ISSUE 25 | MARCH-APRIL 2020

PECB Insights

THE CYBERSECURITY LANDSCAPE

LEADERSHIP STANDARDS EXPERTISE TECHNOLOGY BUSINESS & LEISURE TRAVEL SUCCESS STORY BOOKS INNOVATION

The previous issue of the PECB Insights Magazine at a glance

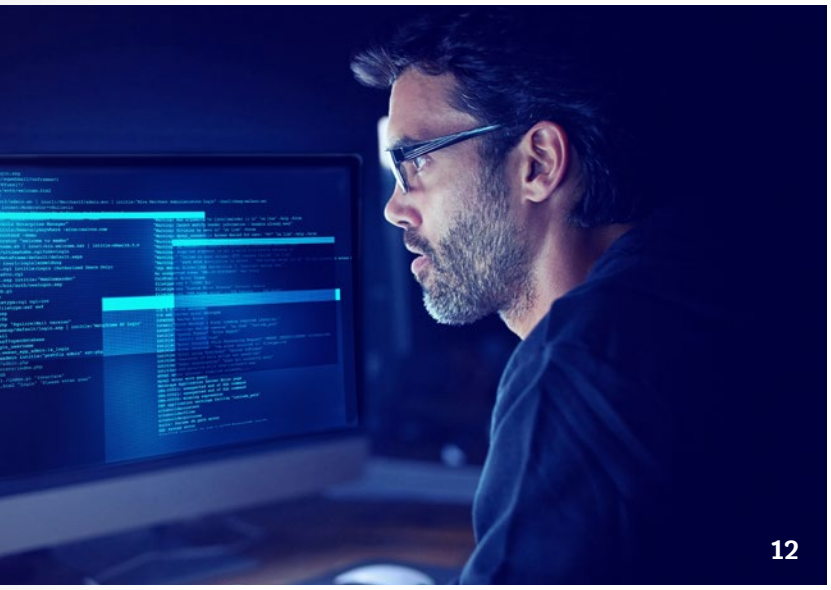
- Artificial Intelligence: The Threat of Deepfake
- California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR): Differences & Similarities
- Meet Raúl V. González Carrión: Risk Manager at Deloitte & PECB Certified ISO 31000 Master
- Why A Star Team Will Always Outshine A Team of Star Players
- One Step Ahead With Privacy by Design
- Abu Dhabi: The Futuristic Jewel of the Middle East

→ READ NOW

HAVE YOU SEEN
OUR RECENT ISSUES?

→

In This Issue



PECB'S STATEMENT ON NOVEL CORONAVIRUS (COVID-19)

The novel COVID-19 pandemic has unexpectedly created a shift in our lives, but our collective ability to adapt, adjust, and respond to these unpredictable events has brought to light our strength and resilience.

The unpredictable nature of events such as COVID-19 makes preparedness a powerful catalyst for safety and prevention. Proper planning is therefore essential in mitigating risks, avoiding consequences, and coping with the negative effects of the pandemic, but at the same time, continuing daily operations so that customer needs do not remain unfulfilled.

At PECB, the health and safety of our staff, partners, trainers, auditors, and end-clients is number one priority. As such, we have been following very closely the unexpected and appalling global developments and have immediately activated our business continuity plan, proactively implemented a range of precautionary measures, from strict sanitation and cleaning protocols, to workplace distancing, and sending staff to work from home.

We aim to protect our staff, clients, and their families while making sure that we continue to offer excellent customer service. Our business is ongoing, our home offices are fully operational, and our production and delivery are secured. Our partners also have adjusted their operations to ensure increased measures for the delivery of training courses, which include also distance learning methods.

Although we are socially distanced, we must remain intellectually connected. Hence, we want to help you keep motivated and engaged, by offering the Pandemic Preparedness and Response Introduction training course material free of charge, for everyone.

→ GET IT NOW

Keep learning, stay positive, and follow the detailed guidelines of the World Health Organization.

Our most heartfelt wishes go to all who have been affected by COVID-19. We are all together during these unforgiving times!

BEYOND RECOGNITION

“AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.”

NEWTON LEE

Evolving Vulnerabilities on the Horizon

In the context of the major health crisis caused by the novel coronavirus (COVID-19), that our planet is going through, hackers and cybercriminals are trying to take advantage of the situation to attack the impacted companies and exploit their vulnerabilities, particularly those caused by teleworking.

A great number of companies have switched to remote working overnight, operating in partial and degraded mode, without necessarily being previously prepared for the risks associated with nomadism.

Organizations that had not previously taken into account or poorly prepared the scenario of unavailability of human resources in the framework of their business continuity plans found themselves deprived and obliged to improvise in an emergency the confinement of their employees and working remotely without taking into account all the necessary security, good cybersecurity practices, and especially without having tested their crisis management systems and remote access in such scenarios.

The weakest links in this equation are on the one hand the company's staff, because they are not sufficiently aware and trained regarding the risks associated with remote working, and on the other hand the information systems, because they are not prepared for this unusual operation.

The risk of exploitation of vulnerabilities induced by the health crisis situation thus becomes stronger by more offensive and opportunistic threat agents in the current context, as the reported attacks and the figures that have been compiled are there to prove. Thus, since the beginning of the pandemic, many serious cybercriminal actions have already been carried out. According to indicators, hundreds of millions of dollars have been paid to Bitcoin accounts that spread ransom, tens of thousands of new domains registered since the beginning of the pandemic including hundreds of domains used by phishing and spear-phishing campaigns.

In this particularly sensitive situation, companies must now adopt an emergency cybersecurity strategy to deal with these unexpected risks.

The experts and analysts of ACG Cybersecurity recommend to carry out an emergency cybersecurity action plan to deal in the best possible way with the submerging threats of the pandemic crisis COVID-19:

1. Awareness of the risks associated with cybersecurity

It is never too late to set up and run targeted and sustainable cybersecurity awareness campaigns among business users on the risks associated with teleworking and the proper use of teleworking tools, by diversifying the awareness channels.

2. Support for information systems specialists

Good management and support of the IT and Cybersecurity teams in charge of the information system and its security is essential in crisis situations. Increasing their skills can become a priority, in particular by supporting external teams of specialized consultants, available on the consulting market, and then by targeted training strategies.

Reinforcing the security of nomadic devices through additional security measures could prove necessary even in the heat of the moment. The ultimate goal is to establish a sustainable culture of security by design from the very beginning of IT projects. As the company is not immune to internal threats, monitoring and control of privileged access must be carried out continuously and effectively through IAM systems and well-defined procedures.

3. Vulnerability assessment and scanning

The first way to protect your information system is to assess its security level by conducting periodic campaigns of scans and vulnerability tests of IT devices and assets. This consists of an examination of the ability of systems or applications, using security procedures and controls, to resist attack, followed by the immediate correction of major and critical nonconformities.

Vulnerability assessment therefore consists of analyzing the network for known security weaknesses.

Vulnerability scanning tools recognize, measure, and classify security vulnerabilities in a computer system, network, and communication channels. They also help security professionals secure the network by identifying security flaws or vulnerabilities in the current security mechanism before they can be exploited by malicious parties.

Vulnerability assessments are used to:

- Identify weaknesses that could be exploited
- Predict the effectiveness of additional security measures to protect information resources from attacks

Typically, vulnerability scanning tools search the network segment for IP-enabled devices and list systems and applications.

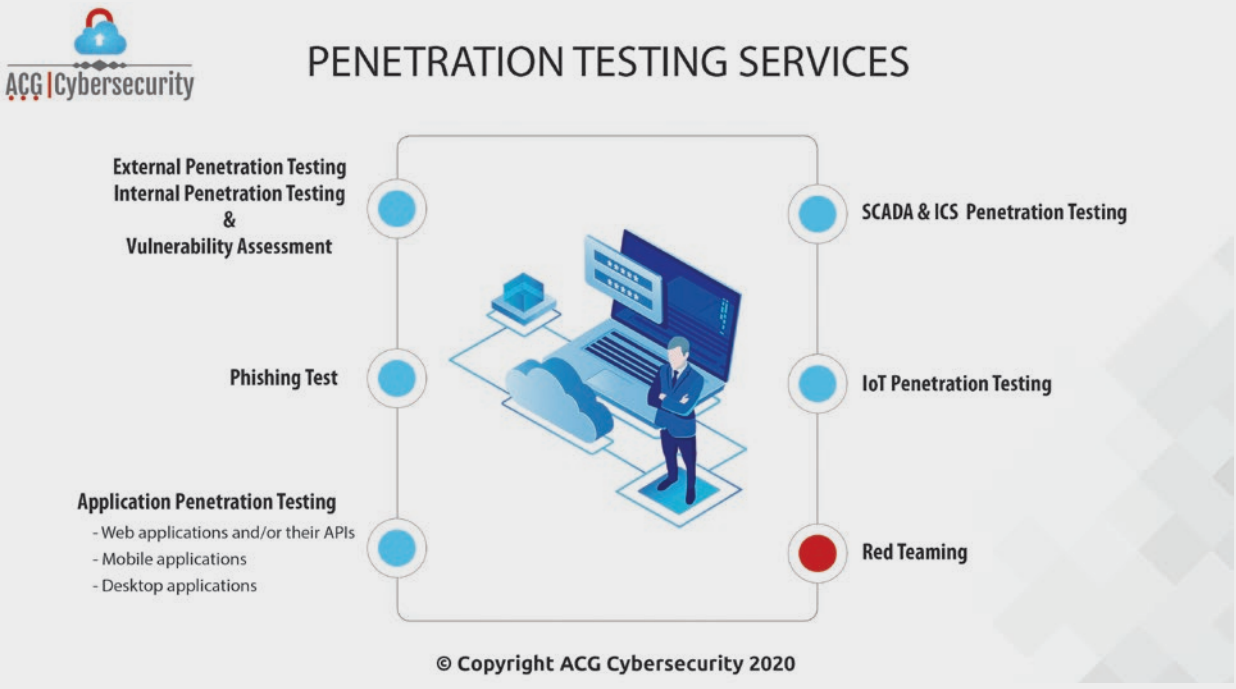
4. Technical security audit and penetration testing

At this stage and in this context of major crisis, vulnerability scans are not sufficient to protect information systems. That is why organizations must also conduct technical audits and penetration tests to test computer systems by putting themselves in the postures of hackers by using other techniques to exploit vulnerabilities not identified by vulnerability scanners.

