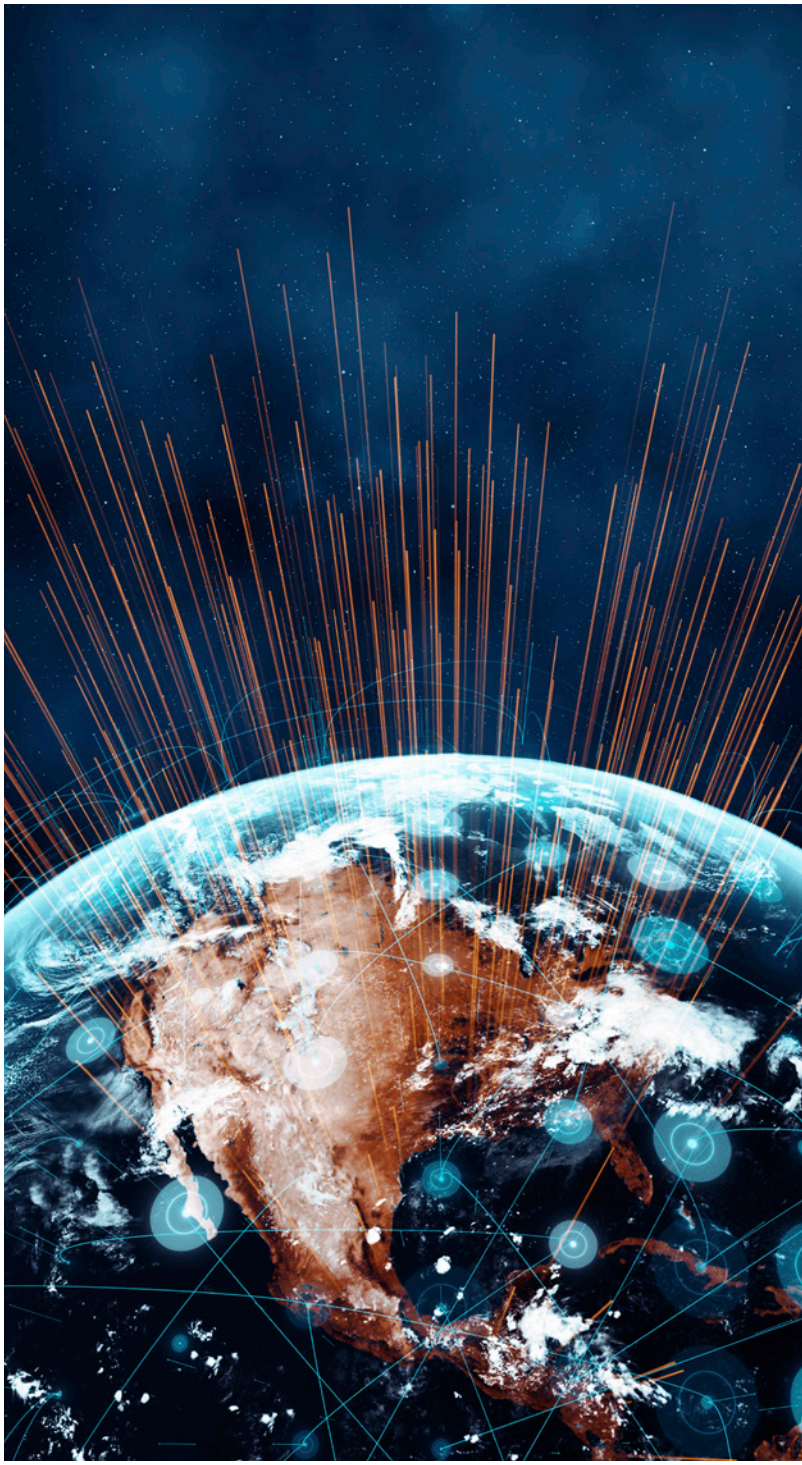
Not an accumulated wealth perspective. I get to do the job I love in a thriving industry so yes; I am successful. I have recently been shortlisted as Cyber Educator of the Year 2022 in the EU Cyber Awards which I am immensely proud of. I see busy years ahead of me as I scale Fortify Institute and partner with other organizations.

I will continue to learn and keep my skills up-to-date. I will continue to be active in the security community and support and mentor those who are entering the industry. If I can aid you with your success, please connect on LinkedIn.

Network Security Architectures for 5G, Cloud, and Disaggregated Telecom Infrastructures

BY SAAD SHEIKH

5G deployments have grown exponentially during the last 24 months, according to industry reports the world will reach **+1 billion** 5G connections in 2022, and **+4.87 billion** connections by 2027, combined with the fact that 6.5GB average consumption per subscriber, with the reach of 15GB in 2022. This is a scale of networks the world has not seen before and the risk of not knowing what we are going to manage is greater than any value that will come from technology advancements.



The biggest concern, doubt, or customer requirement to migrate services fast on these next generation networks largely depends on how the **Security Architecture** will address the following key points:

- Data Control and Security
- User Rights and Privacy
- Network Security

This discussion must be the first starting point for any Future Network architecture plus with early beta type 6G networks expected to be in 2027 era, we are just at a 5 year gap from something, we in the Telecom industry, have not been prepared for.

This is why I have selected this important topic of "Network Security Architectures for 5G, Cloud, and Disaggregated Telecom Infrastructure" to share my view on how we can address these requirements, what we have accomplished, and where there are gaps that need to be addressed promptly.

Why Secure Connectivity is Vital

Telecom systems since the time of inception are trusted and believed to deliver societal value but mostly the trust in security is assumed which raises questions when it comes to 5G Networks which are based on Cloud connectivity models.

Alone in 2021, the Network attacks rose by 31% , this is why Telco's spending on security infrastructure to build future Networks.

It is not only the security of Networks but also data, as per industry progress 73% of Telco's data remains untapped to deliver business value. Therefore, one important aspect of delivering security is enabling the right End-to-End data architecture that enables security as a service solutions across the Networks all the way from Cloud, to Core, to Edge.

5G Security Challenges

There has been a long debate on what should be the right architecture for 5G and future Networks, and already within ITU and 3GPP this domain is well addressed. However, the real challenge of the new technology wave will only come once we deploy it in a distributed fashion at scale.

This is because almost every real-use case of 5G and monetization sits outside the data center or a central colocation. Large scale deployments of 5G means that typical Telco will need to deploy thousands of mini 5G networks for enterprise, each of which will have unique needs. In addition, they cannot afford data aggregation in datacenters, so it must be broken out and processed at the nearest point of value, which mostly will be near to the source at the Edge.

This makes Telecom security discussions more challenging because Edge is where IT&OT really meet the Telco world. It also means that simply Telecom security architecture will not be enough and that to make any real-use case from this complexity there is only one promised deployment model which is based on "Network Disaggregation".

Understanding of this End-to-End story is of critical importance before we devise any architecture or solution.

In an Open and Disaggregated world there are just too many entry points for any security breach. The vital importance of security and how it should be approached was experienced in 2022 by Toyota motors who were forced to halt operations across all of its plants in Japan, following an attack on Kojima Industries, which supplies the auto giant with vital parts.

What it really entails is that merely one view on security is not enough, it also means we need to enable new and agile methodologies in Telecom around security with "intrinsic security" as a base and foundation to design and build any network.

Data Architecture Challenges

During the time the world was shut down due to COVID-19 what kept it still functional behind closed doors was Telecom's critical infrastructure and the systems that made it possible to access the needed services in a secure way.

Therefore, although government support to accelerate new technology rollouts like 5G and Edge was created, what came natively was increased spending on security.

Alone, the global spending on network security has reached $168 billion in 2022 which is over 15% in comparison to the previous year. What is obviously causing this is the horrendous growth of "data" to a level that we can safely say today's business is all about data and an organization's unique capability to manage it in a secure manner.

- Google does it by knowing people search habits
- Facebook does it through social circle
- Uber by navigating world's traffic
- Telco's by monetizing their Pole position

In one way or another Telecom Networks will be designed with more "data Driven Architectures."

Cyber Resilient Networks

The biggest problem I have seen in Telecom Network evolution since the time of NFV is what we call an "Air Gap" problem. What it really means is that we want to keep existing security architectures and tune or reshape it to fit the IT and Cloud world.

Maybe it would have been nice if we started off from the IT world and brought the latest and greatest to meet Telco service needs. This could mean a more pragmatic approach to an operating model as 5G and future networks will scale.

In future networks of 5G, Edge, and Open RAN will be built on cloud native architectures, building secure products will not be enough but rather E2E secure data architectures will be required; “End-to-End Security Architecture based on intrinsic security will be the foundation of Next generation Telecom Networks.”

Such an architecture should be based on the following principles;

1. **Intrinsic Security** – Which will mean security in each layer starting from silicon to supply chain to product retirement
2. **Automation** – Which means real time security insights and security SoC before anything boils up
3. **Intelligence** – As the frontier of data decade where we empower ML and AI on a trusted data to a level where we can make best-informed decisions
4. **Orchestration** – Which means all the unnecessary details are abstracted to give a tenant only what it needs to know

Security Framework for 5G and NextGen Networks

Security requirements and challenges will be wider in 5G than in previous generations, reflecting the far broader range of potential use cases and potential threats.

Further contributing factors will come from the way 5G meets the need for higher speed and lower latency combined with power efficiency needs, a wider variety of actors and device types, and more use of the cloud and virtualization.

5G will be built upon network slicing and the “network of networks” concept. Any security measures must take both this and edge computing requirements into account. Below are the security dimensions in 5G:

Network Challenges

Multi Access
- Massive Multi-Input Multi-Output (MIMO)
- Back, mid, front hauling coverage

Distributed User Plane
- Control/User Plane Separation (CUPS)
- Mobile Edge Computing (MEC)

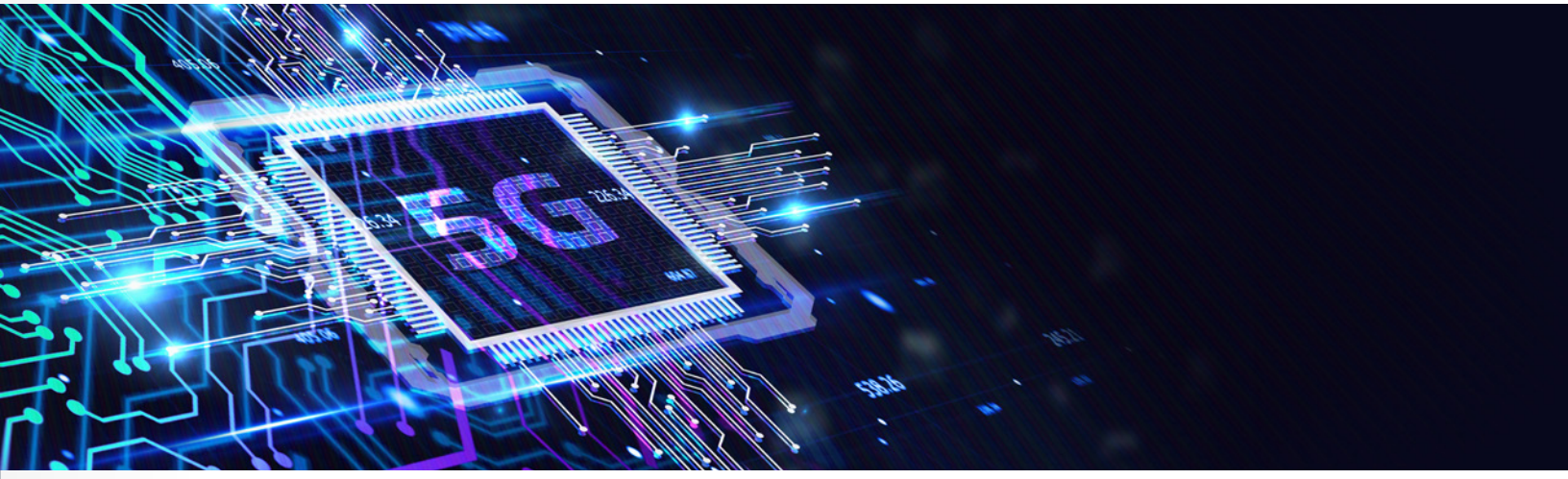
Programmable Network
- NFV/SDN based network slicing
- Automated service function chaining

Security Challenges

Lightweight security
- Sensitive Traffic Encryption
- Connected Nodes Authentication (check)

Security at the edge
- Virtualized and Containerized firewalls
- Cloud SDN Security

Strong Isolation
- Slice Isolation
- Slice Visibility



The main security requirements to secure the upcoming IoT/5G services fall under the following main categories:

- Identity Access Management and Authentication
- Communication Security
- Data Security (Confidentiality, Integrity, Availability)

These security requirements should be distributed over the below security layers:

- **Network Layer Security:** This layer can be split in two parts: network access (part of the control plane) and network application (user plane). Different types of access, i.e. 3GPP (5G, LTE-M, NB-IoT, etc.), or non 3GPP (Wi-Fi, Zigbee, etc.) can be considered.
  Under the umbrella of 3GPP, 5G/IoT will benefit from all the security and privacy mobile features, such as support for user identity confidentiality, entity authentication, confidentiality, signaling protection, and data encryptions.
  Although 3GPP defines several key security methodologies into its specification, CSPs still need to do the provisioning and configuration.
- **Service layer security:** Services can be split into those that are defined by 3GPP, i.e. 3GPP services and services that are provided by service providers or third parties.
  As such, service layer mechanisms are defined within the domain of the service provider and cover aspects, such as service authentication, confidentiality, integrity protection, and privacy.
- **Application layer security:** Service providers implement their services by providing applications to their subscribers. In addition to the security provided by the service layer, each application may implement additional or different security mechanisms. These could cover security mechanisms, such as end-to-end data encryption and integrity protection.
- **Device or Endpoint security:** Certain devices are required to implement security mechanisms in order to make sure only authorized users have access to device resources and in order to make sure that assets, such as the device identifier cannot be manipulated. Those mechanisms are covered within the device security layer. In addition, aspects as provisioning the UE with service or network access subscriptions, device theft, device integrity, and grouping of devices (e.g. for bulk authentication and management) are covered.