It is therefore recommended to conduct security audits and penetration tests in order to identify configuration flaws and complex vulnerabilities by analyzing the attack scenarios envisaged by cyber-malicious agents.

The security assessment through security audits and penetration tests aims to identify configuration defects, vulnerabilities that exist on assets at the level of the organization's information system before they are exploited by malicious actors.

Penetration testing consists of simulating malicious attacks on your information system, network, or organization in real conditions. Its objectives are to determine the level of resilience of your computer system against attacks from inside or outside your network.



There are several levels of pen testing services to deal with cyber-attacks in such situations:

Internal intrusion test: Simulated attacks are employed by a person wishing to commit a malicious act by being present on your company's internal network.

External intrusion test: Simulated attacks will be carried out from the outside, with or without knowledge of your organization's infrastructure. The objective is to mimic the real actions of a hacker who does not have access to your internal network.

Phishing test: The purpose of phishing tests is to carry out an inventory of the level of awareness of your employees by launching one or more phishing test campaigns.

Technical security audit: Configuration or compliance audits allow you to evaluate the IT security of your network by analyzing the configuration of your technical bases, including operating systems, software, application servers, and network equipment. The source code audit allows you to exhaustively detect vulnerabilities affecting an application, in order to validate the respect of good development practices.

In conclusion, neither zero risk nor absolute security exists, and companies remain perpetually exposed to the risks of cyberspace. They must nevertheless know how to anticipate and prepare scenarios and major risk situations that can lead to crises making companies even more vulnerable.

Organizations must ensure the effectiveness of their information systems and guarantee continuous improvement to ensure adequate protection of their most sensitive assets.

In addition, the simulation of cybersecurity attacks through penetration tests as well as the review and testing of continuity and crisis processes becomes essential to ensure that the most relevant scenarios have been taken into account in the risk analysis.

About the Author

Bechir Sebai
Founder & CEO at ACG Cybersecurity
and PECB French Trainer of the Year 2019
contact@acgcybersecurity.fr

Bechir SEBAI has more than 15 years of experience in strategic and operational consulting in Security & Cybersecurity for large private and public groups in France and Europe. He has carried out and led numerous missions in consulting, audit, training, crisis management, implementation, and certification of information security and business continuity management systems. Bechir holds a number of certifications: CISA, ISO/IEC 27701 Lead Implementer, ISO/IEC 27001 Master, ISO/IEC 27001 Senior Lead Auditor and Lead Implementer, ISO/IEC 27005, ISO 31000, ISO 22301 Senior Lead Implementer, ISO/IEC 27032 Lead Cybersecurity Manager, Data Protection Officer (GDPR), ISO 30301 Lead Auditor and ISO 21500 Lead Project Manager.

Embracing the Power of Technology to Protect Us

There is a saying that has been the backbone of many cybersecurity scams over the past 20 years, “You can fool all the people some of the time and some of the people all the time.” With this in mind, cybercriminals have been modifying and reusing tried and tested methods to get us to open malware ridden email attachments and click malicious web links, knowing that they will always fool some of the people.

You only need to look at security advice from pretty much any year since the internet became mainstream and you will find that a lot of it can be applied today. Use strong passwords, do not open attachments or click links from unknown sources. Sounds familiar? Why are people still falling for modified versions of the same tricks and scams that have been running for over a decade? Then again, from the cybercriminals perspective, if it is not broken, why fix it? Better to evolve, refine what works, and collaborate.

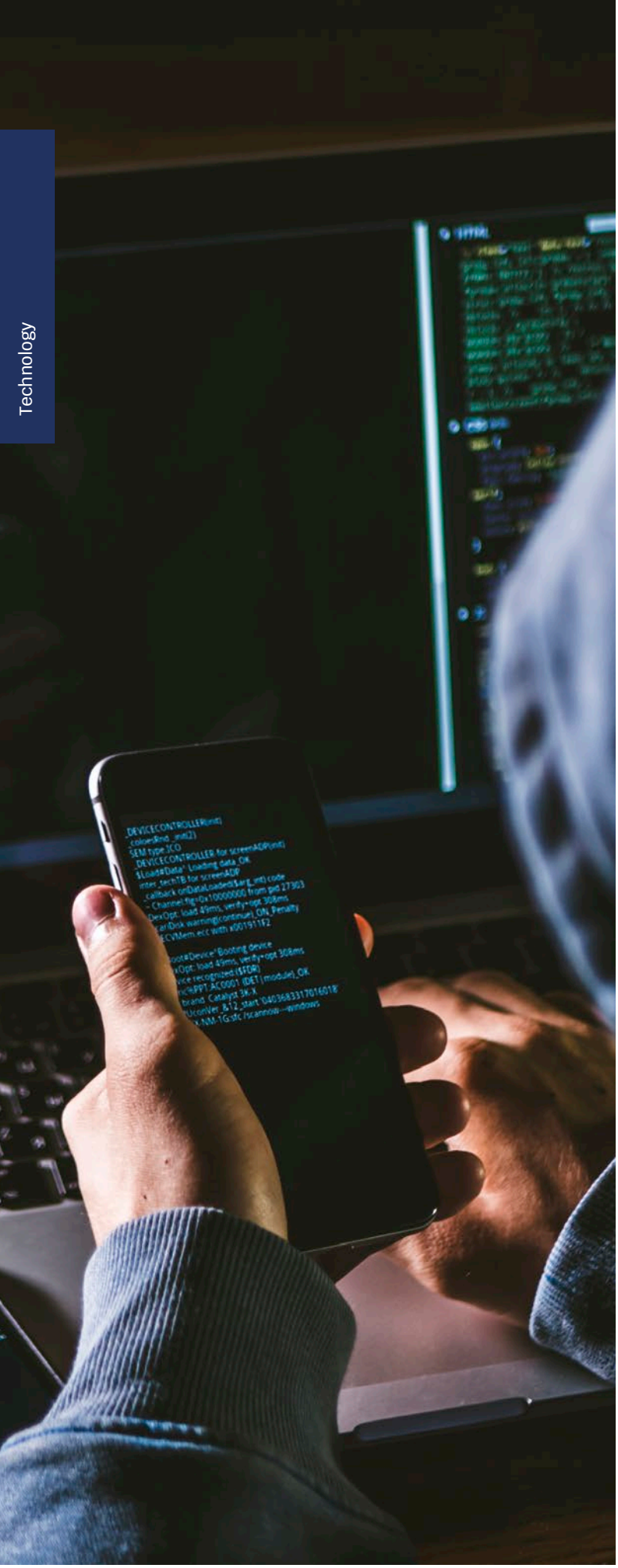
There is a solution though, where it is possible to be in a position where you can no longer fool people, even some of the time, because it is not their decision to make anymore. This is achieved by putting technology in between the user and the internet that decides whether or not to trust something. Trust becomes key, and a lot of security improvements can be achieved by limiting what is trusted, or more importantly, defining what not to trust or the criteria of what is deemed untrustworthy.

We have been doing this for years, as many systems will not trust anything that is classed as a program or executable, blocking access to exe or bat files. The list of files types that can act as a program is quite extensive though, if you do not believe me, try to memorize this list: app, arj, bas, bat, cgi, chm, cmd, com, cpl, dll, exe, hta, inf, ini, ins, iqy, jar, js, jse, lnk, mht, mhtm, mhtml, msh, msh1, msh2, msh1xml, msh2xml, msi, ocx, pcd, pif, pl, ps1, ps1xml, ps2, ps2xml, psc1, psc2, py, reg, scf, scr, sct, sh, shb, shs, url, vb, vbe, vbs, vbx, ws, wsc, wsf, and wsh. As you can see, it is way too much for a person, but easily blocked by technology.

We can filter and authenticate email based on domain settings, reputation scores, blacklists, DMARC (Domain-based Message Authentication Reporting and Conformance) or the components of DMARC, the SPF, and DKIM protocols. Email can also be filtered at the content level based on keywords in the subject and body text, presence of tracking pixels, links, attachments, and inappropriate images that are "Not Safe For Work" (NSFW) such as sexually explicit, offensive, and extremist content. More advanced systems add attachment sandboxing, or look at the file integrity of attachments, removing additional content that is not part of the core of the document. Others like "Linkscan" technology look at the documents at the end of a link, and will also follow any links in those documents to the ultimate destination of the link and scan for malware.

> **Where we are let down though is the area of compromised email accounts from people we trust and work with. These emails pass through most people's email filters as they originate from a genuine legitimate email account (albeit one now also controlled by a cybercriminal) and unless there is something suspicious in the form of a strange attachment or link, they go completely undetected as they are often whitelisted.**

This explains why Business Email Compromised (BEC) attacks are so successful, asking for payments for expected invoices to be made into "new" bank accounts, or urgent but plausible invoices that need to be paid ASAP.