The security requirements should be defined per use case, but at the end it follows the CIA triad (Confidentiality, Integrity, Availability), the below are different use cases for connected cars with the required security profile level, as shown below:

Sector	Use case	Segment	Security Profile
Connected car	Vehicle Platform FOTA	Mission-critical	Very High
Connected car	Autonomous driving	Mission-critical	Very High
Connected car	Stolen Vehicle Recovery	Massive IoT	High
Connected car	In-Vehicle Entertainment & Internet Access	Massive IoT	Medium

Cloud Infrastructure Security

With the future networks based on open and standard open infrastructure it is important that security is enabled as a standard foundation in infrastructure that promises and guarantees SLA for the secure infrastructure, the foundation of such a resilient architecture should comprise of following reference architecture blocks:

1. **Safe BIOS:** mitigates the risk of BIOS tampering with integrated firmware attack detection
2. **Safe ID:** protects an IT and cloud infra using biometric security
3. **Cloud Security:** all the way from TPM to HSM
4. **UEFI Secure Boot Customization:** will protect your infrastructure from security vulnerabilities during boot
5. **SafeSupply Chain Tamper-Evident Services:** verify nothing happens to the device during transport. These tamper-evident seals are added to the device and the box at the factory, prior to shipping. Pallet seals can also be added to increase security
6. **SafeSupply Chain Data Sanitization Services:** prevent spyware or illicit agents from being injected into the hard drive
7. **Data control:** using NIST 800-88 standards to ensure even in the case of 5G networks that are hosted on Public Clouds, the customers can manage to keep their data secure and control it
8. **RSA Secure ID and remote attestation:** to cryptographically determine the identity of Baremetal servers
9. **Cyber Recovery for Sheltered Harbor:** is a fast, cost-effective, and efficient mean to protect critical data by adopting the vault mechanism and to recover the data in case of a network security attack
10. **Network Endpoint Security SafeGuard:** will be needed to detect, prevent, and respond to the full spectrum of modern cyber-attacks with the least amount of administrative effort. It applies artificial intelligence (AI) and machine learning (ML) to streaming telemetry data to proactively detect and block network attacks

Multi Cloud Security

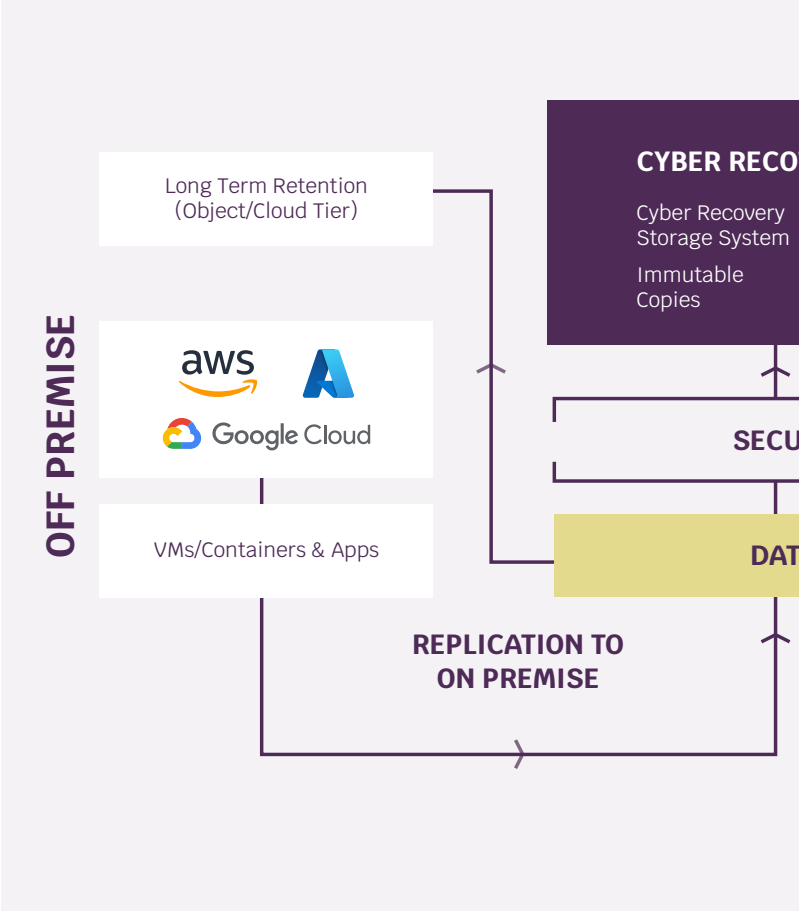
5G and Future Networks will follow different and diverse types of cloud to deliver services ranging from Telco cloud, to IT Cloud, to Public Cloud Providers, in such a case it is important to both reliably define security and also give tenants a real time visibility as it traverses across different clouds.

Based on GSMA FASG and Linux Foundation – Anuket, work and definition in MITRE framework the Multi Cloud Security Architectures should address the following needs:

1. **Policy controls:** where Telco's can declare the intent or policy, and workloads can traverse across clouds while complying to that policy SLA's
2. **Real time visibility:** where a common data model approach to capture events and behaviors across all infrastructures
3. **Security SoC:** where all security related features are monitored to give both the end-to-end view and also enable a timely response
4. **CI/CD of Security Pipelines:** which will focus on end-to-end automation of critical activities focusing on continuous security assessments, compliance monitoring, and security configurations control.

"Finally, the most important piece will be the ***Operational model*** *because there will be workloads that will be distributed across different cloud environments in such a case how we can ensure a consistent single pane of glass."*

Below is one holistic view on how Dell Technologies is supporting customers to deliver secure infrastructure and security solutions, like cyber recovery, to enable true Multi Cloud Era Security Architectures:



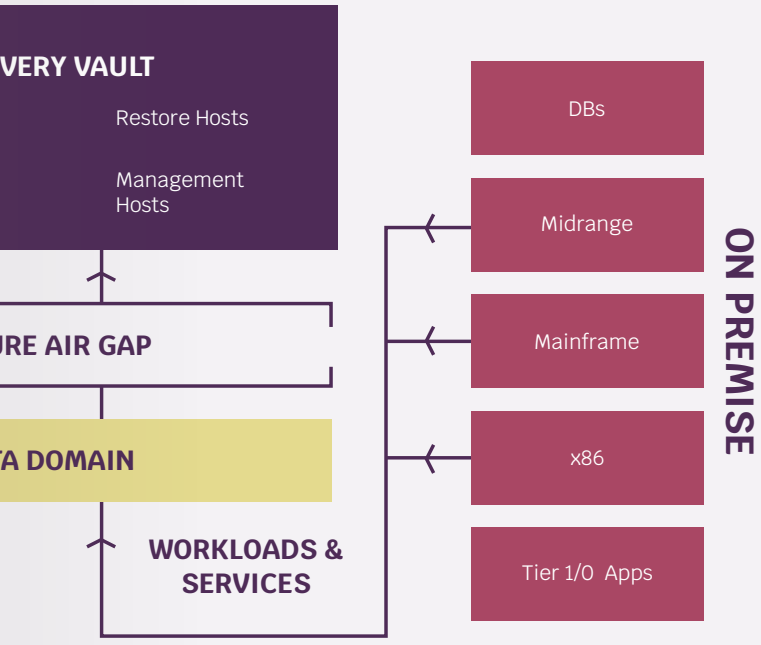
Conclusion

As 5G and future networks are scaling and more services are being migrated, the "**Security**" and "**data control**" become a central discussion.

However, there is no one standard that fully captures the Security requirements that can fulfill the unique requirements of Telecom and vertical industry, it is, therefore, important to build and define a holistic end-to-end architecture based on "**Zero Trust architectures**" using a data driven approach and automation.

This also means that security must be designed intrinsically in every layer and then orchestrated to deliver, as a service, with unique characteristics required by different services and workloads, in a manner that will accommodate accordingly multiple fields and industries.

We, as an industry, still have a lot of work to do, especially by bringing all the Modern Edge and Hyperscaler architectures to the Telco works in a secure and reliable manner, however, it is worth mentioning that we have certainly solved certain issues and have seen and are seeing some early deployments that prove the fact that the Open and Modular infrastructures will be the foundation to deliver a seamless secure connectivity experiences in the new digital world.



Saad Sheikh
Lead Systems Architect APJ – Orchestration and NextGen Ops

Saad Sheikh is APJ Lead Systems Architect for Orchestration and NextGen Ops in Dell Telecom Systems Business (TSB). In this role he is responsible to support partners, NEP's, and customers to simplify and accelerate Networks transformation to Open and Disaggregated Infrastructures and solutions (5G, Edge Computing, Core. and Cloud Platforms) using Dell's products and capabilities that are based on Multi Cloud , Data driven , ML/AI supported, and open ways to build next generation Operational capabilities. In addition, as part of Dell CTO team he represent Dell in Linux Foundation, TMforum, GSMA, ETSI, ONAP, and TIP. He has over 20 years of experience in the industry in Telco's, System Integrators, Consulting business, and with telecom vendors where he has worked on E2E Telecoms systems (RAN, Transport, Core, Networks), Cloud platforms, Automation and Orchestration, and Intelligent Networking.

A dedicated technologist and prolific evangelist with demonstrated commitment to continuous learning and skill advancement. Author and creator of numerous articles, whitepapers, blogs, and informative videos. During his free time he shares experiences to the community through his blog channel https://nfvsdn5g.cloud/

A Day in the Life of a Cybersecurity Expert

BY FRANCIS KURIA

As most involved in the cybersecurity field, my day also consists of a long and tiring schedule, but also as most cybersecurity experts, I love my job and this industry. Working towards a better and more secure digital space is a great motivation each morning. Because of this field I have had the please, and still do, of meeting and working with a great array of cybersecurity experts who have a great deal of experience, however, I still get to meet and work with a great number of aspiring youth with a passion for this industry. As it comes with many challenges, requires a lot of time and effort, studying, staying up-to-date with all new innovations or potential threats, and a great deal of time, for many, an imbalanced work-life schedule, with time away from loved ones and a lot of focus on work. I am sharing with you a day in my life and the balance that I have found.

Getting Started

5:20 AM: It starts this early with the annoying alarm clock emitting a random pattern of beeping sounds. I get tempted to actually chase after the clock in order to shut it off, but fortunately, my wife gets to it before I do, and just like that, the first 'false positive' alert of the day officially checks in. I turn sides and continue sleeping for the next 15 minutes. It happens that the 5:20 AM wake-up alert was for Jeff, the 4-year-old, whose bus driver will be hooting outside the gate at 5:50 AM. After he leaves, it will be my turn out of the same gate at 6:30 AM.

7:45 AM: Thanks to the excellent road network in Nairobi city, I am at the building entrance in the heart of Nairobi City (CBD) staring up at the office on the third floor.

I acknowledge that I am about to undertake my official workout for the day and I cannot help reflecting on my life before the cybersecurity career, where an hour morning run from 5:00 AM to 6:00 AM was the norm. I find my way up panting slightly, but I make it. I also make a mental check and mark the workout task as complete as I proceed to open up my laptop. I grab a cup of tea and start a routine that will take the next four hours.

Getting Work Done

I review and reply to emails ranging from security logs to admin issues and business development. I complete tasks related to the review of the expected receipts, plans for expenses, follow-up on customer leads and I must say that having had a business background early in my career comes in handy, otherwise, I would take the whole day with these tasks.

I will identify and reach out to the established cybersecurity firms and create a business case for them to consider strategically entering into the untapped East African cybersecurity market. On the list of benefits that I will include in the proposal, to such potential firms, is the need to tap into the local affordable talent that this part of the world is currently able to produce.

As an ISO/IEC 27002 Lead Manager, I have to understand and be able to help organizations implement 93 security controls (previously 114), and having first-hand exposure and experience with solution providers that address the required controls allows me to deliver effective solutions to customers on consulting projects. At the same time be a very effective IS auditor, when on an Audit, and Assurance engagement.

I get to review dashboard reports from a Unified Threat Management (UTM) platform for all the managed cybersecurity services customers. I resolve any pending issues or escalate them as required and communicate the event or events to each client as per the agreed Service Level Agreement (SLA). This process is very different for every organization and is dependent on the maturity of each organization's security process.

Working Through Lunch

12:00 PM – It is time to rush for an early lunch and get to work through lunch as I prepare for the cybersecurity training scheduled at 2:00 PM at one of the partner institutions.

Cybersecurity Training

2:00 PM – I get to work with aspiring cybersecurity professionals, help them acquire cybersecurity skills and also get them to pass top cybersecurity leading certifications. I have to be creative with the instructional design as the certification exams are recommended for professionals who already possess some years of experience in cybersecurity job roles. This is not always the case.

Most (about 60%) of those enrolled are recent computer science graduates with one year or less in the cybersecurity space. To close this gap, I ensure that for each student, I provide access to our lab infrastructure that will simulate real-world business environments, processes, and IT infrastructures. I will also ensure that they get access to the latest penetration testing distribution tools and finally ensure I provide them access to the top open-source solutions, which they will use to protect the IT systems that I have provided to them. I will also get them involved in the testing and evaluation of our partner products as well, in any ongoing cybersecurity research. At this point, I am more than ready to call it a day.

The Evening Commute

It is 5:00 o'clock somewhere, and it is finally Nairobi's turn. As the "city in the sun" prepares for sunset, it is time to get home to compare notes of the day with Jeff. For the commute home, I will be using Nairobi's public transport which consists of buses referred to as "matatus", very colorful with most having all the colors of the rainbow in a perfect balance, served with blaring music and branded with posters of legendary American rap artists as well as free Wi-Fi on most of them.

Once inside, my attention is drawn to an IP camera at the front, and just as I thought that cybersecurity work was done for the day, I find myself where we all start, i.e., information gathering phase (Wi-Fi name and password name in plain sight), I find myself asking the question, "What other devices are connected in addition to the IP camera?"

As I am about to jump to the weaponization phase, I make a quick glance around the bus, first at the young man sitting next to me who has been engaged with his phone the entire trip.

His phone seems capable of handling advanced mobile penetration testing tools and I start thinking of what he could be capable of accomplishing.

I, now turn to the other passengers and start asking myself, "Are the hackers here?", "Have they already taken over the IP camera?", I question the thoughts in my head and even start asking myself if a medical doctor happened to be on board, whether he would be sitting around imagining how one of us would look like after multiple fractures from an accident. After that thought, I immediately stop and fortunately it is time to alight from the matatu.

As I alight, I promise myself to focus on good thoughts and leave the challenges of cybersecurity to official working hours.

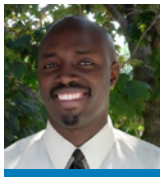
Finally Home

It is now 6:00 PM and I am finally home. I find Jeff in the sitting room and after some warm hugs, he quickly invites me to check his new "invention". It turns out to be a combination of my old gadgets (cables, computer parts, and more related stuff) all precariously connected together using my tool kit set as the base.

I make a good effort to listen to his explanation of how it works, but as I listen all I can picture is his entire invention coming down once I take my tool set kit, another example of a poor security design. He seems to be no different from the software and application developers in the world who ignore the need to implement secure software development practices.

It is now 6:30 PM and the mom is home. It turns out that this is the best time to pull my tool set kit from the invention. I will have a good laugh when I see the invention come down. I also understand that I am about to start the final official workout of the day as I have to run as fast as I can.

I will eventually get caught, just as it happens in the real world where getting hacked is a matter of when not if. And just like that, I will be looking forward to the challenges of the next day.



in

Francis Kuria
Cyber Security Lead | CLEH, CEH, CISA, ISO/IEC 27001 Lead Auditor

Francis is a cybersecurity lead who lives in Nairobi, Kenya, with his wife and 4-year-old son. He holds a Master's Degree in Information Systems from the University of Central Oklahoma (USA). His current industry certifications include: Certified Lead Ethical Hacker (CLEH) from PECB, Certified Ethical Hacker (CEH) from EC Council, Certified Information Systems Auditor (CISA) from ISACA, ISO/IEC 27001 Lead Auditor (PECB), ISO/IEC 27002 Lead Manager (PECB), Network+ Certification (CompTIA), A + Certification (CompTIA) among others. Francis is a PECB Certified Instructor and serves as a mentor, helping individuals navigate their careers in cybersecurity. His dream is for a robust cybersecurity framework for Africa. And when not in the office, you will find him working in his beautiful garden.

PECB INSIGHTS 2022 CONFERENCE

This upcoming PECB Insights Conference is an especially noteworthy event, marking a return to in-person conferences after a three-year period! Designed to ignite and inspire, this event will feature various new and exciting makings, where you will be able to see all the trends, influences, and inspirations of this decade, and where you can connect with C-level professionals.

This conference will host over 40 experts who will be discussing the latest trends and developments in the world of **Information Technology, Security, and Privacy** – with topics surrounding Information Technology, Digital Transformation, Artificial Intelligence, Blockchain Technology, and much more.

Save the date for the PECB Insights Conference 2022 sessions, scheduled for **17-18 November!**

Set to be held in the memorable city of **Brussels**, this event not only includes two full days of interactive and immersive sessions but also features two Pre-Conference Intensive Training Courses.

We are happy to let you know that we are launching the following Training Courses as part of the Conference in Brussels from **November 14-16**:

- → **Digital Transformation Intensive Training Course**
- → **Lead Crisis Manager Intensive Training Course**

These Pre-Conference Intensive Training Courses will be delivered by two highly distinguished trainers with extensive backgrounds in their fields:

- → **Rinske Geerlings**
- → **Graeme Parker**

These sessions and courses will convene the world's most influential and brightest minds across industries. By building bridges between specialists and experts from various industries, we aim to create a community that is inclined to embrace changes and join forces toward a safer world.

Mark your calendars, as we look forward to seeing you all there!