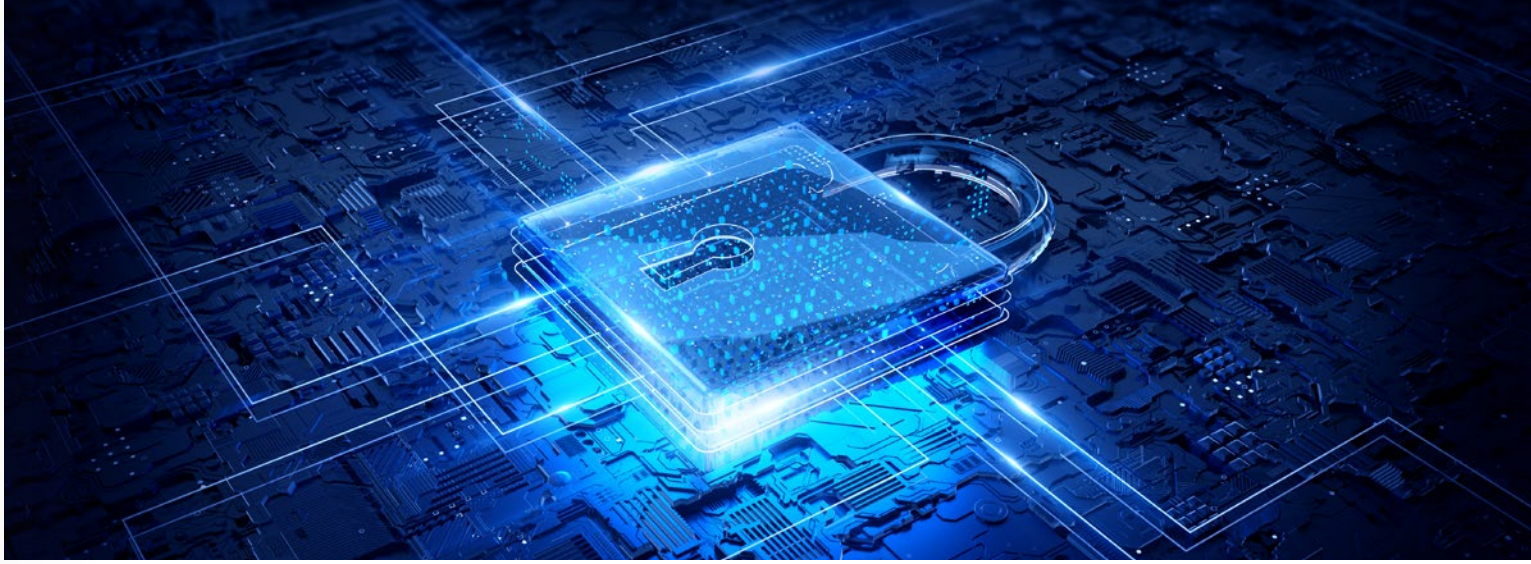
If the cyber-criminals are careful and copy previous invoice requests, and even add in context chat based on previous emails, there is nothing for most systems to pick up on. Only processes that flag up BACS payments, change of bank of details, or alerts to verify or authenticate can help. Just double-check the telephone number in the email signature before you ring, in case you are just ringing the criminal.

Not all compromised email attacks are asking for money though, many contain phishing links or links to legitimate online file sharing services, that then link to malicious websites or phishing links to grant permission to open the file. To give you an idea of the lengths cybercriminals go to, I have received emails from a compromised account, containing a legitimate OneDrive link, containing a PDF with a link to an Azure hosted website, which then reached out to a phishing site.

In fact, many compromised attacks are not even on email, social media is increasingly targeted as well as messaging services or even the humble SMS text message via SIM swap fraud. As a high percentage of these are received on mobile devices, many of the standard security defenses are not in place, compared to desktop computers and laptops. The one thing that is available is two-factor authentication (2FA) which will help protect against phishing links, regardless of the device you use, so long as you train everyone in what to look out for and how they can be abused.

One area I believe makes even greater strides in protecting users from phishing and malicious links is to implement technology that defines what not to trust based on the age of a web domain and whether it has been seen before and classified. It does not matter how good a clone phishing website is for Office 365 or PayPal if you are blocked from visiting it, because the domain is only hours old. The choice is taken out of your hands, you still clicked on the link, but now you are taken to a holding page that explains why you are not allowed to access that particular web domain. The system I use called Censornet, does not allow my users to visit any links where the domain is less than 24 hours old, but also blocks access to any domains or subdomains that have not been classified because no one within the ecosystem has attempted to visit them yet. False positives are automatically classified within 24 hours, or can be released by internal IT admins, so the number of incidents rapidly drops over a short period of time.

Many phishing or malicious links are created within hours of the emails being sent, so having an effective way of easily blocking them makes sense. There is also the trend for cybercriminals to take over the website domain hosting



cPanels of small businesses, often through phishing, adding new subdomains for phishing and exploit kits, rather than using spoofed domains. I have seen many phishing links over the years pointing to the domain of a small hotel. Either way, as these links and subdomains are by their very nature unclassified, the protection automatically covers this scenario too.

Other technological solutions at the Domain Name System (DNS) level can also help block IP addresses and domains based on global threat intelligence. Some of these are even free for business use, like Quad9.net, and because they are at the DNS level, can be applied to routers and other systems that cannot accept third party security solutions. On mobile devices both Quad9 and Cloudflare offer free apps which involve adding a Virtual Private Network (VPN) profile to your device. It is preferable though to have a premium VPN solution on all your users' mobile devices, as these can be centrally managed and can offer DNS protection as well.

Further down the chain of events are solutions like privileged admin rights management and application whitelisting. Here, malware is stopped once again because it is not on a trusted list, or allowed to have admin rights. There is also the added benefit that users do not need to know any admin account passwords, so cannot be phished for something they do not know the answer to. Ideally, no users are working with full administrator rights in their everyday activities, as this introduces unnecessary security risks, but can often be overlooked due to work pressures and workarounds.

Let us not forget patch management is also key, because it does not matter how good your security solutions are if they can be bypassed because of a gaping hole via an exploit or vulnerability in another piece of software, whether at the operating system or firmware level, or via an individual application. Sure, no system is perfect and there is no such thing as 100% security, which is where the Endpoint Detection and Response (EDR) solutions and Security Information and Event Management (SIEM) solutions come into play. These can help minimize the damage through rapid discovery and remediation, hopefully before the cybercriminals achieve their goals.

By embracing the power of technology to protect us, layering solutions to cover the myriad of ways cybercriminals constantly attempt to trick us, we can be confident that emotional and psychological techniques and hooks will not affect technological decisions, it is either yes or no. The more that we can filter out, makes it less likely that the cybercriminals will still be able to fool some of the people all the time. The trick is to spend your budget wisely to cover all the bases and not leave any gaps, which is no easy feat in today's rapidly changing world.

About the Author

Nick Ioannou
Head of IT, blogger, author, and speaker

Nick Ioannou is an IT professional, blogger, author, and public speaker on cloud and security issues, with over 20+ years' corporate experience, including 17 years using cloud/hosted software as a service (SaaS) systems. As an early adopter of cloud systems, including BPOS, the first iteration of Office 365, he has been paying for the privilege of bug testing them ever since. He started blogging in 2012 on free IT resources (www.boolean.co.uk) currently with over 450+ posts.

Nick is the author of "Internet Security Fundamentals," "A Practical Guide to Cyber Security for Small Businesses," and "A Practical Guide to GDPR for Small Businesses" as well as contributing author to three "Managing Cybersecurity Risk" books and "Conquer the Web" by Legend Business Books.

Leading During a Pandemic

A CYBERSECURITY PERSPECTIVE FROM DR. IZUAKOR, A CYBER CULTURE HACKER

What does leadership mean to you from a cybersecurity perspective?

When it comes to cybersecurity, it seems as though there is always a fire to fight. Whether it is a new vulnerability impacting the company, the risk of failing an audit, the doomsday realization that the company has been breached, or something as unprecedented as a global pandemic that brings nations around the world to a halt, leading in such a high risk environment is not an easy feat.

There are many leadership skills that are helpful in fast-paced industries dealing with cybersecurity, which is every company nowadays. Generally, it requires passion, dedication, authenticity, patience, and most importantly the ability to inspire. Beyond these fundamentals, there are four traits that stand out to me as the most critical when leading in cybersecurity.

The first is prioritizing the protection and safety of human beings. Almost every security team out there is short-staffed right now. There are more open jobs in the security industry than people to fill them. Those who work in the industry today, are often going above and beyond to secure and protect their companies from growing threats. If you throw an incident or breach into the mix, and it just gets worse. Before focusing on anything, focus on understanding and support the people involved. No matter how important work is, it should never be done at the expense of a person's health, safety, or family.

The same applies to end users. Despite the current slowdown happening around the world, end users generally move at a fast pace and are overloaded with information. People quickly navigate through constant emails, texts, social media, calls, travel, and more. It can be difficult to slow down and pay attention to detail. This fast pace is what attackers take advantage of as they trick unsuspecting individuals into helping them carrying out attacks. By getting an end user to click on malicious links guised, for example, as pandemic support information or other news, they get one step closer to breaching security. Again, prioritize the human beings in this situation. Seek to understand what their motivations, goals, and priorities are and help them get there in ways that are secure.

> **The bottom line is that whether you are a leader dealing with end users, cybersecurity professional, or another group — as a leader, the biggest priority should be starting by taking care of the human being in the equation.**

Beyond that, the additional traits are being able to anticipate and articulate risks, being prepared for the unknown, and get really good at inspiring people to walk through unchartered territories with you. The only thing constant in cybersecurity is change. There is always a new attack, a new vulnerability, or something new we did not think of before. I think a great leader is good at anticipating what could go wrong, to the extent possible, in order to manage those risks. Sometimes this means putting on the hat of an attacker and seeing things from your offender's perspective. This is why conducting penetration tests and other offensive security programs is important.

Leaders also have to be prepared for the unknown. This is not just about zero-day attacks in the security industry. There are simply unimaginable threats that arise as technology advances. For example, the world is embracing the power and value of artificial intelligence, autonomous vehicles, e-enabled medical devices, and more. As security leaders, while these advancements are great, we have to think about all of the bad things that can happen if one of those devices is hacked. We have to think about how attackers are leveraging artificial intelligence to attacks us in more sophisticated ways. We have to look beyond the positives and find what can go wrong. It can be taxing on

security professionals to constantly look at things from such a pessimistic perspective, but it is in that perspective and the awareness that it brings that we can find optimism is finding a way forward. And, as a leader, you have to inspire your company, team, customers, and key stakeholders to trust you every step of the way. Talk about pressure.

How has your background and experience prepared you to lead?

Ah, where do I begin? Everything I have ever experienced in life prepared me to be a leader. Three elements that were the most important in helping me prepare are the amazing people I have worked with throughout my career, being an eternal student, and starting from the bottom.

Role models, mentors, and the power of diversity

Over the last decade, I have had the honor of working with some of the greatest security professionals in the world. Seeing how experts from different backgrounds approach security, has given me such a broadened view of the industry and the true value that diversity can provide. I have also been blessed with critical mentors and role models both within security and beyond. I cannot begin to name the list of leaders who believed in me early on, took a chance on me, and gave me the opportunity to not only learn from them, but lead others. Mentors and role models matter! In addition, through over seven years of formal security education, I have studied and worked with amazing academic leaders across the industry. I have seen firsthand the need to balance learning in academia, with real world experience to produce well-rounded security professionals. Lastly, as a cybersecurity culture and engagement expert, I spent the majority of my career focusing on educating and inspiring people from different backgrounds and walks of life within organizations to care about security. This helped me immensely.

Being an eternal student and educator

In my spare time, I am a graduate cybersecurity professor. Doing this means I have to stay up to date with the latest trends in the industry, and break them down well enough to explain them to students. Ultimately, this makes me an eternal student which I believe is critical for any security leader. Curious students also ask a million questions, which forces me to listen and help increase understanding no matter how tough the question is. It is not too different in a boardroom or in other settings. As a security leader, you are the expert and stakeholders will ask tough questions you must be able to answer. During a crisis, like an incident

or pandemic, this is an important skill to have. Whether it is your board, your team, your customers, or a new reporter — people want answers.

Starting from the bottom

I started in the industry ten years ago as a cybersecurity intern. Early in my career I was in the trenches going through hundreds of thousands of incident alerts, weeding out false positives, and investigating potential data leakage from the real alerts. I went on to do the same in other cybersecurity domains such as vulnerability management, social engineering, auditing, and more. As I began to lead others, this experience gave me a certain appreciation for and ability to empathize with the teams I have led. One of the most demotivating things a team can face is working for someone who is so far removed and disconnected from the reality of what you do, that they cannot effectively lead you.

Unfortunately, this is a position many leaders land in. Due to the new and budding nature of the industry, cybersecurity executives leading today usually have transitioned into the industry from another field. They may not have had the opportunity to start on the front line. This makes focusing on people even more important. No matter where you start, it is important to get in the weeds a bit even if just in the beginning and truly understand "a day in the life" of the different security roles — especially the ones you have never done before.

> **Starting from the frontline of operations and knowing what it is like to struggle through the tasks your team does will put you in a better position to empathize and make good decisions. That is something I could not learn in school. I had to learn it by doing the work.**

When disaster strikes, what advice would you give to leaders?

Focus on health and safety, before anything else

I might sound like a broken record at this point, but people first! The safety of people should always be the number one priority. Depending on the circumstance, different approaches may be required. For example, the way you lead through a pandemic, may be slightly different from the way you lead through a global health scare. In the event of a significant technology incident or breach, you want to act quickly to triage and contain the impact, and then work to do damage control and bring things back to normal. This could mean days, weeks, or months of long hours and hard work in an absolutely chaotic environment. This can be very taxing on tech teams, making the "people first" mantra important here. Make sure that people are putting their health first, taking time to rest, caring for their families and more.

The same applies in a pandemic or natural disaster. The security industry does not have the option to hitting pause during these events, otherwise consider it a dark web field day. Not only do attackers continue to try and breach security during these times, their efforts often increase. For example, during the coronavirus pandemic phishing attacks saw a 40% increase. The work will get harder during these times, and it is important to support people through it.

Communicate like your life depends on it — it just might

Generally, during crisis people understand that there is uncertainty. However, that uncertainty can lead to added stress and panic, especially when enough information is not being shared. It is important to be open and honest with people. Share what you know and overcommunicate to ensure the message is heard. Be honest about the things you do not have answers to yet. People can be a lot more understanding when they know that you hear their concerns and are trying to address them, rather than feeling ignored.

Priorities will likely shift, be prepared

It is important to define priorities during crisis, as they will likely need to shift. If there are new directions or new priorities teams should be focusing on, make that very clear and be conscious of the things that may be put on hold as a result. Another highly demotivating thing that can happen during crisis is for leaders to ask people to put "all hands on deck" to solve an issue, and then hold people accountable or punish them for neglecting other areas unrelated to the crisis. While it seems like common sense, unfortunately, I have had it happen to me before, and it was dreadful to navigate. I was able to see, however, that the leader did not have bad intentions. They were just so stressed out and on edge with the crisis and trying to hold everything together, that they did not stop to think about the tradeoffs the team would have to make.

Lead by example

Dealing with crisis might require heavy sacrifices. For example, it could be spending a weekend in the office working to address a ransomware attack and bring systems back up. Or it could be taking a pay cut because the company has been impacted by a global economic downturn. In either case, leaders who walk to walk and sacrifice first before ever asking others to do so, command much more respect and loyalty. It is kind of hard to explain to your team how they are all taking a reduction in pay to save costs, while their leaders are all getting big bonuses at the same time.

Never waste a crisis

There is always a lesson, no matter what. During the pandemic, for a lot of companies to lesson highlighted here is the need to have a good contingency plan in place. Incident response, disaster recovery, business continuity, and more can make all the difference in how well a business fairs through a crisis. Some companies planned for how they could set up remote worksites, and alternative office locations in the event of a natural disaster, but many had not planned for a scenario where workforces must be fully remote. Many businesses had not planned to make their companies or services completely virtual. All of these changes are lessons and opportunities to continually improve and prepare for the way to world will likely continue to operate for quite some time.

How do you keep people motivated and engaged through rough times, especially when it comes to cybersecurity?

Beyond the points mentioned above, just listen to people and do what you can to help them feel heard and understood. During a crisis they are likely concerned and stressed. Though not always the case, often people do not need answers right away, but are seeking to at least be heard.

Make people a part of the solution. Sometimes we do not realize the goldmine of innovative minds and talents we have all around us. As leaders, instead of relying on yourself or someone with a certain job title or role to come up with a solution that is pushed down, get others involved. For example, I have seen many organizations post a challenge and solicit ideas from their larger employee population on the best ways to address it. The best ideas get upvoted and they work towards those. Whether it is a strategy for how you plan to win your customers trust back

after a major incident or asking employees to share their tips on how they are dealing with the current pandemic, for example, it makes people feel a little bit better when they are contributing to the way forward. They are no longer sitting back helplessly.

Lastly, pay close attention to how eminent risks are evolving in association with your business and find engaging ways to educate stakeholders on what can be done to mitigate the risk. For example, phishing attacks are up. Share engaging tips and trips to help people identify them.

> **Leading through crisis can be difficult; however, within the cybersecurity industry it starts to feel like the norm. You cannot go wrong by putting the safety, health, and sanity of human beings first. That is my guiding principle as I weather any storm.**

About the Author

Christine Izuakor
Founder and CEO of Cyber Pop-up

Dr. Izuakor is a Cybersecurity Culture Hacker. After amassing a decade of experience solving global cyber challenges at Fortune 100 companies, she went on to become the Founder and CEO of Cyber Pop-up. Christine earned a Ph.D. in security engineering from the University of Colorado, becoming the youngest and first African American woman to do so. Christine completed a master's degree in information systems security from University of Houston in 2012 and is a Certified Information Systems Security Professional (CISSP). In 2017, her rapid growth within the technology industry landed her a spot on Chicago Business Crain's Tech 50 List. She was also featured on The 2018 Crains 20 in their 20s list, The Wall Street Journal, Hemispheres Magazine, Cheddar TV, and more.

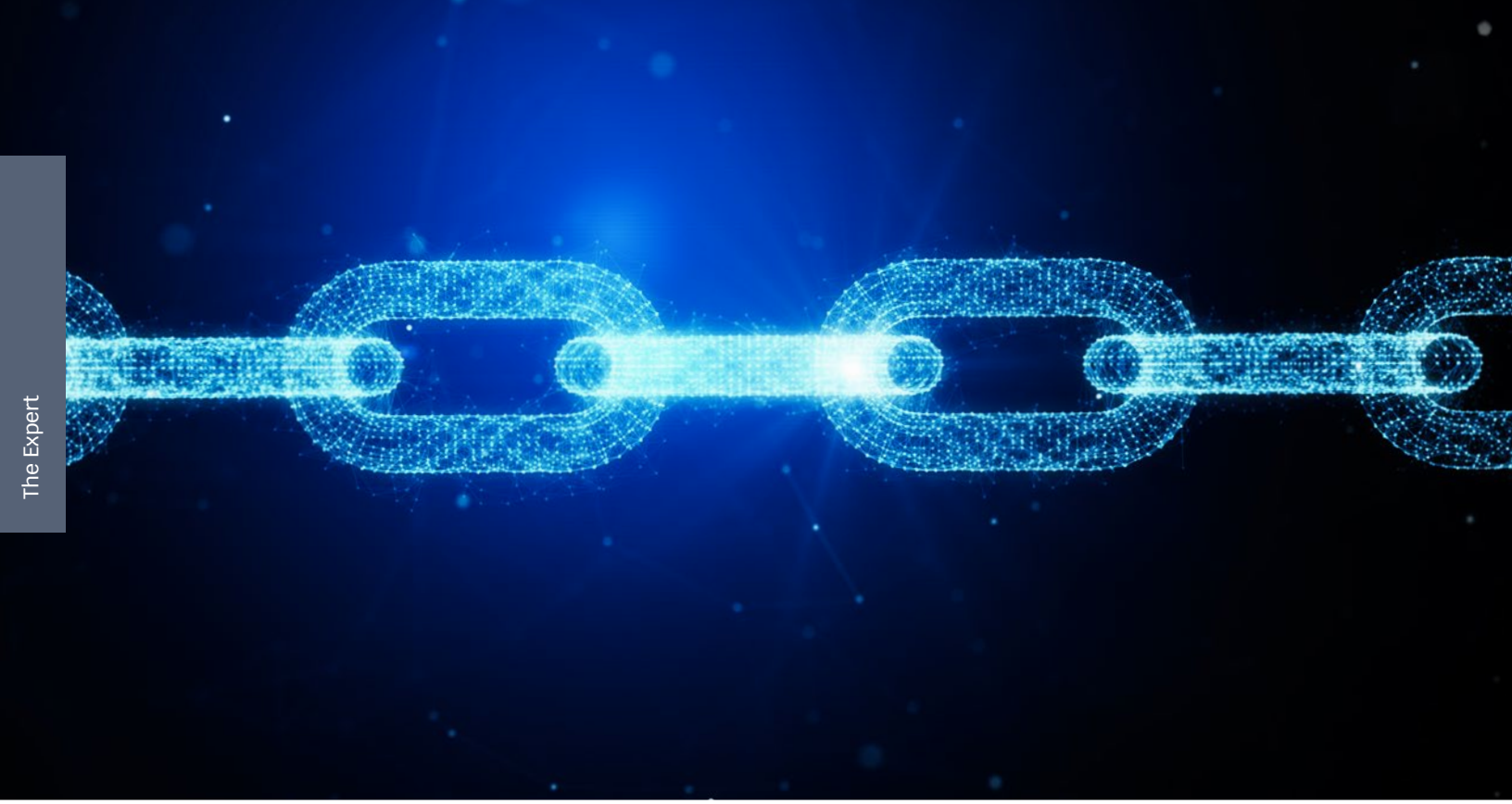
Dr. Izuakor is also active in the diversity and inclusion community. She's co-founded and served as the Vice President of Gen Trend, United Airlines' Millennial business resource group, served a 2 year term as the Head Editor of the Illinois Diversity Council Editorial Board and is an avid Year Up ambassador.