PURCHASE YOUR TICKET ▶

The Use of Blockchain in Cybersecurity

BY RUDY SHOUSHANY

These days cyber-attack trends are increasing in magnitude, frequency, and sophistication constantly. In recent years, we have witnessed escalated cyber-attacks, such as distributed denial of service (DDoS) attacks, phishing, ransomware attacks, man-in-a-middle (MiTM) attacks, SQL injection, and much more, aimed at major networks like Mailchimp, LinkedIn, Canva, Google, Amazon, CNA, WHO, etc. It is safe to say that as technology evolves, so do the bad guys.

The most recent cyber-attacks were launched by nation-states, hacktivist groups, and lone-wolf hackers. Cyber-attacks render a significant threat to government agencies, businesses regardless of size, and all internet users.

Hence, birthing the need for tight cybersecurity to protect online networks from digital attacks on sensitive data, information, and transactions.

In April 2022, email marketing company, Mailchimp revealed that its system was hacked and information was exported from the platform's accounts. This affected users such as Trezor and Bitcoin's wallet, whose newsletter database is hosted on Mailchimp.

In March 2021, insurance firm, CNA experienced a ransomware attack where the company had to pay a settlement fee of $40 million to retrieve their stolen data. The attack also logged employees out of their systems and blocked access to corporate resources.

In October 2020, Google announced the details of a major cyber-attack against its servers in September 2017, to the public. According to the report, the incidence was a distributed denial-of-service (DDoS) attack that lasted for over six months.

Thus, topping the record as the biggest attack of its kind. Undoubtedly, hackers hide behind the decentralized nature of the internet to keep their anonymity and overcome any opposition to their attack.

For instance, a DDoS attack will first, infect multiple nodes across different domains to produce a semi-coordinated network called a “botnet.” Hackers then hijack each bot and launch them against centralized targets.

Meanwhile, other ways to make centralized targets less vulnerable include database management, increased software deployment, security protocols, and depending less on central "trust."

The decentralized solution relies on blockchain technology to increase the resilience of cybersecurity.

Blockchain technology is equipped with multiple features, configurations, and applications specific to improve security. Configurations including public and private cryptographic keys, contracts, and identity control ensure data protection through verification and authentication of transaction records, privacy, and traceability maintenance.

Blockchain technology is trustless and consensus-focused, which distributes transaction records across a network of computers.

Thus, shifting record-keeping and transaction verification processes from a central authority to a decentralized network. Thereby, removing the single point of failure, thus, enhancing resilience to attack and security.

5 Uses of Blockchain in Cybersecurity and Privacy

1. Decentralization of Data

Due to blockchain's consensus nature, data stored on-chain are tamper-proof, blockchain-based storage solutions will help achieve decentralized storage that will secure digital data.

2. IoT Security

Blockchain technology can be used to maintain cybersecurity in the IoT system by apportioning operation and administrative controls away from central authority, enhancing device-to-device encryption, and key management techniques to secure data. Distributing information redirects users when a centralized database is hijacked.

3. Software Authentication

Blockchain is perfect for verifying updates to detect and stop malicious software from sabotaging the devices. Companies can use blockchain hashing to verify patches, updates, and downloads to prevent chain attacks.

4. DDoS Attacks Resistance

The most common and potent cyber-attack is the DDoS attacks, which hit Google and Amazon. Distributed denial of service (DDoS) attacks are launched to hijack the traffic on a targeted network or service by spamming it with false requests from different infected bots. These attacks are decentralized in nature.

However, blockchain's decentralization and immutability solution will be 'beating the hackers on their game' as it efficiently bypasses these attacks.

5. DNS Security

Like a public directory, the Domain Name Server (DNS) connects domain names to their IP addresses. Decentralizing DNS Security can ensure the domain names are tightly secured and beyond reach during a DDoS attack.

The Benefits of Blockchain in Cybersecurity

1. Eradicates single-point failures

Unlike centralized structures, data is decentralized on the blockchain, thus, one node failure can hardly disrupt the system. Therefore, not even DDoS attacks (which are unlikely to happen to a decentralized structure because of insane computational cost) can compromise the system.

2. Transparent and traceable

Blockchain's transactions are trackable due to its accurate record-keeping. Each transaction is verified, recorded, and digitized across the network for transparency.

3. Reliable transfers

Blockchain is ideal for authenticating data transfers. Here, smart contracts play a vital role since they execute instructions (in this case, transfer) once pre-set agreements are met.

4. Efficient storage

Once records are verified and stored on the blocks, they become unchangeable. This blockchain's immutability keeps the data entries safe in a manner never seen before.

5. User confidentiality

Blockchain's built-in cryptographic key features ensure user confidentiality across all networks.

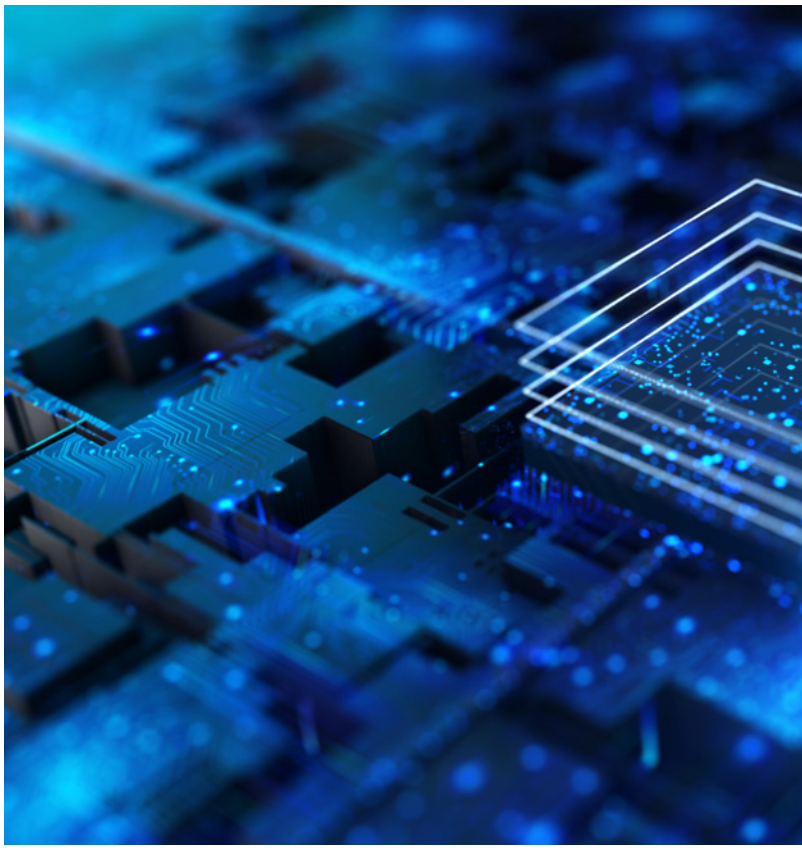
Drawbacks of Blockchain in Cybersecurity

1. No governance

Even though blockchain is bubbling with use cases virtually in all industries, it lacks global regulations.

2. Irrecoverable keys

Keys (private and public) are to blockchain what keys are to cars. These private keys enable device-to-device data encryption. But what happens when a driver loses his car keys? The car becomes inaccessible.



However, in blockchain, once these keys are lost, they are irrecoverable, meaning that encrypted data could be lost forever.

3. Blockchain literacy

Although blockchain technology has been around for over a decade, understanding its concept requires deep knowledge of some tools and programming languages. As a result, few blockchain developers are readily available.

4. Complexity and costs

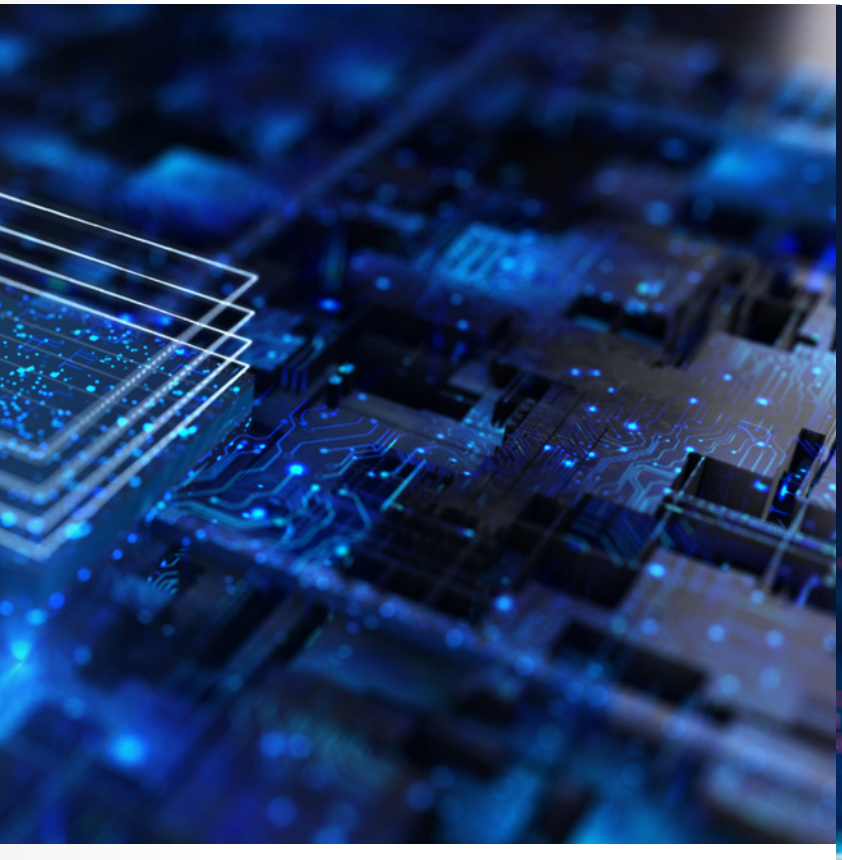
As expected, blockchain technology is very complex and comprises of many nodes and computers actively working. This inadvertently requires high computing power and storage capacities, which in turn causes high transaction fees.

5. Satellite development ecosystem

Though blockchain is secure, more and more security efforts and focus should be put on satellite development around the blockchain, which we are seeing being compromised more and more.

Final Thoughts

Cyberattacks like data breaches, DDoS attacks, phishing, ransomware attacks, etc are cause for alarm especially as the attack keeps evolving with technology, growing in volume and frequency.



The financial impact cost thousands of victims millions of dollars yearly. We are seeing more and more utilization of Blockchain use cases, government agencies and companies must join hands in cyber warfare by looking out for ways to counter or prevent these attacks.

Employing Blockchain's decentralization feature will not only prevent these attacks but pay the bad guys in their coins.

in

Rudy Shoushany
Founder of CryptoTaks
and DxTalks

Rudy has a wide experience in the Information Technology field in the financial sector with over 20 years of experience, which gives him the ability to aid organizations. His specialty is ICT Governance, Compliance, Strategies, and CyberSecurity in the Digital Transformation of fintech.

Rudy is a Certified professional with many achievements and awards, skilled in executive leadership. He has been an active speaker, Board Member, coach, and mentor for startups. He is the Host and Moderator of the DXTalk Series, a Digital Transformation talk show. Which has lately been selected as top 50 Global Thought leaders and Influencers.

IoT Security: Definition, Threats, Issues, Defenses, Tools, and Importance

BY CHRISTOPHER MAGNAN

Definition

Internet-of-Things (IoT) security integrates processes and tools that defend networks from cybersecurity threats. These threats continuously evolve and exploit IoT device's vulnerabilities. Proactive threat analysis and risk mitigation strategies counteract these threats through policies, technology, and people. IoT networks are diverse, so a single strategy or industry standard will not apply to all networks. Device (also called endpoints, nodes, or sensors) manufacturers design are not forced to comply with security standards, old devices with outdated technology are integrated into the IoT network, devices are placed outside a secure perimeter, different communication protocols, and ad-hoc reconfiguration increase IoT security complexity. This article will summarize recent adoption trends, list common security threats, present underlying IoT vulnerabilities, recommend risk mitigation strategies, and present common security tools to strengthen the IoT security posture. Given the breadth of this article, references have been hyperlinked to aid further analysis.

Significance

IoT technology has catalyzed global digital transformation, identified in many reports as the greatest business driver. Corporations harness the technology to improve processes, develop new capabilities, quickly pivot to new markets, or compile data for strategy development. Smart cities, smart homes, telehealth, and industrial automation are applications driving this adoption. Consumers now rely on IoT to improve daily habits, automate home appliances, and for entertainment. Technology adoption has accelerated despite supply chain disruptions, a global semiconductor shortage, and the COVID-19 pandemic. Technology catalysts include decentralized processing capability, cloud computing, cheap hardware, wireless spectrum access, and scalability.

Reports estimate that 12.3 billion IoT devices exist on networks and predict 14.4 billion devices in 2025.

Despite the explosive growth, IoT security has not kept pace with technology adoption. The devices themselves pose many security risks: poor password management, software is not properly updated, and many devices lack security features. Users also do not adopt best security practices since they are not held accountable, nor do they properly understand the risk or how to manage security. Effectively, network security is as strong as its weakest link. Therefore, hackers view IoT as the bridge into the enterprise network. For example, a Las Vegas casino's network was compromised through an unprotected aquarium temperature sensor, this sensor was part of a third-party system design that was not reviewed for cyber readiness and actively managed by the Information Technology (IT) team.

Hackers who are motivated by financial gain, revenge, or politics, can cause significant damage once they access the network. Users can experience injury, death, financial loss, damaged reputation, corrupted data, data theft, data loss, and service disruption. Corporations must protect personal data including credit card info and Personally Identifiable Information (PII). Once compromised, corporations must reach out to their customers and remedy the breach. Recently, hackers have targeted medical IoT during the COVID-19 pandemic to compromise data or disrupt medical devices, such as insulin pumps. Ethical hackers, in an exercise to demonstrate a connected car's vulnerability, were able to access the car's network and remotely control the brakes, the car's acceleration, and door locks.

Threats

In addition to the short-term damages mentioned above, hackers can cause long-term damage once they access the network. The following threats have been repeatedly identified.

Malware is a type of attack that occurs when software is installed on a network device. The malware could take the form of a worm or virus that potentially infects other network components and servers. Malware can be used to deny access to critical components, gather sensitive data, or corrupt system automation. If a hacker can access an IoT endpoint, the malware will be installed on that sensor. Historically, malware was distributed through e-mail attachments that required unsuspecting people to open them.

Botnets are distributed malware used across an endpoint array to disrupt a portion of the network. Botnets are typically used for denial of service (DoS) attacks or transfer enterprise command and control to the hacker. The hacker will install the malware on one node, which then infects other nodes with the malware. Removing this distributed attack will require remediating each infected node.

Ransomware is a type of malware that will lock out system users and administrators until a payment (ransom) is made. Command and control could also be transferred to the hacker and increase the urgency and motivate immediate payment. An example is the compromised vehicle where the hacker will control a compromised vehicle until the payment is sent. The Baltimore City government and Atlanta City governments were affected by this type of attack between 2018 and 2019.

The following two threats are exclusive to sensors and hardware located outside the security perimeter (also identified as defense-in-depth).

Physical theft is the removal of the endpoint or infrastructure from its location. Most likely the network will not be accessed through the stolen node, but service continuity is at risk if it is used to relay data from other endpoints or commands from the enterprise.

Reverse engineering techniques will examine the stolen hardware to replicate the node design. The design can be manufactured and integrated into the network to collect network data or distribute malware across the network.

Issues

Analysts report that IoT adaptation has exceeded growth expectations. However, IoT security has lagged the accelerated technology deployment; many systems are deployed without any cyber readiness or vulnerability assessment. The underlying concern is an exponentially growing vulnerability gap that also has exceeded projections.

Common causes leading to the gap are designs, sensor security limitations, asset management, corporate policies and procedures, and education.