THE ULTIMATE CERTIFIED LEAD ETHICAL HACKER TRAINING COURSE IS COMING!

The PECB Certified Lead Ethical Hacker training course is going to be delivered as a pre-conference training course exclusively for PECB Partners and Trainers.

EVENT COUNTDOWN / NOVEMBER 16-18, 2020

Think like a hacker!
Discover the evolving vulnerabilities before attackers do!



End Users and Cybersecurity: From Weakest Link to First Responders

ARE PEOPLE REALLY THE WEAKEST LINK IN THE INFORMATION SECURITY CHAIN?

This question sounds familiar, right? Indeed, information security is often considered as a chain, and everyone knows that a chain is only as strong as its weakest link is. Starting from this metaphor, it seems like a good idea to find this weakest link in order to strengthen it so that it is no longer a threat for the organization.

When trying to identify this weakest link, most people will state that people are the weakest link. I would like you to think about the number of times you heard someone say that “the problem came from the eighth layer of the OSI model” or that “the problem existed between the chair and keyboard.” I am pretty sure this sounds familiar to most of us. A good joke cannot hurt, most people will say.

I read an interesting research paper lately about how the vision we have of ourselves can really impact who we are and our perception of the things around us. I will not focus on this for too long, but this made me think differently. The idea was the following one: you take a pool of people and ask them if they usually feel like lucky people or not. Then you tell them that they have to find specific information in a text and that usually only the luckiest people can find all this information. When the experiment is over, ask the people about what they found and let them tell you if they think they found everything or not. Guess what, most of the people that said they were unlucky either missed some information or found all of them but thought there were still some they missed.

Now, you may be wondering what is the link between this research paper and our topic here. I am convinced that if you keep telling your coworkers that they are the weakest link in your company's information security chain they will somehow become. It is a state of mind. How can one change this into an opportunity?

How to turn people from weakest link to first responders?

Instead of telling your employees that they may be the reason why security will eventually fail one day, tell them how they can be involved in the company's security posture. Make them become your greatest strength when it comes to enforce security everywhere.

How can one achieve this magic trick?

You need to run a security awareness program in your company if you want to achieve this. If you do not know where to start with, I would definitely recommend reading the National Institute of Standards and Technology Special Publication (NIST SP) 800-50. Even if this document was published nearly two decades ago there are still some good ideas inside, as in any SP NIST ever published.

Your awareness and training program needs to be able to make everyone in the company feel involved. And if you want everyone to feel involved in this program, the core actions of this program need to be adapted to your public every time.

Adapt your actions to the targeted public

When it comes to adapt actions to the public I like to use storytelling and live demos.

The decision makers of the organization might not be concerned about a penetration testing report where you tell them that "you can trigger an XSS vulnerability on the company website as you can see on this screenshot with a popup saying 'XSS here'." But I can tell you that they will feel concerned if you show the whole website defaced with images shaking while playing French cancan music. Of course, do not attempt this in any penetration testing if this is not allowed in the terms of engagement. They will feel even more concerned if you tell them that you would be able to become an administrator of this website by chaining this with a configuration mistake.

The HR manager may already be aware that one should always verify the file extension before opening it, but do they know that most of the file formats can be payloaded? Maybe it is an opportunity for your team to show how an attacker can leverage vulnerabilities in a software that never got updated after it was installed.

Now let us talk about more tech-savvy people, system administrators, or developers, for instance. Do you still happen to have users amongst them that "need" to be administrators of their computers? Do they use this local administrator account when browsing the web? Most of the time, they think that this is a mostly harmless practice. If this sounds familiar, then maybe it is time to introduce them with the BeeF framework.

The most important thing to remember about these live demonstration examples is not that you can cause fear amongst your users. For sure, you will. But even if fear is a powerful lever, the most important thing is to understand that people usually believe what they can see. When you are able to show them that these threats they heard about in a previous awareness session or email communication can be real, they will start to think differently about them.

You can also use examples of other companies that reported breaches in the last few weeks or months. Explain what happened and how this could have been avoided. I feel like it is the perfect time to work in information security because we now have a lot of after-breach communications. Companies no longer keep their breaches secret and you can learn from others' mistakes. Some will even demonstrate a very good crisis management, and this can become an example when it comes to handle crisis on your own side.

One of the most dangerous threats for your end users is obviously phishing. Every day, thousands or maybe even millions of phishing emails are sent all over the world. Luckily enough, most of them can be recognized in a matter of seconds. But some of them are really finely tailored. To explain how phishing works and how attackers are really imaginative to make their message seem realistic you can run your own internal phishing campaign or you can store a few really good phishing attempts, run a live session with a group of users, and explain how you noticed that this was a phishing attempt. Give them tricks, reflexes, and most importantly, the opportunity to have someone from the security team removing doubt on any email they find suspicious. The Société Générale CERT provides an outlook addin coded in C# on Github called NotifySecurity that allows your users to forward any email as an attachment with a reporting template. In this way, removing the doubt on any email received becomes as easy as counting to three. It is worth mentioning that if someone took the time to send a suspicious

message to your team, your team definitely needs to take time to inquire about this. They also need to provide feedback on the message itself and thank the user for being involved in increasing the company's security posture. A positive message is always appreciated.

Offer an e-learning platform to your users

Another option I like to take when it comes to raising awareness is to deploy an e-learning platform. I usually host this platform on an open source Learning Management System (LMS) and add content over time. The content on this platform is split in modules. Each module has a specific topic: information security fundamentals, operational security in the company, ISO27xxx norms, vulnerability management, etc.

Each module is divided in small chapters. "Bite-sized" chapters have shown better results when it comes to raise awareness on a specific topic. This way, the targeted audience can learn something in a few minutes without going through twelve pages of documentation. Going straight to the point is the way. If you feel comfortable with storytelling, try to use it. Quite often a good short story will give better results than just pure information security jargon or risk analysis. If you wonder how to use storytelling efficiently in this specific context, I would recommend that you read the "Transformational security awareness" book by Perry Carpenter. If you have people that can draw infographics in your company, have them doing some to illustrate your chapters.

There is something really important about security awareness programs. You need to ensure that everyone understood the information you gave them. In such cases I make sure that people understood the concepts introduced in a module by running a final quiz. I usually ask them to answer 20 questions out of a pool of 30 to 40. I assume that they understood the key concepts of the module as soon as they get 15 good answers. And this is where we added gamification in my current company. To go further, we installed a module on our LMS to transform it into a roleplaying game experience. Every user has an avatar with a level and experience points. Whenever you validate a module, you get enough experience points to reach the next level on your avatar. The avatar's appearance then evolves into something stronger and you get access to the next module on the platform. When people reach a higher score on quiz, with 18 good answers, they are also rewarded with a digital badge. This works very well for us. People were really proud because they obtained all the badges or because they got a higher score than their coworkers. Gamification creates a real involvement and makes people feel competitive. This gave us really good results on modules completion and improving the overall security posture of the company.

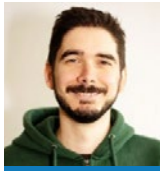
Communicate on important new threats

Whenever a new threat seems really dangerous for the organization I send an email to everybody in the company. I do my best to keep it short and go straight to the point. I want my users to be able to know what can happen and how they could possibly notice that something is happening. I also want them to know that we are setting some security measures up to mitigate the threat whenever it is possible.

Leverage all of this to make them first responders

You may wonder why I talked about transforming people into first responders without even referring to it again in this article. I am convinced that if you raise awareness properly among them with an appropriate program and give them a way to contact your security team whenever they notice something suspicious, they will. As in the example about phishing attempts, make sure to send them appropriate feedback after examining what they submitted to you. This will, without a doubt, make them feel really involved in the security posture of your company. In this way, you will no longer miss a piece of information about something suspicious because of "who cares? I don't even know who I should tell about this and we never receive feedback."

About the Author



Matthieu Billaux
Security Team Leader & Deputy CISO
at Cloud Temple

Matthieu Billaux is a seasoned IT and Security professional with multiple certifications when it comes to security. He has worked for the French military navy for 10 years before working for Gemalto as a Worldwide Operational Security Officer. He is now the security team leader and deputy CISO for Cloud Temple, a leading cloud provider in France. He is in charge of operational security and security awareness programs. Penetration testing, incident response, and security automation are amongst his preferred topics. Matthieu is a certified PECB Trainer for a number of PECB training courses including Lead Penetration Tester and ISO/IEC 27001 Lead Implementer. He also delivers training about fundamental technical skills in infosec for Deloitte's Cyber Academy in Paris.