Rapid adoption also requires technical talent capable of managing enterprise assets. However, the necessary talent pool size is also not growing proportionally. As stated by an ISC2 report, analysts estimate a global 2.7 million cybersecurity professional shortage in 2021.

Skills critical to maintaining the security posture include hands-on experience with tools, technical writing, system design, data analysis, and technology lifecycle management. Traditionally, cybersecurity professionals started in information technology (IT) and transitioned into cybersecurity. However, Generation Z and Millennials have completed self-paced or university education to enter the profession but lack technical acumen. Finally, analysts show that cyber professionals are predominantly male (76%) and Caucasian (72%) in the United States and the United Kingdom. These three trends quantify severe limitations with current hiring strategies.

Budgets are also not keeping pace with accelerated IoT adoption. An executive survey reports IoT cybersecurity spending will not increase year over year (YoY). Budgets limit staffing, tool acquisition, training, corporate culture, and risk management capabilities. Recent inflation further limits budget and spending impact. Executives also need to identify critical vulnerabilities that pose the greatest corporate threat and dedicate resources to mitigate risk.

IoT nodes can range from simple sensors that digitize and transmit data to complex command and control systems. Endpoint design standards do not exist and designs range in processing capabilities, local storage, firmware, communication protocols, and memory. Unfortunately, security features are not a design requirement and it is the responsibility of the system designer to implement security controls. Many manufacturers also do not update software nor release patches to mitigate discovered vulnerabilities. Nodes with patches and new software have finite processing power, memory, and storage that limit data collection or processing while upgrading software.

In many IoT systems, IoT nodes are located outside security perimeter and communicate via unregulated wireless channels in the Industrial, Scientific, and Medical (ISM) bands. Wireless transceivers in these bands are commercially available and access barriers do not exist. Hackers actively exploit the vulnerabilities through the wireless channels to penetrate the network.

Consumer IoT adoption is also a developing vulnerability. Employees link their wearables (such as biometric trackers) and virtual assistants to both public, home, and enterprise wireless networks. Consumers are predominantly ignorant about cybersecurity and poorly managed risk. Wearable manufacturers rarely design security features nor update operating software to patch vulnerabilities. Since personal devices are not corporate assets, they rarely adhere to enterprise compliance and risk mitigation standards.

According to ArchonSecure, recently, many older endpoints have been integrated into IoT networks. This practice is common in manufacturing facilities that do want to disrupt optimized industrial processes. These nodes are no longer supported by the manufacturers and operate on antiquated firmware that predate basic security features. In many corporations, the assets are not managed by the enterprise IT team but are managed by industrial engineers or facilities maintenance. Many sensors operate on outdated communication protocols, such as RS-232, that are not compliant with internet based schemas, such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). To effectively communicate with the corporate network, these sensors are connected to aggregators which translate data and commands from multiple sensors between the native protocol and the network. This strategy increases network vulnerability because these sensors do not have an IP address and are isolated from asset and configuration management tools. This isolation compromises asset management since the legacy sensors are often not properly catalogued, managed, and decommissioned when the system is permanently removed from service.

Executives have identified broader IoT asset management as a vulnerability. In addition to the deficiencies mentioned above, new designs and capabilities are not properly reported to the Enterprise IT staff nor the cyber team.

The endpoint vulnerabilities are not properly analyzed and risk mitigation strategies are not developed and implemented. The endpoints' risk profile also increases as critical software updates and security patches do not propagate to the network edge.

In the event the network breach is caused by an unknown sensor, forensic analysis and an incident management remediation plan will be unable to quickly quarantine the affected sensor and mitigate damage.

Corporations adopting IoT typically lack system design expertise and outsource the project to engineering firms. One common mistake is omitting a cyber professional's design assessment of its cyber readiness. Cyber professionals can also advise on asset management, event management, and cyber awareness training. Unfortunately, cyber specialists are in high demand, and adding them to the design team significantly increases project costs. Finally, policies to assess cyber readiness continuously through audits are not implemented to improve the security posture.

Recent surveys have also reported password management is a significant IoT vulnerability. In many sensors, passwords are never implemented nor changed from the default one set by the manufacturer. Because many sensors are not managed by the IT, corporate policies for password complexity and periodic password changes are never enforced. As a result, generic or default passwords are easily deciphered.

Business leaders are also concerned with the lack of cyber awareness and accountability. Trending vulnerabilities are not disseminated to employees. Also, employees' cyber awareness is not audited, and refresher training is rarely presented. Employees also develop risky habits, for example, people who telework may travel overseas and work from unsecured locations with public WiFi. In addition, employees should be held accountable for IT assets issued to them, such as corporate keycards or laptops. Poor management, for example, such as leaving assets unsecured in a public space, is a significant risk, since they can be lost or stolen. Unfortunately, many security concerns remain unreported and violators are not held accountable. This behavior empowers irresponsibility.

With the recent COVID-19 pandemic, business operations have transitioned from offices to homes. Cyber risk has also increased with employees using corporate assets on home networks with unsecured IoT controls and sensors. Since corporate IT does not have the capability to manage employees' home devices, they cannot quarantine, upgrade, or segment them.

The vulnerabilities listed in this article represent trending security concerns. As technology evolves, new threats will emerge. The optimal cybersecurity strategy is to continuously analyze potential threats and apply best practices to mitigate the risk and the potential impact.

Defenses

Countermeasures to mitigate the risks listed above involve processes, people, and tools (e.g. technology). Processes define the expectations and the sequences implemented to improve the security posture. People need to be trained to follow processes and management's expectations. Tools aid people with event detection, enforce policies, and evaluate cyber readiness.

A cyber champion or evangelist is needed in many organizations to improve their security posture. This person should be the face of cybersecurity within the organization. Key messaging disseminated throughout the organization should highlight potential improvements to mitigate security gaps, success metrics, any recent security events, and any lessons learned. From an IoT perspective, the evangelist should focus on implementing a strong cyber awareness that is reflected in the system lifecycle, cyber readiness evaluation, event management, and training programs.

A cyber evangelist's most ambitious goal should be a cyber aware corporate culture throughout the organization, including clerical and hourly staff. In addition to training programs and information sharing, evangelists can recommend rewards for cyber adoption, incorporate cyber practices into performance reviews, identify performance gaps, and recommend improvement plans.

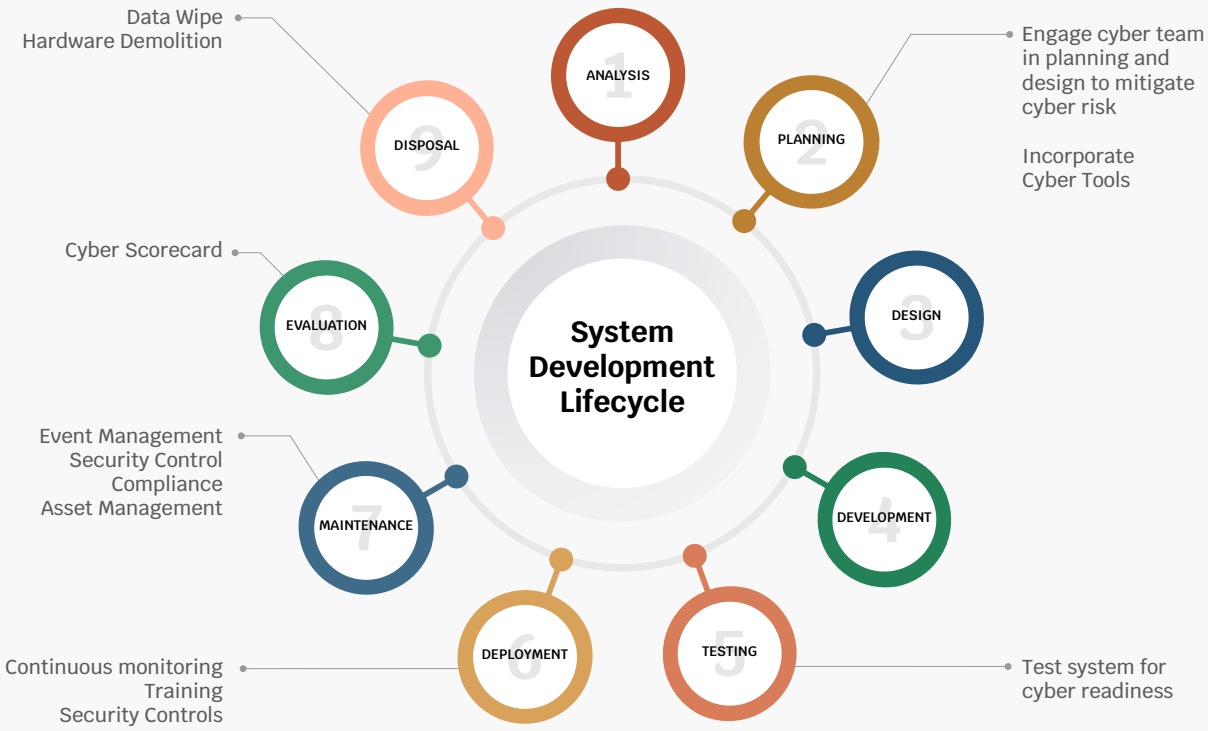


Figure 1: System Development Lifestyle

Businesses typically lack the system design expertise and outsource projects to engineering firms. One common mistake is omitting a cyber readiness design assessment. Implementing cybersecurity best practices into a system lifecycle is shown in Figure 1. A system lifecycle is a standard framework that describes the event sequence from the initial strategy through system obsolescence. Key cybersecurity contributions are highlighted through the system lifecycle. During the design phase, security tools are integrated into the system design.

The tools consist of both hardware and software platforms that strengthen the system's security posture. After the prototype has been implemented and is ready for a pilot phase, cyber tools scan the infrastructure, for both, vulnerabilities and best security practice compliance. These security gaps must be remedied before the system is activated for use.

Event management is a critical gap in cybersecurity. When a data breach or virus infection occurs, key players must react to isolate the affected areas, remedy the vulnerability, collect lessons learned, and recommend strategies to mitigate future risks.

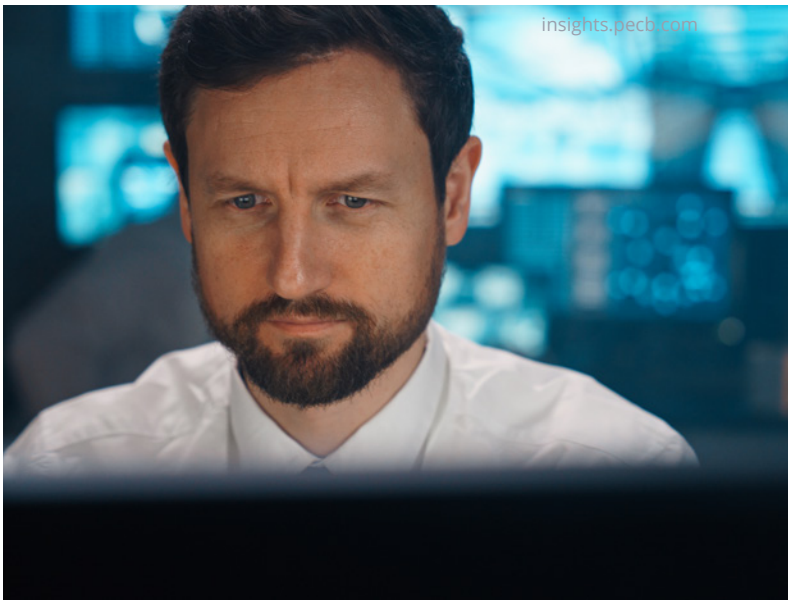
To prepare for events, roles and responsibilities must be clearly defined and processes must be planned and broadcast to the key players. Periodic simulations or rehearsals with key players help refine event sequences, identify dependencies, and address any discovered gaps.

Asset management has been identified as a key defense against cyber risk. IT personnel must track the IoT assets throughout the lifecycle and manage software updates, configuration changes, repairs, and decommission.

If properly managed, the sensors can be properly retired when they are no longer useful. The assets must also have their memory wiped and hardware must be demolished so data is not compromised nor can the hardware be repurposed or re-engineered to enable unauthorized network access.

Virtual Private Networks (VPN) can mitigate the risk incurred by employees' use of personal home networks. VPN's establish a secure and encrypted internet connection between the workstation and the corporate network.

Unfortunately, the VPN's security is as robust as the device accessing it. If an employee is using their personal device on the VPN, then any viruses or malware installed on it can migrate to the corporate network. The best practice with teleworking employees is to distribute laptops with enterprise antivirus software and other security tools.



The partitioning of vulnerable sensors into Virtual Local Area Networks (VLANs) (also known as network segmentation) is important to mention at this point.

VLANs partition the network and will restrict traffic from the vulnerable sensors into the enterprise. VLANs can also quarantine compromised devices from the network itself. Firewalls and firewall rules can be implemented between VLANs to enhance security between different network subnets.

The growth of personal IoT devices used on enterprise networks has increased network vulnerability. The best risk mitigation strategy is to deploy an unsecured wireless network firewalled from the corporate network. A policy mandating these personal assets connect to this network needs to be released and enforced. Tools, such as Network Access Control (NAC) can be used to enforce these policies.

2-Factor Authentication (2FA), also loosely referred to as Multifactor Authentication, enhances Access Management by adding another access variable to strengthen the enterprise network's access portal. The three main types of authentication are:

- "What I possess?" – Examples include a cell phone to receive SMS messaging, an e-mail to receive a temporary password, or a key card
- "What I know?" – Ranges from username and password through security questions that pertain to you
- "Who am I?" – Such as a fingerprint or facial recognition

2FA protects against asset theft or password compromise. In terms of network access via the IoT endpoints, the first two options (What I possess and What I know) are implemented.

Tools

Scanning tools audit both hardware and software. Compliance scanners are software tools that audit the network and notify administrators of devices that do not operate on recommended software versions or have not been properly patched.

Scanning can occur daily, weekly, or monthly. Once non-compliant systems are detected, the administrators must update the software and patches to maintain compliance. Vulnerability scanners are software tools used to detect misconfigurations, nonconformance to cybersecurity best practices, and other risks in network components including IoT nodes. Scans can be configured to recommend mitigation strategies for reported vulnerabilities.

Network access control (NAC) incorporates Access Control Lists (ACLs) to grant entry into the network. Devices not existing in the ACL will either be quarantined or redirected to a VLAN. NAC can also be configured to restrict compromised devices from accessing the network.

NAC also replaces port security, where a specific network port goes to a specific network device. This capability eliminates device replication.

IoT networks are dynamically scalable and use Certificate Authority to manage the public key Infrastructure (PKI) for the network. The CA releases certificates to trusted devices. When a device comes online and starts communicating, it shares its credentials with the enterprise. If the enterprise recognizes its credentials, the device is integrated into the network. If the credentials are not recognized, it is not allowed to join the network. Figure 2 shows this interaction.

Figure 2 (a) and (b), demonstrate a wireless device whose credentials are not recognized and are firewalled from the network. In Figure 2 (c) and (d), the enterprise network recognizes the certificate and allows the device to join the network. PKI can also be used to encrypt the data through key use, further hardening the sensor network.

An Intrusion Detection System (IDS) actively monitors the wireless network access and reports anomalous behavior.