COVID-19: Isinnova Engineers, the Brains behind the Life-Saving 3D-Printed Valves

INTERVIEW WITH CRISTIAN FRACASSI, CEO AT ISINNOVA

As the globe remains gripped by the devastating impact of COVID-19, noble acts of selflessness have never been more manifested and have given us strength to cope with the consequences of the pandemic.

It has been only a few weeks since the world was full of admiration hearing the news on the life-saving efforts of the Issinova team, Cristian Fracassi and Alessandro Romaioli, who designed and created unofficial copies of respirator valves in just 24 hours for an Italian hospital that was short in supply. For more, they also created the so-called Charlotte valve — an adapter to turn a snorkeling mas into a non-invasive ventilator for COVID-19 patients. This seemingly small yet grand and human act has not only been beneficiary to Italy's region that has been hit hard by the pandemic, but also to other hospitals and manufacturing companies who have decided to follow this path.

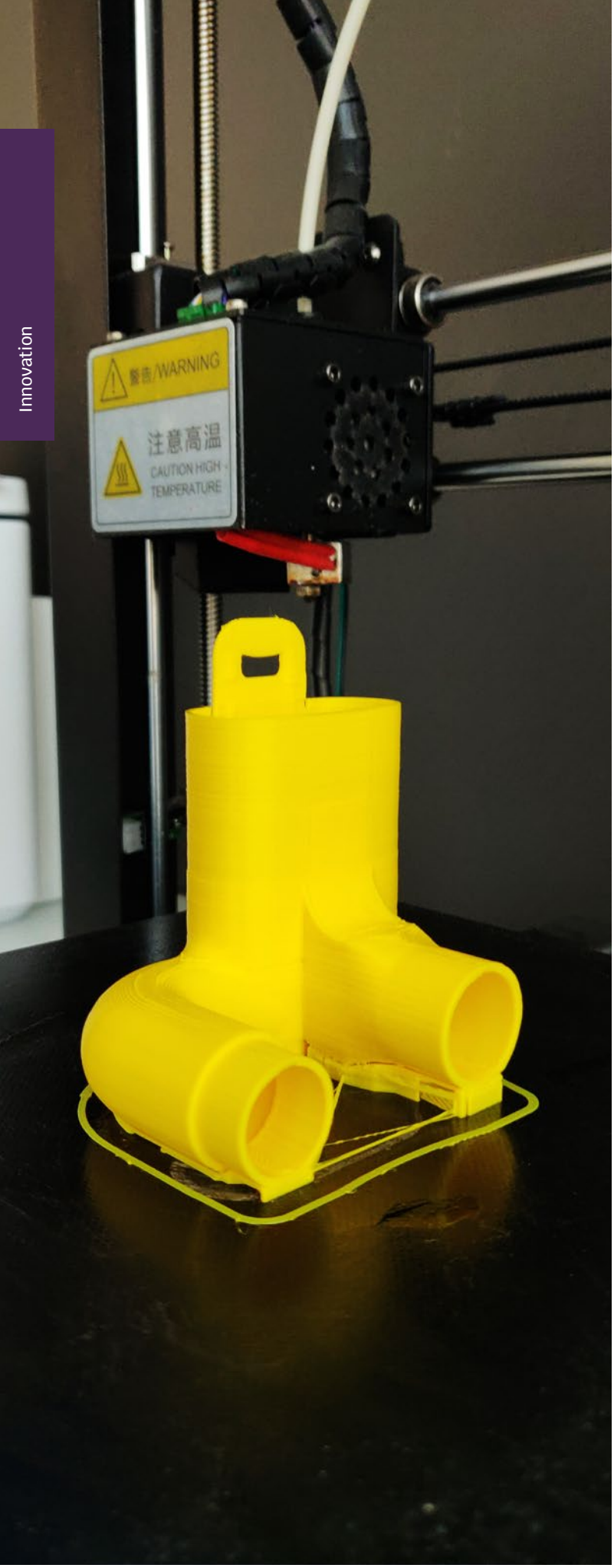
With this news, the assumption that 3D printing, or additive manufacturing, was ushering in a new era has definitely proven to be right. This technology, producing objects of any shape, on the spot and as required, has been rapidly spreading and advancing over the past years. As such, meeting individuals' needs has come to the fore, as there is a software that takes instructions and applies them accordingly.

However, the idea that almost every product would be produced locally, and that the need for supply chain management would be eliminated, seems to be too futuristic. While the best is yet to come, the world has benefited from what has happened today: technology and creativity equaled innovation.

The Isinnova team's achievement has been praised and acknowledged by everyone, and we had the honor to interview Mr. Cristian Fracassi, the founder and CEO of Isinnova, who provided us with information regarding the company and the creation of the respiratory valves and snorkeling masks:

> **"Isinnova is a reality formed by a heterogeneous team of engineers, designers, and communication experts that collects ideas from all types and sectors and transforms them into concrete objects. We address companies and individuals who have an innovative idea and wish to transform it into a finished product."**

From innovative projects, business consulting and research to development services, Isinnova also offers advice from



technical feasibility to marketing. “Usually we start from a problem that the company has to solve, for example, on a machinery or on a productive process.” Although it seems to be customary for the company to have problem-solving a crucial factor of their work, they were initially contacted by the physicist Massimo Temporelli, founder of FabLab.

When asked about how they came up with this innovative idea that would result in saving the lives of so many people, Mr. Fracassi explains:

> **“It all happened very quickly. The director of the hospital of Chiari (Brescia) contacted the Giornale di Brescia to ask if they knew anyone who could print the valves in 3D because they were finished, and there they mentioned our name. So we decided to make ourselves available immediately.”**

In such chaotic yet crucial situation, not only they made themselves available, but they offered this service free of charge.

“In a single day a hundred Venturi valves were printed, immediately used. The prototype was made of polylactic acid with a filament technique that allowed it to be ready in just a couple of hours, although not with great precision. Successfully tested on a patient, the other valves were printed in 3D, this time with two different techniques: one with a light-sensitive resin, and the other with aluminium-filled Polyamide12 powder, which allows very high precision, but requires a longer time, 24 hours.” – he adds.

However, he makes it clear, that as is the case with all things new, they faced difficulties at the beginning: “Being a medical device it has to fit perfectly in order to work, so we had to use more than one 3D printer to make several tests. The advantage of our 3D printers is that they are fast, so we completed the first tests very quickly and during the first day we printed 100 valves.”

Seeing the success of the first valve created, they went on to create the so called Charlotte and Dave valves: “Yes, we created and printed two valves: the Charlotte valve and the Dave valve. The intuition came to Dr. Favero, a retired doctor. He thought he could use diving masks as breathing

masks, which were missing in intensive care in hospitals. So we set to work so that we could adapt the Decathlon masks to the respirators. And so we created the two valves."

After the effective functioning of the masks, Isinnova has shared a detailed file for the realization of the link in 3D printing on their website, allowing for others, be that a company or hospital, to adapt and use them around the world: "Of course, our everyday work is to help people find a solution to their problems. Even more in this critical situation for the whole world, we are convinced that unity is strength. We decided to make the files available because so many people were asking us about the valves or how to help us. Lots of people made the difference in their own house and helped the world."

Mr. Fracassi tells us that they are beyond happy to help people, and at the same time they find themselves caught in the moment, and still do not realize what is going on: "It all happened so quickly, we are working a lot, but we are happy to help people."

In light of these events, the ways and the extent to which 3D printing will change the economy, industry, and culture in the years to come, has been rethought and has made everyone think about the future of 3D printing. Mr. Fracassi agreed that the 3D printing machines will be revolutionary in the near future: "Certainly this project has increased awareness of the potential of 3D printing in many contexts beyond the industrial one."

> **Medical applications for 3D printing are expanding and are expected to revolutionize health care. From prosthetics, to medications and surgery, many medical and tech experts believe that by 2025, 3D printed human organs will be in use for surgery to replace human organ transplants.**

Additionally, through the usage of 3D printing in medicine, medical products, drugs, and equipment would be better customized and personalized, producing a cheaper version of surgical tools, thus improving the lives of those reliant on prosthetic limbs.

From what it is expected to happen in the future to what has already become a reality, the 3D printing's potential to revolutionize our society is yet to be seen.


COVID-19

Never Too Late To Get Ready

We are living in challenging times. Putting to one side the immediate personal health impacts of Coronavirus, its economic effects are likely to be felt for a long time. With suggestions that similar outbreaks might become a regular occurrence, we need to ask what we can learn, and what steps can be taken to prepare for the future.

Some businesses will be forced to close their doors permanently, and many will struggle to recover. Few will come through unscathed. CEOs and business owners alike count on perseverance, knowledge and adaptability, both from themselves and those around them, to get through times like these. But with a crisis of such unprecedented scale and so many unknowns, it will take more to survive.

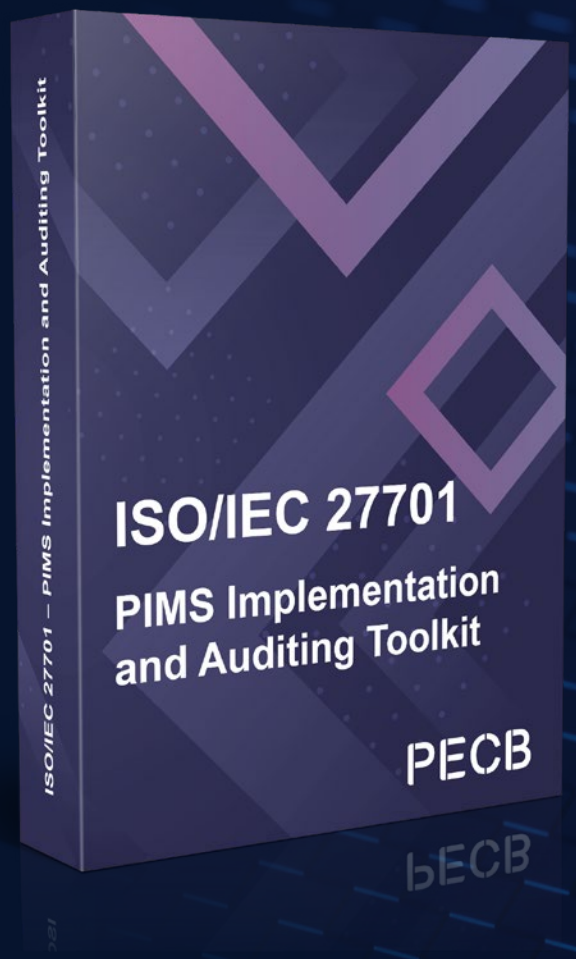
A return to stability and growth will require systematic plans that take into account a fragile economy overshadowed by the threat of a drawn-out pandemic. An ISO business continuity management system is the right way to start filling in the blanks. Often abbreviated to "BCMS" within industry, we're talking about ISO 22301 and related ISO standards.

The entangled nature of globalized business adds layers of complexity to the current situation with governments and experts conflicted on the best way through. What they all agree on is that you can't be too prepared. The good news is that increasingly granular data allows us to understand both the causes and effects of disruptions with better clarity. An information-driven approach is at the center of ISO 22301, which was updated just last year under the direction of ISO's technical committee on security and resilience (ISO/TC 292).

Considering that a BCMS identifies preventative measures, leaders and entrepreneurs might well ask if it's too late to start. Is now really the moment to create, or update, a BCMS?

At a time when all hands are on deck, most businesses will have more immediate priorities. But there is a message of hope for businesses of all sizes. You can get through this, but you cannot afford to be hit twice. If you have never implemented, or even considered, a BCMS, now could be the right time to do it.

PECB Store



The ISO/IEC 27701 PIMS Implementation and Auditing Toolkit is Just One Click Away!

→ BUY NOW

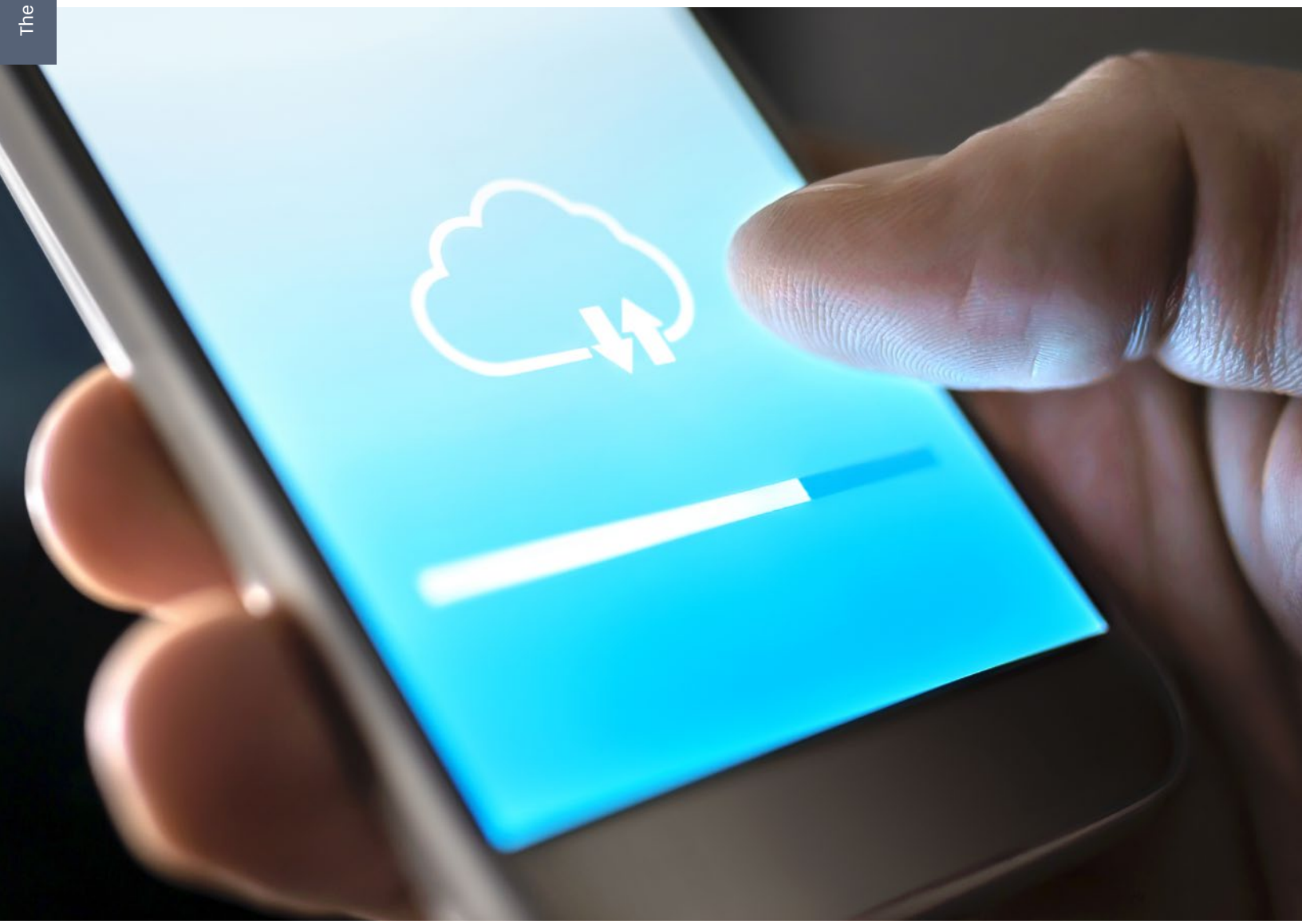
GIFT CARDS ARE THE FUTURE OF GIFTING

Show your appreciation by getting the ones you value a PECB Store Gift Card!

→ store.pecb.com/giftcard

Your Data Travels Even If You Don't

www.reviews.com



Do you ever wonder why things like Facebook or Instagram are free? You pay in privacy. These types of online services are free of monetary charge because they collect your data in exchange for their hosted services.

The more connected we become, the more data we will continue to share. Think about how often you access the internet and input or view sensitive information. From accessing health care information to paying bills online to even tagging your location on social media, you are sharing information that can be collected.

According to a recent study, 47% of Americans were not sure they understood what was done with their personal information and 59% were confused by the privacy policy presented by companies. In a time when our lives are so heavily entwined with the internet, knowing what is done with the data you share is critical.

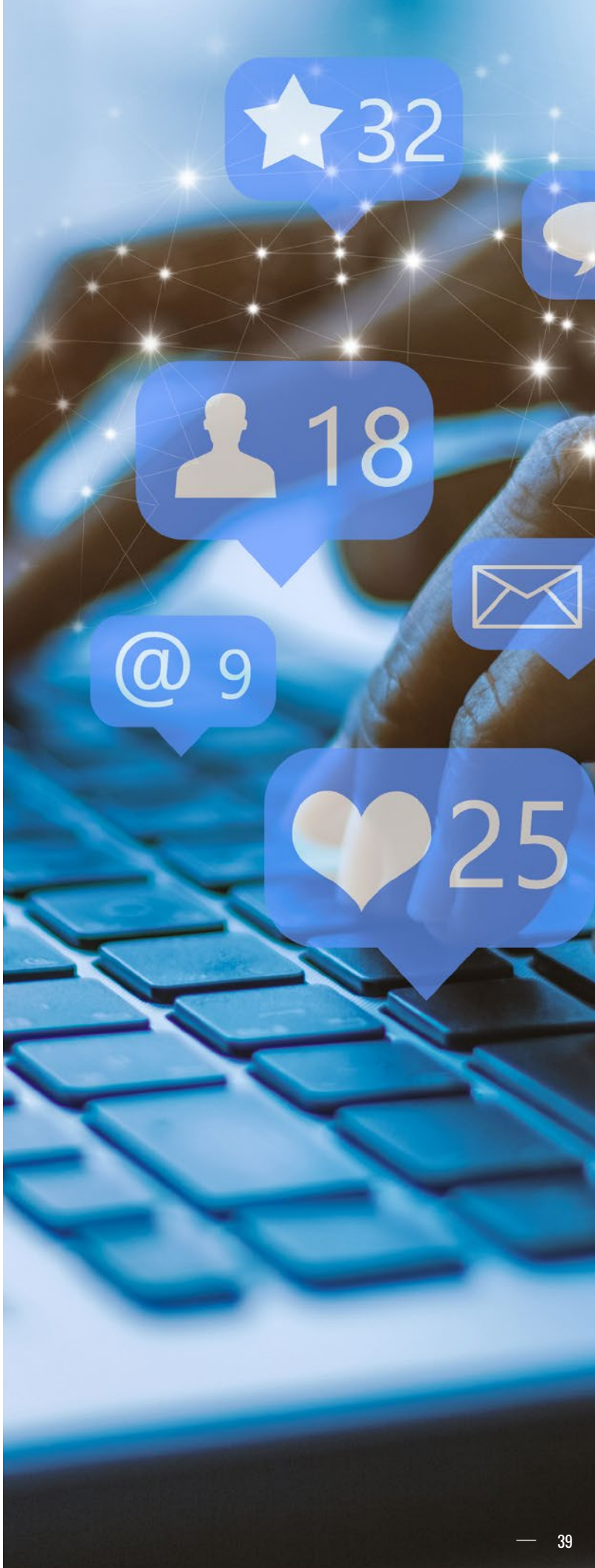
Why it matters

Landmark security breaches remind us how vulnerable our data really is. Equifax, one of the top three credit reporting agencies, disclosed a data breach in September of 2017. Information like social security numbers, names, addresses, and driver's license numbers were compromised for 147 million people, along with 209,000 customer credit card numbers. Given the severity and importance of the information leaked, the Equifax breach is regarded as unprecedented in impact. The settlement reached with the Federal Trade Commission amounted to $425 million to be paid out to help people who were affected.

Facebook has experienced a series of security breaches, which has resulted in federal investigation. In 2019, the user data of 540 million Facebook users was exposed on Amazon's cloud computing services. It was revealed that Facebook partnered with more than 150 companies to share personal information of the hundreds of millions of people who use the social media platform. Users were not aware of this exchange. In a focus group conducted by the Pew Research Center, people spoke negatively about the consequences of sharing data and cited that companies could have an ulterior motive for collecting their data.