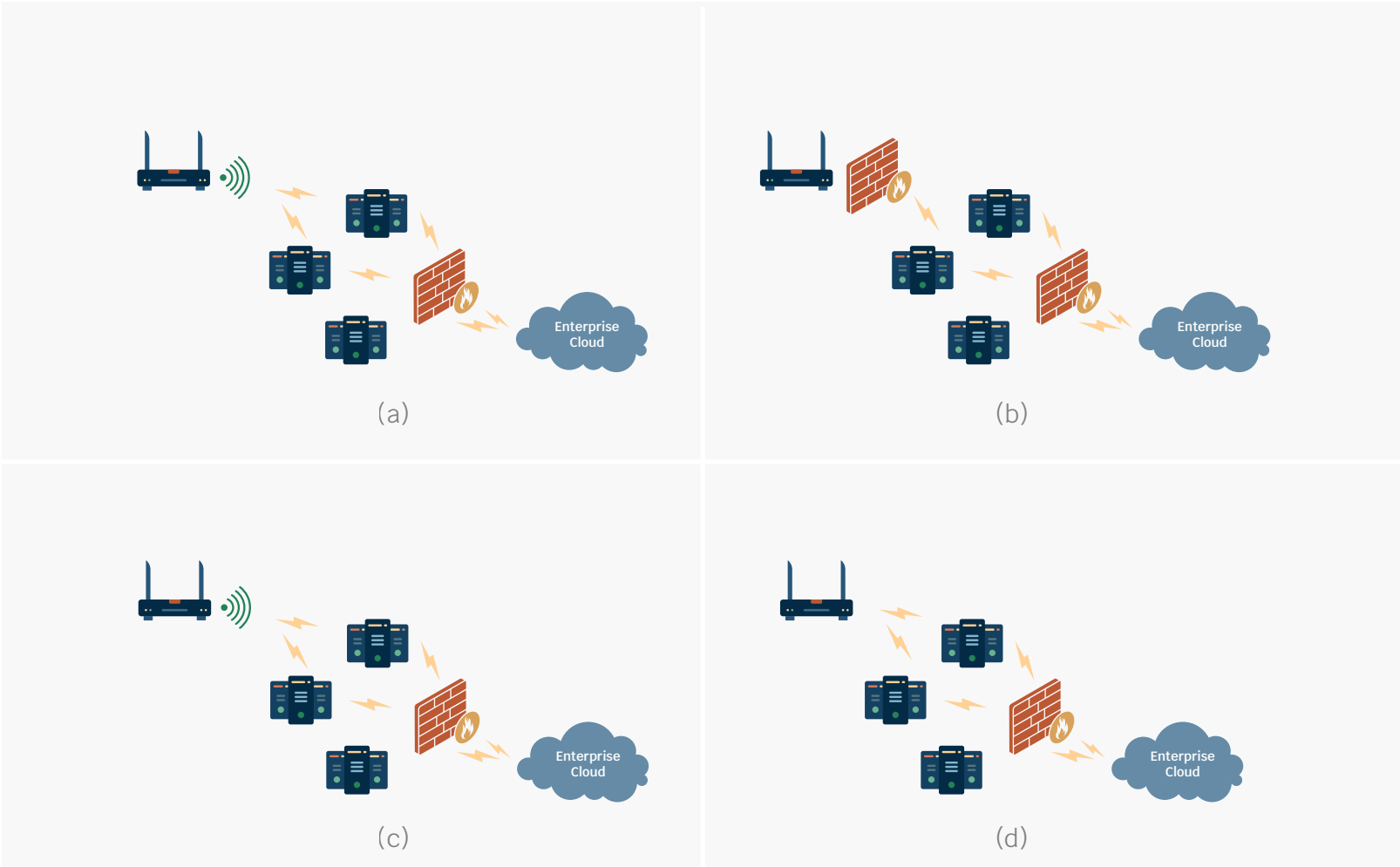


Figure 2: Network Access with PKI Certificate Exchange

Intrusion Detection Systems can also be configured to alert administrators when black-listed devices try to communicate with the network. IDS can also be configured to alert users of anomalous traffic, such as a device repeatedly trying to access one device or cycling through a string of network addresses. IDS is a monitoring tool and is not used to actively manage the network.

Many sensors are placed outside the organization's secure perimeter and are not protected by fencing, access controls, and guards. These endpoints are not protected from theft or damage. To mitigate risk, designers can explore placement in inaccessible locations to limit physical access. Designers can also house the nodes in weather-resistant enclosures with locks. The enclosures can be designed to include an alarm trigger that notifies staff when a node is accessed or damaged. The design tradeoff is cost and accessibility to service the nodes.

Risk matrices can help identify which vulnerabilities are most likely to cause significant damage and drive cybersecurity budgets.

A risk matrix is a high-level analysis tool organizations use to identify key areas that require the most resources.

The matrix compares different risks in terms of the occurrence probability and the potential damage. Figure 3 shows a generic risk template.

		CONSEQUENCE				
		Negligible 1	Minor 2	Moderate 3	Major 4	Catastrophic 5
LIKELIHOOD	5 Almost certain	Moderate 5	High 10	Extreme 15	Extreme 20	Extreme 25
	4 Likely	Moderate 4	High 8	High 12	Extreme 16	Extreme 20
	3 Possible	Low 3	Moderate 6	High 9	High 12	Extreme 15
	2 Unlikely	Low 2	Moderate 4	Moderate 6	High 8	High 10
	1 Rare	Low 1	Low 2	Low 3	Moderate 4	Moderate 5

Figure 3: Risk Template

The cells in the matrix are also color-coded to highlight criticality. Each risk is scored on a scale of 1 to 5 on its occurrence and impact respectively. Red-colored cells identify risks with the greatest probability and impact that require immediate attention while green-colored cells have minimal impact or probability and can be passively monitored.

A generic scorecard is a dashboard used to continuously assess cybersecurity training, policies, and infrastructure. A scorecard should be simple and easy to read, however,

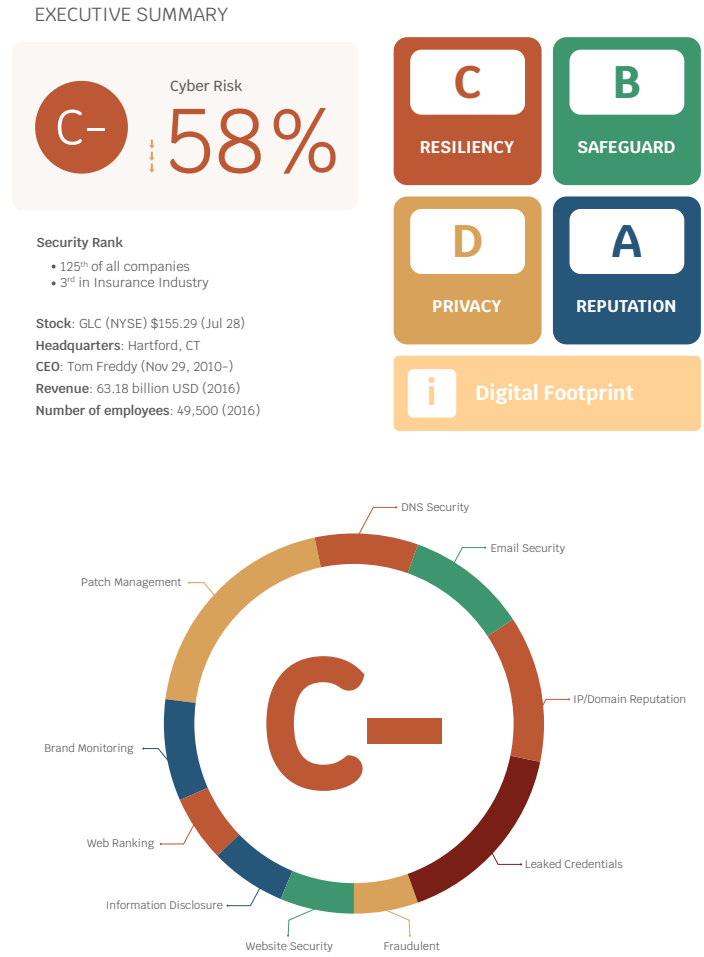


Figure 4: Scorecard Example

The top quadrant is an evaluation of how the company's cyber posture compares to its competitors. This scorecard is just an example, but the key data points are the overall score, the score breakdown to the individual metrics, such as patch management, the score weighting, and the trending score over the past year. Other data points not presented in this scorecard are key security events, such as a data breach or bullets describing deficiencies. A generic scorecard template can be downloaded or a custom scorecard highlighting key metrics can be designed in a spreadsheet tool.

Finally, organizations must complete periodic reevaluation and audits should be implemented to identify developing vulnerabilities. Remediation plans are then evaluated and implemented to mitigate risk. The Deming Cycle (Plan-Do-Check-Act), shown in Figure 5, is a management framework used to assess cyber readiness continuously and implement corrective action. During the Plan stage, multiple strategies are evaluated for cost, complexity, and potential efficacy. The success criteria is also planned during this phase as is the fallback plan in the event the strategy is not successfully implemented.

The best strategy is selected and the implementation team plans the roll-out. The implementation team then integrates the strategy during the Do phase. During the Check phase, the implementation is evaluated against its key success factors, and lessons learned are also discussed. Finally, in the Act phase, the next improvement is selected based on the success and lessons learned. The Deming Cycle is repeated as the iteration is planned, implemented, and evaluated.

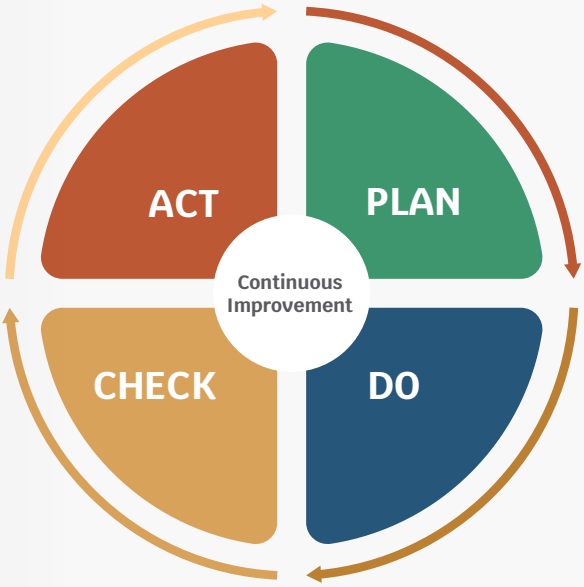


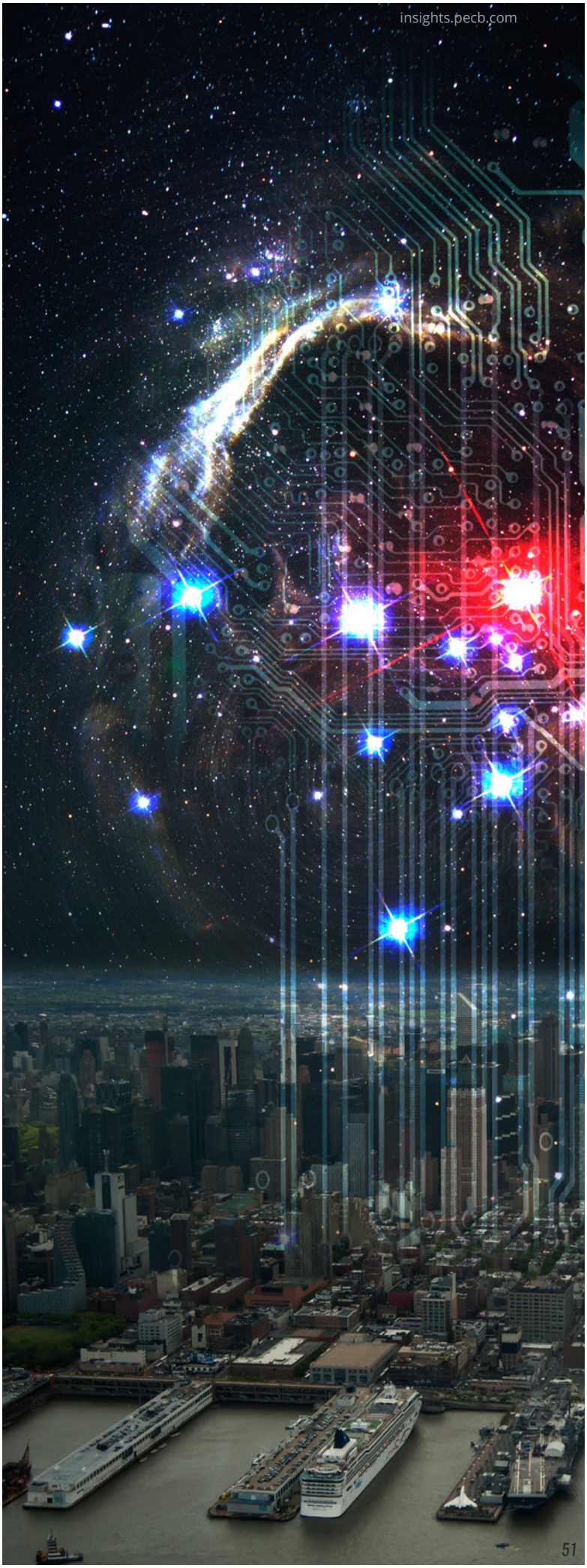
Figure 5: Deming Cycle

Conclusion

IoT technology represents transformational opportunities for many businesses. The benefits include; data mining, new business opportunities, and reduced cost. However, IoT is a growing vulnerability within enterprise networks. Many factors, such as training, oversight, and system design, contribute to this vulnerability. Fortunately, there are many tools and strategies that can mitigate this risk. Organizations must determine what their greatest risk is, develop a strategy to mitigate it, assess the strategy's efficacy, and improve the strategy.

Christopher Magnan
Senior Manager of Network Consolidation | Cloud | Cybersecurity | Unified Capabilities

Christopher manages a telecommunications program supporting the Defense Information Systems Agency (DISA). During his career, he has led a team that has implemented cybersecurity technologies and best practices, integrated telecommunications, and implemented Bring Your Own Device (BYOD) to a diverse global enterprise. Prior to SuprTEK, he managed the design and deployment of Smart City technology across Naval District Washington. He received his MBA and Master's in Electrical Engineering from the University of Maryland – College Park.



BUSINESS & LEISURE

A place to be

SEKONDI-TAKORA
THE TWIN CITY OF GHANA

Sekondi-Takoradi serves as both the capital of the Sekondi-Takoradi Metropolitan Assembly (STMA) and the Western Region of Ghana. The twin city is a coastal city made up of Sekondi and Takoradi. Sekondi is the older of the two cities. These two cities were combined in 1946. Due to the discovery of oil in the western region, the twin city has been nicknamed, the oil city of Ghana.

In Sekondi, you can see old and new buildings on a hilly site that extends to the seashore. Its old port is used by craft boats and fishing vessels, and it is adjacent to a naval station. Several modern buildings and tree-shaded residential areas are present in Takoradi, which is well-planned to accommodate the lifestyle.

Economic Activities

The city is the industrial and commercial hub of the Western Region. Some of the prominent industries in the city include; cement factories, flour mills, harbor, crude oil production, cocoa processing, timber production, and fishing. Also, the majority of government installations can be found here.

The city can be accessed both by road and by air from any part of the country. It is approximately a four hour journey by road and 40 minutes by air from Accra, the capital of Ghana.

The city hosts the Essipong Sports Stadium, which is a multi-purpose stadium with a capacity of 20,000 people. It also hosts the Takoradi Mall, which is the largest modern shopping center in the region.

Places to visit

There are numerous places one can visit in the city. This includes beaches, pubs, nightclubs, and cinemas. Some of the popular beaches in the city include Last Hour Cultural Beach, Africa Beach, Vienna City Beach, and Sports Club Beach.

Tourists and travelers can have first-class accommodation in hotels like Best Western Plus Atlantic Hotel, The Eagles group of Hotels, Raybow International Hotel, Planters Lodge, and Airport Ridge Villa, however, there are many other options for those seeking a more local-like experience.

One of the major places to visit in the city is the Bisa Aberwa Museum. Bisa Aberwa in the local language means “ask old lady”. The museum is located in Nkontompo, a suburb of the city.

The museum contains about 2000 artifacts, sculptures, and photos of African heroes, and other international African heroes across the world.

Some of these artifacts narrate some of the events of the slave trade in Africa.

The Festivals

The name of the twin city cannot be mentioned without the popular annual Takoradi Street Carnival, which attracts lots of tourists. This carnival which is also known as the Ankos Festival is celebrated during every Christmas, from December 24th to 26th, and concludes on January 1st, which is New Year’s day.

Tens of different groups of masqueraders assemble to entertain themselves and the public by showcasing their unique dances, dresses, and brass band music. The best group of masqueraders is given an award by the sponsors, based on the set criteria. This festival attracts thousands of masqueraders and spectators across the country. This is one of the festivals people would not like to miss in Ghana.

It is also worth mentioning the Potomanto Festival, which is celebrated every Christmas in Sekondi. The festival was introduced in Sekondi by Andy Solomon through Ebenezer Kwamena Thompson.

The name Potomanto in Ghanaian parlance is a large suitcase that usually contains valuable items like kente, jewelry, and other expensive clothing. This festival is celebrated in the last week of every year, from December 29th to January 1st of the following year.

The objective of this festival is to showcase the old rich traditional culture of Ghana. During this period, very old-fashioned dresses are worn, and very old vehicles are displayed on different days based on the schedule. There are community sports competitions, including soccer competitions by old prominent Ghanaian footballers. Cooking competitions also take place, in addition to comedy shows by local comedians within the city. Old movies are shown to the participants. Exhibitions of crafts also take place during the period.

Yesu Asor which translates to "Christ has risen" in English, is a carnival that takes place during the Easter celebrations. This used to be a gathering for churches in Sekondi but the youth of Sekondi, led by Nana Eshun, Ebenezer Kwamena Thompson, John Sencherey, Richard Kirk Mensah, and Kingsley Jonsia later revamped it to the current version.

This program takes place on Good Friday, Easter Saturday, and Sunday of each year. On the Good Friday, a replica of Judas is tied and beaten mercilessly. They then move on a procession in town to mourn the death of Jesus. In the subsequent days, popular musicians and upcoming artists are invited to perform their music to the audience. Other activities that take place include modeling, football competitions, and the sale of goods. This carnival usually takes place at Kundum square which is popularly known as Komfoase.

Conclusion

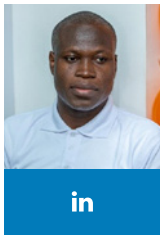
The twin city is a place one can relax and enjoy a very good stay for holidays, training and conferences. To have a fuller experience in the city, you need to visit during the Christmas and Easter holidays. It is a place I will strongly recommend for anyone wanting to have a better feel and view of Ghana.

Partnership with PECB

With PECB being the global lead in ISO Certification trainings, we have been able to tap into its expertise and reputable brand to render quality services to the people of Ghana, through our partnership.

These trainings have been successful due to the timely support and interventions we have received from PECB. The marketing support provided by PECB has been very valuable to our partnership and we encourage PECB to continue the good work. We welcome individuals who want to take any of the PECB ISO Certification trainings in Ghana. This offers these candidates the opportunity to kill two birds with one stone: they can experience the Twin City of Ghana and also earn their PECB certifications in addition.

We, at The-Eye-See-T, are very willing and available to support individuals to successfully attain their preferred PECB certifications in Ghana.



Sherrif Issah
Information Security | Risk and Compliance | Business Continuity | Public Speaker Columnist

Sherrif Issah is an Information Security Governance, Risk and Compliance Professional, and a Data Privacy activist with 15 years of work experience. He is a Cybersecurity Manager at Deloitte Ghana, a Subject Matter Expert for EC-Council, and Director of Communications for the Institute of ICT Professionals Ghana (IIPGH).

He consults for institutions across Africa; on the implementation, maintenance, and auditing of international security standards and frameworks. As a PECB Certified Trainer, he facilitates ISO Lead Implementer, Lead Auditor, and Lead Manager courses for PECB.

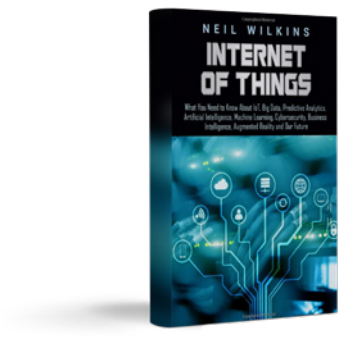
He is a columnist with several articles to his credit and has spoken at local and international conferences on cybersecurity and data privacy. He was a Panelist at the PECB Virtual Insights Conference 2021.

He holds PECB certifications in ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27032, ISO 22301, and ISO 37301, in addition to CCISO and PCIP.

Ensure Your Cyber Safety – Essential Reads

Due to the misuse of data and the rise in cyber-attacks, ethical hacking, network security, and cybersecurity have also been on the rise as many organizations rely on them to stay safe and secure. The need to have your data protected has become very prominent as cyber threats evolve on a worldwide scale, therefore, every organization must take adequate precautions to protect its sensitive data.

Understanding how to create a secure environment for its users against any malicious activity has become most organization's highest priority. Exploiting your organizations vulnerabilities through a process of evaluating a system for potential security breaches or data threats, in order to fix any vulnerabilities prior to cyber-attacks is highly important. Get a better understanding on staying protected through the books listed below:



Internet of Things: What You Need to Know About IoT, Big Data, Predictive Analytics, Artificial Intelligence, Machine Learning, Cybersecurity, Business Intelligence, Augmented Reality and Our Future by Neil Wilkins

With an excellent coverage on IoT and a thorough explanation, this book also covers topics such as; ethical hacking, predictive analytics, machine learning, artificial intelligence, cybersecurity, big data, business intelligence, augmented reality, virtual reality, and much more. With the growth of internets usage this book presents an understanding of where our future is going and how to be prepared for it. It covers concepts and methods powering the most aspiring technological concepts of our century, the Internet of Things (IoT), meanwhile elaborating on gadgets and tools to use to stay better prepared for the future of the internet. A well-written and knowledge-based reference book for anyone who is interested in deepening their knowledge on IoT and relevant technologies.

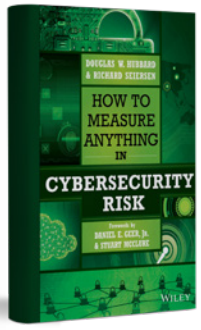
Cybersecurity – Attack and Defense Strategies 2nd Edition by Yuri Diogenes and Erdal Ozkaya

This book delves into recent trends in threats and cyber defense, with great information included on various recent or growing technologies such as; Zero Trust, Cloud Security, Cyber Kill Chain, identifying types of cyber-attacks, and much more. It offers an understanding of how cyber-criminals gain access to organizations and provides a framework of how organizations could protect themselves with cybersecurity defense strategies that are well laid out and easy to follow. A highly informative book for a wide range of audiences, from those who are new to cybersecurity to experts who want to self-review. For those new to the security field, this book provides an understanding that is required to define strategies, implement procedures, and refine the tools at your disposal to impact the security posture of your organization, whereas, for senior executives, a high-level holistic view of what the current threat landscape looks like is provided. With no shortage of case studies of real-world occurrences, cybersecurity specialists can use this book as a manual to improve their organization's security posture through the methods explained.

Advanced Penetration Testing: Hacking the World's Most Secure Networks by Wil Allsopp

Nowadays threats are organized, professionally run, and for-profit. All types of organizations and institutions, from financial institutions, health care organizations, law enforcement, government agencies, to other high-value targets, need to reinforce their IT infrastructure and human resources against advanced targeted attacks from motivated professionals. This book incorporates social engineering, programming, and vulnerability activities into a multidisciplinary method for targeting and compromising high-security environments. The author portrays highly advanced topics and in-depth understanding of penetration testing through each chapter about sample hacking scenarios, with each chapter exploring different hacking methods in various environments with real-world examples of hacking networks. Commonly penetration testing involves low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans. The hackers' professionality of today's threats operate at a much more complex level and this book shows you ways to defend your high-security network.

How to Measure Anything in Cybersecurity Risk by Douglas W. Hubbard and Richard Seiersen



In this book, Hubbard lays out the foundation for decision-making and strategy within cybersecurity through a solid approach to quantitative risk analysis. Using examples and common tools, he shows how to apply probability concepts easily to solve questions that many businesses face today regarding cybersecurity. By presenting a clear framework for non-mathematicians to become statistically literate, this book debunks common misconceptions and allows readers to move beyond qualitative "spotlight charts" into quantifiable probabilities. Presenting a whole new approach to measurement, the author opened the business world's eyes to the critical need for a better measurement system, besides the common; Low, Medium, and High measurements used in cybersecurity. An insightful read, How to Measure Anything in Cybersecurity Risk motivates organizations to do a closer examination of its own risk management practices in the context of cybersecurity. The aim is to airtight data protection and ensure your organization's safety, prior to any malicious attacks.

The Updated Version of ISO/IEC 27002 is Available!

The ISO/IEC 27002 training course provides guidelines for implementing, managing, and improving information security management in an organization.

Find the training course that suits you best:

- → ISO/IEC 27002 Introduction
- → ISO/IEC 27002 Foundation
- → ISO/IEC 27002 Manager
- → ISO/IEC 27002 Lead Manager

FIND OUT MORE ▶

The Impact of AI on Cybersecurity

BY JOHN A. ADELOYE

Cyber-attacks are a key concern for every organization today. As the development of more new technology to make lives better increases, the chance of being a victim of a cyber-attack is also on the rise as every system supposedly has a vulnerability that attackers can exploit to compromise the system for the purpose of stealing information, demanding ransom, and to misinform the public. With the increase in cyber threats that each organization now has to deal with on daily basis, ranging from phishing, distributed denial of service, rootkits, man-in-the-middle, and a few others more. There is now an urgent need for assistants who can help the security analysts more proficiently and faster, and this led to the involvement of artificial intelligence in cybersecurity that can analyze data faster than humans could do and give better predictions in the very shortest time possible.

IN THE AGE OF AI

Now in this age of artificial intelligence, where automation has now become the essence of the fourth industrial revolution, ranging from web search technology, human speech analogy, self-driving cars, and a few others. There is now a higher risk of the system being compromised. As more systems are now automated, thanks to AI; now there is also a greater need for its protection to be automated as well. Many pieces of research have shown that 2021 recorded the most cybersecurity attacks, and this number is intensively expected to increase by the end of 2022 with the majority global workforce grinding away from the secure confines of a cooperative network as recorded by Fortinet.

In this age of AI, attacks are becoming faster in their deployment, and they quickly get to the target because of the way their program is written. About 10 years ago, we have a lesser number of programmers and cyber intruders compared to the large numbers circulating in different countries of the universe today.

While many are leaning towards learning, those on the part are becoming more advanced with new discoveries of tools, libraries, and machines.

Back then, one can use any of the varieties of an antivirus to repel attacks, but now, the attackers are also following trends by becoming smarter in their deployment and using updated tools. With the help of an AI-based security system, an attack can now be detected and repelled before it even gets to the system, and the data collected from the attacks will also be useful in training the AI if it is a supervised or a semi-supervised learning model.

HOW AI MADE CYBERSECURITY RELIABLE

With the involvement of AI, the sustainability of cybersecurity is continuously greatly improving. It has also increased system reliability and dependability by helping the system to behave as expected even when it processes a false input (at least periodically).

On the other hand, AI helped in system response advancement - most of the works done previously have relied on applications, and sometimes they take a long time to load or encounter loading failure due to low memory or other possible reasons.

But in this era of AI, most of the work is now done at a click of a button (thanks to machine learning algorithms running either on the machine or in the cloud, and its operation consumes lower memory and performs more functions at a shorter time frame). This machine learning model understands the system that sends the request and what an expected output is supposed to look like due to its ability to read and understand the system's data (for an unsupervised learning model) in other to process its response.

Other numerous impacts of artificial intelligence have now offered a strategic advantage to cybersecurity through its ability to reduce its vulnerability to cyber-attacks, and some of the cyber-attacks are:

Zero-day Attack – is an exploit through a vulnerability of an application or a system before such vulnerability would be detected and patched. It is almost impossible to create a system or an application without at least a vulnerability or potential vulnerabilities, which technologically means all systems are prone to or potentially prone to this particular threat.

With the help of artificial intelligence, detection of anomalies in data and sharing of data results can now be quickly disseminated to the security analysts when the system detects zero-day threats, even though it may not be able to stop them, but the result will provide security analysts with something to start with, rather than having to do the groundwork themselves which could take a sizable amount of time, and therefore, unnecessarily delay the quest to defend the system from being compromised. Some AI systems even went as far as analyzing the data gathered by themselves and providing the IT engineers with insights on the attack surface and suggestions that can be useful in the process of defending against this attack. Therefore, using Artificial Intelligence reduces the Mean-Time-To-Respond (MTTR).

Ransomware Attack – is a type of malware deployed by attackers to block owners or authorized personnel from accessing the system, or maybe encrypting the system data with the hope to demand a ransom before a pass key to decrypt the system would be given. In this attack, the network has to be compromised first, while the attacker finds its way to the domain controller to deploy the ransomware which blocks access to a server until a ransom is paid. However, there could be more steps to this if it is a multi-staged attack.

While most ransomware attack happens on a work-free day, this is done to delay the responsiveness of the IT engineer due to fewer cybersecurity engineers on duty.

This can happen and has unfortunately happened numerous times to some organizations. Maximilian Heinemeyer, VP of Cyber Innovation at Darktrace says, “It’s one thing to detect an attack that has not been seen before, it’s another thing to stop its ransomware” – While it is easy to detect an attack, stopping its encryption is far opposite due to the limited time. The involvement of AI in such an attack can help to detect the attack at an earlier stage and repel it before it gets to the domain controller. Since some ransomware starts with file encryption, AI can also help stop the intrusion before it gets to the encryption process.

These are a few attacks among many that a system can be exposed to, one of the others remaining is phishing mail, which comes with an intention of gaining access to steal information which may be login credentials and other types of data. Artificial Intelligence can help by detecting this type of mail earlier and killing its command control that will navigate the victim away from the original page and can even go as far as killing the attacker's network connection depending on how the AI algorithm program is written.

DRAWBACKS OF AI ON CYBERSECURITY

While it is true that AI is a smarter machine that can process, evaluate, and predict faster than human intelligence, it requires constant updates and enhancement to meet up with the current trends of attacks, and most times when this is not done on time, the system can become more vulnerable due to the AI model limitations to associate with its usability. AI is not human; it is a machine trained by a developer (supervised) or allowed to train itself with available data (unsupervised) to recognize some particular patterns or do certain tasks based on conditions. Due to this, AI can raise false alarms when it discovers discrepancies that are irrelevant as low as web traffic or network instability, this may lead to the organization making unnecessary moves to curtail a supposed attack that never happened and that can even sometimes make the system more vulnerable during the process of stopping or discovering what never happened.

Another great setback in fully relying on artificial intelligence is that it reduces the alertness of the security experts in that organization as it creates an impression that AI will always do the most jobs and when the AI itself is compromised, they find it more difficult to defend the threat, and that buys time for the attackers to fully operate and succeed in their quest. If the attacker is skillful enough, he can even manipulate the AI remotely by just feeding it with the wrong dataset causing the AI to misbehave due to data bridges.

When talking about the human relationship with the AI in repelling an attack, it should be limited to humans monitoring the AI activities, and they must be smart enough to know when the AI is about to misbehave. Trusting the AI to do the whole job comes with lots of consequences, and partially allowing the AI to do part of the job (sharing the responsibilities with humans) makes the system that implements the AI even more porous, and that cancels out the benefits of the AI involvement.

The previous initiation of cyber threats is targeted mostly at stealing information, either for personal usage, demanding ransom, or for fun. But the new form of recent attack

from attackers now involves AI, and that has provided the attacker with more influence to attempt to gain full or partial control of the target systems remotely and went as far as changing its behavior if necessary or desiring.

Most importantly, relying fully on AI can sometimes lead to human destruction. Professor Mariarosaria Taddeo of the Oxford Internet Institute declares, “By adding 8% of erroneous data to an AI system for drug dosage, attackers could cause up to 75.06% change of the dosages for half of the patient relying on the system for treatment”. She further discussed that similar results can be achieved by manipulating the categorization models of a neural network. Once an AI system is launched, attacks on the AI itself are difficult to detect due to its lack of transparency because of the dynamic and adaptive nature of an AI system which makes it almost impossible to explain the system's internal processes.

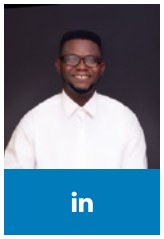
CONCLUDING OVERVIEW

Cyber infrastructures are now more exposed to diverse interruptions and warnings that may be due to the processing of complex information.

Hardware devices are no more adequate to guarantee the security of these infrastructures. Due to the buildup of the internet, attackers now have access to the tools and expertise that are needed to deploy an attack right at the convention of their homes.

We must fully agree that AI has helped advance the field of security and provide some sophisticated ways of analyzing, evaluating, predicting, and repelling an attack, and due to this providence, old hardware conventional cybersecurity measures are not adequate anymore in fighting the ever-increasing cyber threats.

The existing cybersecurity methods are now becoming obsolete due to ineffectiveness. The old common method of cybersecurity through firewalls now has limitations in the security process. Therefore, there is now a heavy demand for efficient security measures to defend against these newly modern clustered attacks as cyber interventions that are carried out by intelligent agents are not sufficient to meet the pace of these cyber threats, but also we should not quickly forget the challenges that lie in fully relying on the AI to do all tasks that IT engineers are expected to take care of.



John A. Adeloye
Python Developer | Web Developer | Data Analyst | Data Entry Specialist | CyberSecurity Personnel | Technology Write

John graduated at Brigham Young University-Idaho, Rexburg; Idaho. He currently works as a research Assistant at Strategic Alpha Investment Advisors Inc., Irvine; California. John is a solution-driven programming analyst with measurable experience in Data Analysis using Python Programming and Excel, Microsoft Power VI, and Tableau. Well-versed in all phases of Information Technology, and with a strong working knowledge of algorithms. Proven success in engineering customized solutions, data entry, computer networking, computer hardware and software, health and safety, and improving business processes, operations, and profitability. You can reach him at ade21007@byui.edu.

Certified Lead Ethical Hacker

PECB offers the Certified Lead Ethical Hacker (CLEH) training course in both, English and French, enriching our library of content, quality, and high-liability. With the increase of cyber-attacks,the global need for ethical hacking is increasing as well.

Benefits of getting certified in Lead Ethical Hacking:

- Mastering methods and techniques
- Learning about different attacks that affect an organizations security
- Obtaining necessary expertise to conduct a penetration test
- Gaining the ability to analyze the results of penetration tests
- Increasing your chances of getting hired in the security career
- Acquiring the ability to support organizations' security

For additional information, please contact us at: marketing@pecb.com

Become a CMMC Certified Professional

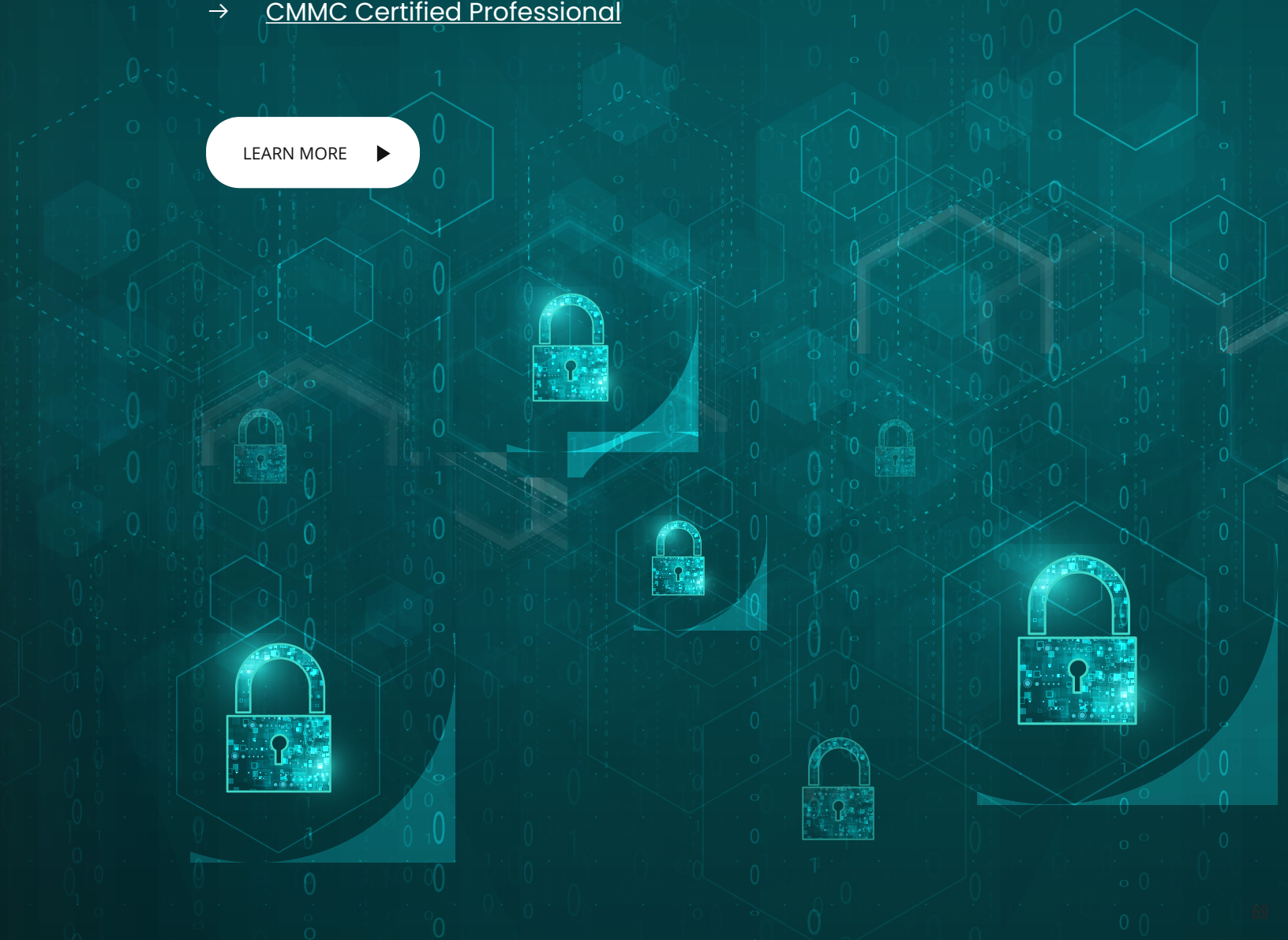
CMMC framework is a verification mechanism designed to measure an organization's maturity level regarding the protection of unclassified information.

This course is ideal for those interested in learning about the principles of CMMC, its core concepts, as well as how to manage and implement it effectively.

Get started now with PECB's CMMC Training Course:

→ CMMC Certified Professional

LEARN MORE ▶

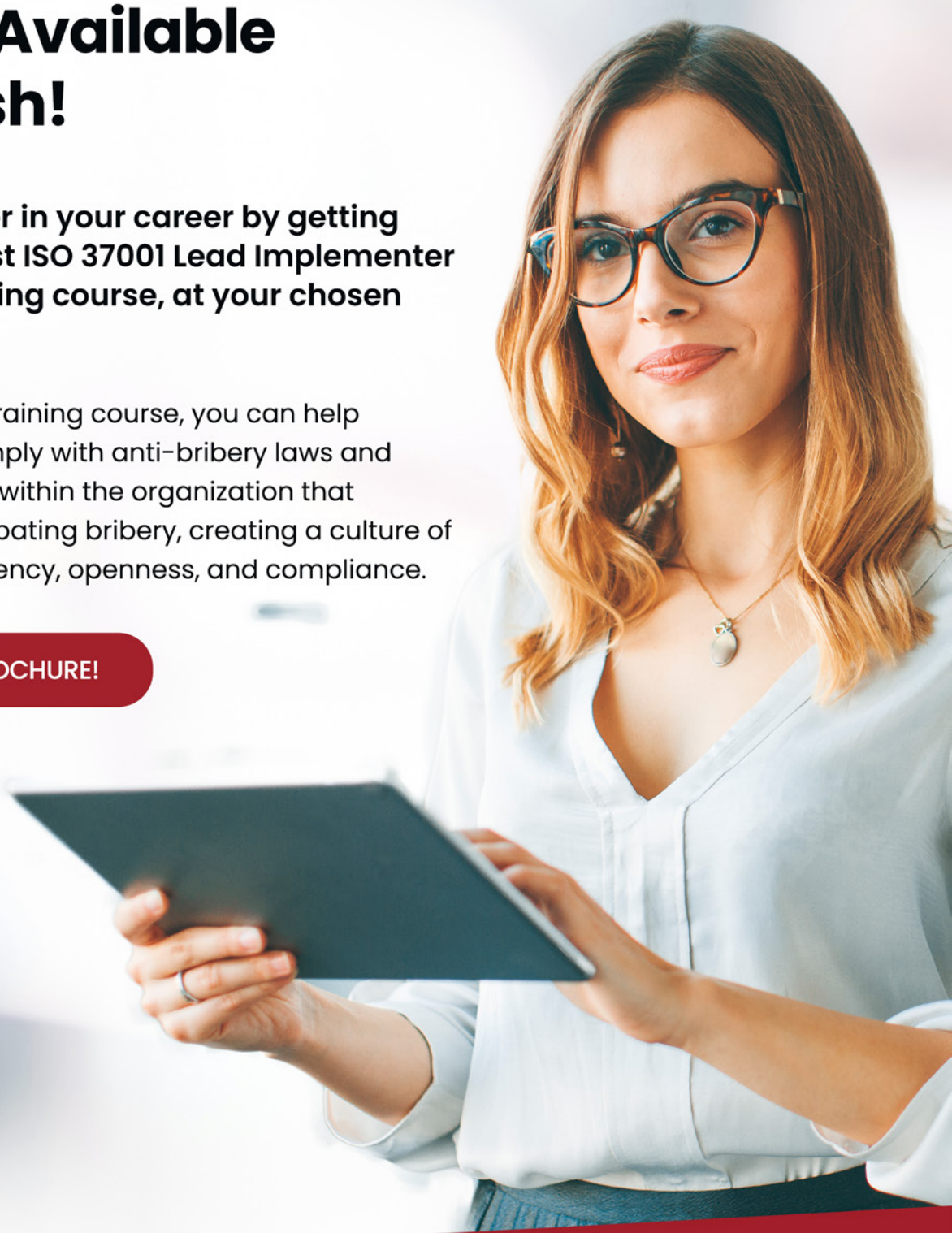


ISO 37001 Lead Implementer eLearning Training Course Available in English!

Advance further in your career by getting certified against ISO 37001 Lead Implementer eLearning training course, at your chosen environment.

By attending the training course, you can help organizations comply with anti-bribery laws and establish controls within the organization that contribute in combating bribery, creating a culture of integrity, transparency, openness, and compliance.

CHECK THE BROCHURE!



WEBINAR LIVE

BE ON THE LOOKOUT FOR AUGUST'S WEBINAR

The importance of a secure online presence is becoming more and more evident. Avoiding any type of breach, be that organizational or individual, is gradually becoming a priority to most. Understanding the relation, importance, and effect of ISO/IEC 27001, cybersecurity, and risk management will help your quest for digital safety.

Learn more on how to keep your stay safe, in our upcoming webinar in August.

TOPIC: ISO/IEC 27001, Cybersecurity, and Risk Management: How to avoid data breaches?

August 17, 2022 at 3:00 – 4:00 PM CEST

SIMON LACEY
Principal Information Security Consultant

→ REGISTER HERE

Top Five High-Paying Job Positions You Can Pursue with an ISO/IEC 27032 Cybersecurity Certification

Organizations today are facing fascinating, yet distressing advancements of technology. The evolution of technology and its wide application has come with many limitations, challenges, and countless sophisticated risks. The frequency of cyber-attacks has grown exponentially during the last few years and hearing news of big data breaches is becoming very common. In order to protect and secure their cyberspace, organizations must take preventive and safety measures. Cybersecurity is considered to be in the top five ranked risks of 2022.

According to Cybersecurity Ventures, cybercrime costs are expected to grow tremendously in a few years, reaching $10.5 trillion USD annually by 2025. Besides cybercriminals and cyber-attacks themselves, a top threat of cybersecurity is considered to be the negligence of employees who do not follow security guidelines or are not familiar with cybersecurity and its importance. ISO/IEC 27032 provides security techniques and guidelines for cybersecurity.

Considering the high need for cybersecurity experts, ISO/IEC 27032 Cyber Security Trainings would be a great solution and asset for any professional who wants to pursue a successful career in the field of cybersecurity.

ISO/IEC 27032 Cybersecurity Management Certification enables you to protect an organization from cyber threats, strengthen your knowledge and skills, and demonstrates your competencies in cybersecurity.

Note: The salaries presented below are according to information from PayScale, Glassdoor, and ZipRecruiter.

1. Chief Information Security Officer (CISO)

The average U.S. annual salary of a CISO is **$166,150**.

2. Security Architect

The average U.S. annual salary for an Information Security Architect is **$142,123**.

3. Cybersecurity Manager

The average salary of a cybersecurity manager is **$129,817**.

4. Cybersecurity Engineer

The average salary of a cybersecurity engineer is **$106,911**.

5. Penetration Tester

The average salary of a penetration tester is **$95,981**.

The PECB ISO/IEC 27032 Cyber Security training courses equip participants with the necessary skills and competencies in protecting privacy and data from phishing scams, cyber-attacks, hacking, data breaches, and other cyber threats. ISO/IEC 27032 certification is also a competitive advantage that raises the chance of certification holders to get employed.

Note: The salaries of the above-mentioned positions are not definitive and they may change with time and industry development.

CHECK OUT THE BROCHURE! ▶

Network Security and Management A Deeper Understanding

BY PABLO BARRERA

To talk about network security and management, we need to split this subject into smaller bits of information, concepts, and a bit of history. First, let us go back to the concept of security and where it comes from. Security is described as the state of being free from danger or threats. Discussing a network free of dangers or threats is something utopic and unrealistic, which is why when we talk about network security we should focus on reducing or controlling threats to an acceptable level to the organization and its processes.

Many of the concepts applied to cybersecurity, network security, information security, and related fields are concepts already used in military practice. A few decades ago, we were talking about Demilitarized Zones in the network to expose our services to the internet; defense-in-depth, and many other concepts that are part of the military vocabulary, which is why some of the concepts still apply.

We can build the concept of network security as the strategies, policies, processes, and technologies used to secure an organization's data, applications, devices, systems, and resources connected to the organization's network. It is important to understand that network security is a part of cybersecurity. In the past, we used to see organizations as castles or fortresses and the data as the gold inside the chest located in the safest room in the castle.

How important can Network Security be for an organization?

Nowadays, we need to see our organizations as ships, ships that travel in a vast ocean of interconnected organizations, and that sometimes the information travels from one ship to another by small boats that leave the ship with precious cargo. Those little boats represent the fact that now we have adopted other ways of working with colleagues, other ways of communication, and other technologies in our daily lives.

The precious cargo we mention is data, sometimes sensitive and critical. And as we know from the basic cybersecurity awareness courses, humans are the weakest link in the chain. Networks are now extended to places outside the physical constraints of an office or a corporate network, they have extended to public Wi-Fi at coffee shops, our desktop or dining table while doing home office, and even sometimes the bench on a sandy beach while nomad working.

The way we use devices now, statistics are incredible, they show that mobile devices represent about 68% of the total traffic on different websites globally, and desktops are becoming a thing of the past.

We are changing the way we access our information and how we share it. These new ways of being interconnected to networks and how we work, consume, and share information provides a solid base to create new conversations, that we as security practitioners, need to address and respond to according to our organizational priorities.

We need to ask ourselves what new risks we face and if we are ready to provide our organization and users with the right strategies, policies, processes, and technologies to secure information and assets. Therefore, Network Security is still a growing and exciting field, with new strategies to be developed, and new technologies to be invented.

One of the biggest insurance companies in the world categorizes cybersecurity incidents as the number one risk organizations of any size, location, and sector face. Insurance companies are aware of the risks.

This talks directly into management, cybersecurity is no longer an IT thing, it is a transversal function and should be addressed with a risk approach.

What about the new risks we face?

Besides the traditional strategies we already know and do, such as perimeter defense, defense-in-depth, and others, we need to talk about the ones that can affect our networks as we have them today. As we mentioned before, networks are now more than just Ethernet cables and Wi-Fi at our offices, with a bunch of servers and network devices connecting computers, users, and services.

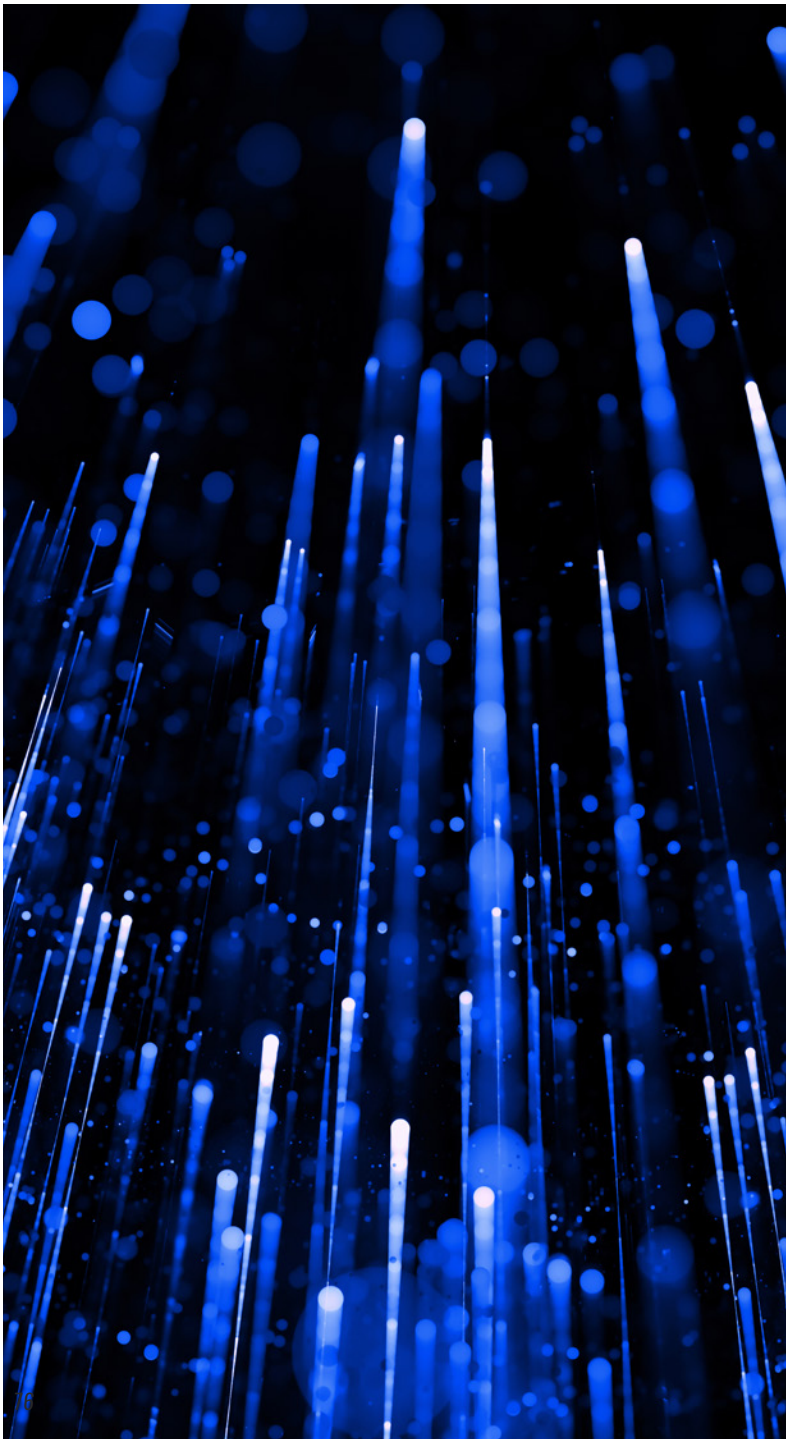
Networks now can be as extended as the coffee shop's Wi-Fi where the C-Level executive takes the morning coffee while checking an email or CRM, to the sandy beach in Thailand where the developer you hired is working on your new project. This means that our devices, no matter where they are, have become the "last mile" of our networks.

With the "new mobility" we have achieved, cybercriminals have found a very fertile soil to grow cybercrime and create more advanced ways of achieving their goals.

One example is the way ransomware is expanding now, as it has grown almost 150% in the first quarter of 2020. Usually, it uses three main methods to spread; social engineering, credential harvesting, and vulnerability exploitation. Each method takes advantage of different organizational vulnerabilities. However, the innovation of ransomware attacks is that it has become more alike cybercrime, as a service model manner, rather than just one individual looking for data or crime monetization.

This expands the threat horizon even more, if our devices are the "last mile" of our networks, it means that they are an entry point to our network and our information.

Another entry point that represents high risk and that sometimes we do not see as a real threat are suppliers. Supply chain attacks have been in the news more recently and the impact we know is that those attacks can become a red flag for any organization. It is true we cannot extend our controls to our supplier's network most of the time, but we can generate policies that can help our organization to choose better suppliers and enforce compliance with our acceptable risk levels. Risks and threats now go beyond our local area network or our data centers, they go wherever there is a user accessing our data or services.



Is it a visibility problem?

We have discussed a bit about cybersecurity, network security, and threats, and this discussion led us to understand that network security is not only a technology problem. As engineers, we say that the more information we have, the better decisions we make. Visibility in the networks is something all cybersecurity professionals want to achieve, yet, how can we achieve visibility in an environment that changes and moves so fast? Some network security solutions have come to solve this kind of problem. SIEM, for example, which stands for "Security Information Event Management", is a technology that together with other new technologies, such as artificial intelligence, gives us not only visibility but also the ability to prevent incidents before they happen. If it were only a visibility problem, Syslog and other known logging technologies would solve it. The problem is that we need to have confidential information digested, and be quick to make the right decisions.

Sometimes we are even letting technology take care of big decisions, such as the case of using machine learning to create anomaly behavior detection. Something security teams and network security devices rely on a lot these days. In the end, it is not a visibility problem but a speed problem.

How fast can we make decisions based on the information we have; how fast can we respond to attacks and compromise; how resilient we are when we face attacks.

What is the right approach?

Let us talk about risks before we decide on technologies. Many organizations burn millions of the cybersecurity budget purchasing network security hardware and software, sometimes without a previous strategy or risk approach.

We do understand that some technologies that need to be there just because they are the foundations. Firewalls, endpoint protection, intrusion prevention and detection, and user management are examples of network security technologies that need to be in place before going for more advanced solutions. Also, strategies such as network segmentation or least privilege access have been there for a reason.

The goal here is not to criticize the purchasing of new technologies but to take the right approach. We need to hit where it hurts. Where it hurts us in fact, everything we do needs to be based on lowering the risks we face.

Whether it is to deploy new technologies or to create a new policy or process. Everything should be against threats and minimize our vulnerabilities. This way, we can say that we are doing a smart investment and not just reactive purchasing.

Is Zero Trust network security?

When we talk about network security, the new concept is Zero Trust. It talks about defining our users as our final frontier. The Zero Trust security model tells us that users should only have the necessary access and permissions that they require to accomplish their roles in your organization. This allows organizations to have more granularity on what users can and cannot do, also get more visibility and less reaction time in case of an attack. The answer is yes, zero trust is network security, and managers should start to dig into it.

Pablo Barrera
Cybersecurity Services Director for ES Consulting

He has over 20 years in cybersecurity and holds several certifications, such as CISSP, Ethical Hacking, ISO 27001 Senior Lead Auditor, ISO 27032 Cybersecurity Manager, ISO 27035 Lead Incident Manager, and others related to the field of cybersecurity. A certified trainer for PECB and Mile2, and a known cybersecurity speaker. He is the OWASP Chapter Leader for Guatemala. Currently teaches cybersecurity, networking, and IT audit courses at two universities. Passionate about technologies and cybersecurity, he enjoys discovering vulnerabilities and coaching new cybersecurity talents at ES.

My ongoing time at PECB University is leaving me with an open mind and critical important skills, particularly in communication and project management skills, which I have begun to deploy to my work. My vision has broadened to the endless opportunities available to make a difference in a field that is important to my career.

Following the communication skills lecture this semester, my communication skills have drastically improved and I have developed a strategic way of going about projects; there are fundamental concepts that my activities are now based on that emanated from my studies at PECB University. By the time my course will be finished, I am sure to add value to whatever I am involved in.

PETER OKOLOH

Executive MBA in Business Continuity Management

PECB University offers a multitude of different courses in various academic programs, e your journey to success in your chosen field.

Graduate Certificate Programs

Graduate Certificate in Cybersecurity
Graduate Certificate in Governance, Risk, and Compliance
Graduate Certificate in Business Continuity Management
Graduate Certificate in Management Systems Administration

Executive MBA Pr

Executive MBA in
Executive MBA in
Executive MBA in

nlightening

rograms

Cybersecurity

Governance, Risk, and Compliance

Business Continuity Management

ENHANCE YOUR SKILLS, FOR A SUCCESSFUL JOURNEY

Advance with PECB's new and updated training courses!
Contact us at **marketing@pecb.com** or visit our **website** for more.

New and updated training courses

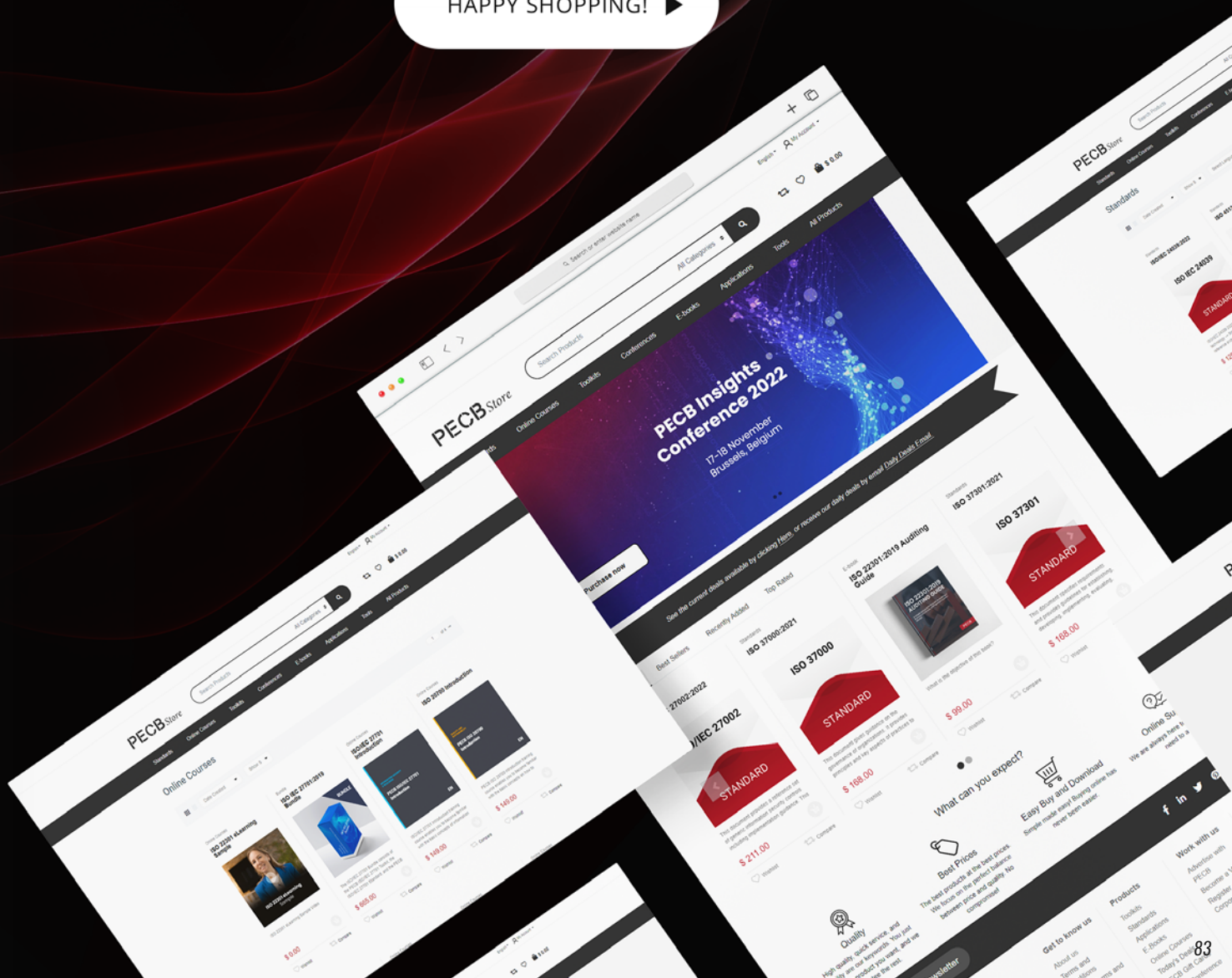
Training Course	Language	Status	
ISO/IEC 27005 Lead Risk Manager	English	Updated	→
ISO/IEC 27005 Risk Manager	English	Updated	→
ISO 45001 Lead Implementer	English	Updated	→
ISO 45001 Lead Auditor	English	Updated	→
ISO/IEC 27002 Lead Manager	English	Updated	→
ISO 37001 Lead Implementer	English	Updated	→
ISO 9001 Introduction	English	Updated	→
ISO 37001 Lead Implementer	Spanish	Updated	→
ISO 37001 Lead Implementer	Indonesian	New!	→
ISO/IEC 27001 Lead Implementer	Italian	New!	→

SHOPPING MADE EASY AT YOUR FINGERTIPS!

We are happy to announce that you can now find PECB Store products on our Facebook profile as well. Browse through our catalog of Toolkits, eBooks, Online Courses, and Insights Conference Tickets directly from our Facebook Shop.

You can access our Facebook Shop by going to our **PECB profile** on Facebook and clicking Shop, or directly by clicking **here**.

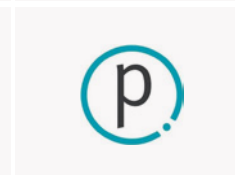
HAPPY SHOPPING!

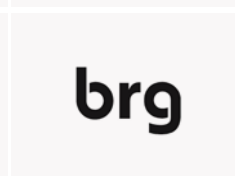


SPECIAL TI

TITANIUM

GOLD PA



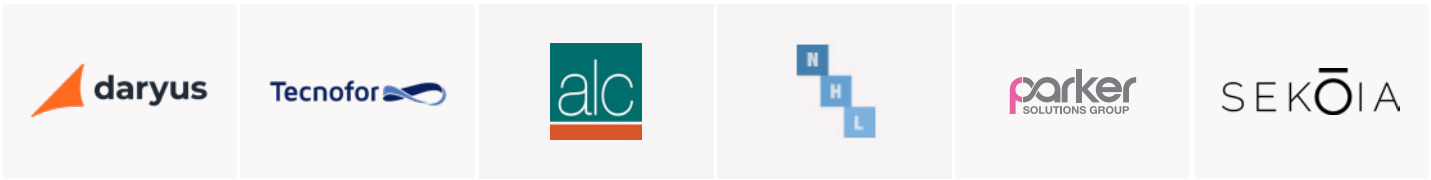


Note that PECB Partners are listed as per the credits

HANKS TO

PARTNERS

ARTNERS



acquired from January 1, 2021 to December 31, 2021.

STRENGTHEN YOUR ORGANIZATION'S VULNERABILITIES