Quick Tips to Protect Data at Home

Possible security breaches and companies collecting your information are only one facet of data safety. Your data is also susceptible to being stolen or compromised by hackers. The latter are especially using the present crisis (COVID-19 outbreak) as a tool to attack companies, professionals, and individuals via phishing attacks. Thankfully, there are a number of things you can do at



home to combat them. You do not need advanced tech skills or world-class equipment; these are things you can do on your home computer.

Security software

Installing security software on your computer is one of the first steps you should take. Security software keeps your computer healthy and your information safe from attacks or computer viruses. Make sure you stay up to date with any and all updates of your software. It is easy to close out the persistent pop-up box that reminds you to update, but do not ignore it! Security software is especially important if you are regularly connected to public WiFi networks. While most in-home routers are encrypted, there is no way to know if the internet you are connecting to is safe.

Use a password manager

Using the same password for everything leaves you vulnerable to potentially giving someone access to all of your information. But remembering a gaggle of passwords is no easy feat. Using a password manager is an easy way to ease the burden. Password managers are designed to generate long and complicated passwords that are less likely to be compromised. Your passwords are encrypted and can only be accessed through the master password you create. Depending on the password manager, it may offer an automatic fill feature that kicks in when you go to a page you have a saved password for.

Backup your data

In the event that your information is lost, compromised, or stolen, backing up your data is a way to make sure all of your hard work and cherished memories are not lost. When you back up your data, you are making a copy that is not stored on your computer. Whether you use a local storage option or the cloud, the point is to make your files unavailable to anyone else except you.

Data encryption

Data encryption is an essential way to keep your personal information safe. It works by taking readable text from an email or document and scrambling it into an unreadable cipher text. Encrypting your data will secure it not only on your computer, but also when it is transmitted over the internet. For the information to revert back to its original form, both the sender and recipient have to have the encryption key.

What to Do after a Data Breach

So you have heard on the news or received an email that there has been a breach and your data may have been affected. A security breach does not automatically mean someone is going to steal your identity. Before you panic, use these steps to help you through the process.

1. Confirm if you were affected by the security breach

Beware of scammers attempting to coax more information out of you with fake emails. If you receive an email that a breach has occurred, contact the company directly to confirm. Do not reply to the email.

2. Find out what information was compromised

What you do after a security breach may vary slightly depending on the type of company that was breached. You should tailor your response to the circumstances and to what information was stolen. If you find that you are the victim of the security breach, do not pass up the company's offer to help.

3. Change your passwords

The next important step to take is to address your personal security. Update your login information and security questions for all of your sensitive accounts – not just the ones affected by the breach. Take this time to enact two-factor authentication into your login process to add another layer of security to your accounts.

4. Contact a credit reporting bureau to report

To make sure you are not the victim of identity theft, call any of the major credit reporting bureaus and have them file a fraud alert on your name. This alert makes it harder for someone to open new accounts under your name and lasts for one year. Additionally, you may also consider putting a credit freeze on your report, which will restrict access to your credit report. Bear in mind this will require you to manually lock and unlock your credit report when filing for new lines of credit, like a rewards card or a house.

5. Monitor all accounts closely

Finally, after you have changed your passwords and placed a fraud alert in your name, the last thing to do is closely monitor your account for any suspicious activity. A fraud alert and credit freeze will make it harder for thieves to open new accounts, though it does not guarantee safety to the accounts they may already have access to.

The Mindset of a Successful Woman

AMINA DEJI-LOGUNLEKO'S SUCCESS STORY

I am Amina Deji-Logunleko, wife to Deji, mother to Maryam and Abdulbarr, Independent Consultant and CEO/Principal Consultant at Auphysh Services Limited. I studied Industrial Chemistry at both undergraduate and master's degree levels at the University of Ilorin, Kwara State and the University of Ibadan, Oyo State in 1998 and 2003 respectively, while I earned a second master's degree in Oil and Gas Engineering from the Robert Gordon University, Aberdeen in 2008.

My journey into quality assurance and standardization, and subsequently my career, started upon getting employed as a Standards Officer by the Standards Organization of Nigeria (the National Standards Body of my country) in January 2003. The best thing that happened to me was being gainfully employed by the National Standards body in 2003 as I got the opportunity to attend loads of trainings, develop standards, as well as participate in a lot of activities that have greatly enhanced the much needed skills required to survive in the industry.

Becoming a certified ISO 9001:2000 Auditor in 2003 exposed me to the world of ISO Standards — a journey I have continued till date. I also earned certifications in a couple of other ISO standards, thanks to my former employer, the Standards Organization of Nigeria.

My years at the Standards Organization of Nigeria as well as my position as the Technical Secretary for THC 05 with the African Organization for Standardization had further exposed me to the world of ISO standards where I honed technical as well as auditing skills from among the best in the industry.

Participating in a number of trainings and meetings in different parts of the world further helped to enhance my knowledge and skills. These provided me the opportunity to learn from the best in the industry as well as maintain an enviable network. I had unconsciously sponsored myself to attend trainings within and outside Nigeria without knowing I was preparing myself for the task ahead. Auphysh was registered in November 2015, and its operations fully commenced in January 2017, two months after I had resigned from the Standards Organisation of Nigeria.

Taking the decision to resign from a paid job after about fourteen years where I had a lot of potential for growth, was a very difficult one.

I had discussed with my spouse, my siblings, a couple of close associates, a very close elderly friend (who is instrumental to a greater part of who I am today), and an immediate former boss. I intentionally did not discuss it with a number of my other former bosses because I wanted to take a decision solely based on my convictions and did not want a situation where anyone of them would make me change my mind.

Taking this step was made easier as I was exposed to a number of opportunities by being a PECB Certified Trainer. I had always desired to be a renowned businesswoman and fathomed that remaining in paid employment would not make it an easy feat. At some point, I had to take a decision to quit my job without knowing what laid ahead of me.

I was convinced that leaving a paid job to venture into the unknown could only bring either success or failure. Staying back would never make me know what the outcome would be.

It took me about a year of praying and fasting (February — September 2016) to ensure I was headed towards the right direction with the challenges I knew I was bound to encounter. It was not a year of preparing myself for the business world neither was it to acquire any business knowledge and skills. All I knew was that I needed the conviction that I was headed in the right direction and all other bits would fall in as time went on, or so I thought.

I attended the PECB Certified Advanced Audit Techniques training course in Stockholm, Sweden, in June 2016 and became more convinced that my decision to leave paid employment was for a greater good.

PECB was offering two things in one — the opportunity for me to become an independent auditor as well as the opportunity for me to run my own business.

The first had already been achieved and when the chance for the second opportunity came, I had to wait until after I had left paid employment before taking it.

The early years were tough, as in tough with capital letters. I had to learn almost everything related to the business

industry on the move while ensuring I maintained the home front. My family had supported my dream and I had to ensure I did not let them down as well as had to make the time to be with them. I had to give up trips that required attending training sessions in person. I needed to do all I could as well as develop grit. There were late nights of voracious reading. There were eureka moments when I had to write down solutions, draw up plans, permutate and combine a lot of numbers and times when I had to draw up a To-Do list for each day hence the need to have books at the bed side as well as writing materials. There were times when I unconsciously worked while sleeping, while other times when I would meditate and map out my strategy to achieving unprecedented success.

I had encountered a couple of challenging times during my career. The first was shortly after I resigned and I had advertised for a training course which was scheduled to run in December 2016. I had not considered the season neither had I mastered consumer patterns. I used social media and traditional media to seek attendees but I was not able to get the required class size. Eventually, I had to cancel the class. There were times when I ran some training courses with a few candidates. For those times, I was unable to receive the Trainer Fee because all I was after was to break even. Another time was when candidates canceled at the last minute or they had made the installment payments and did not abide by the terms and I had to monitor the debtors list. Another challenging time for me was when the foreign exchange rate soared and I was at my wits end. I was forced to deep my hands into personal savings in order to run a few training courses as it was increasingly difficult to manage with the earnings from course fees. The most challenging time was when sales were extremely low and all of a sudden I seriously considered heading for a paid job. I was not sure why all the pieces were not adding up and it seemed that my qualifications, certifications, and experiences were not making it happen. At this point, getting a job was not even forthcoming and I decided to face the problem head on and restrategize. I met with a couple of mentors who explained that the curve was normal and all I need to do was to hang on, go back to the drawing board, and seek new ways in which to create and launch new products.

One thing I knew was that ISO standards were in my DNA (Auphysh tag line) and I had to muster the courage not to give up as well as hone the business skills I required while the business was in a trough.

The bottom line became extremely important, business knowledge was critical, and increasing my client database was a key objective. SWOT analysis taught me what I needed to work on with respect to weaknesses and threats that were glaring at me, internal and external issues such as capability and competition respectively, coupled with interested party requirements that had to be considered during risk analysis in order to come up with controls.

> **Above all, I knew I could not give up. Determination was the rule of the game and I was not about to lose out.**

I had to attend classes both physically and online, read more, hone skills from the Zimba Women and Cherie Blair Foundation program mentors as well as mentors from the industry in order to bridge the business gaps. I also had to bring a uniqueness to my way of delivering training and consulting projects, which is a non-one size fits all approach, as well as by way of implementing the PDCA cycle for all projects.

Albeit my next to zero business skills, PECB provided me with the platform to grow amid a tough business environment as well as expand my offerings to clients and intending clients and provided so much back end support. They offered webinars to improve my technical skills, supporting marketing tools such as flyers, and published Auphysh training events on social media to improve sales. I also had access to a pool of Trainers and Consultants, and resources which I could use to expand my knowledge, improve training experiences as well as give real life examples to clients.

With the gathering of business knowledge and skills and a strengthened strategic plan, I drew up a number of plans to improve our sales trajectory and periodically monitored the entire process to ensure my team and I were in alignment with the strategy.

> **The visibility made possible by PECB was a major life saver. I was able to showcase my skills and people were able to see what I had to offer.**

This opened many doors inclusive of opportunities of handling projects for multinational companies. Auphysh, in about three years, had become a brand to reckon with.

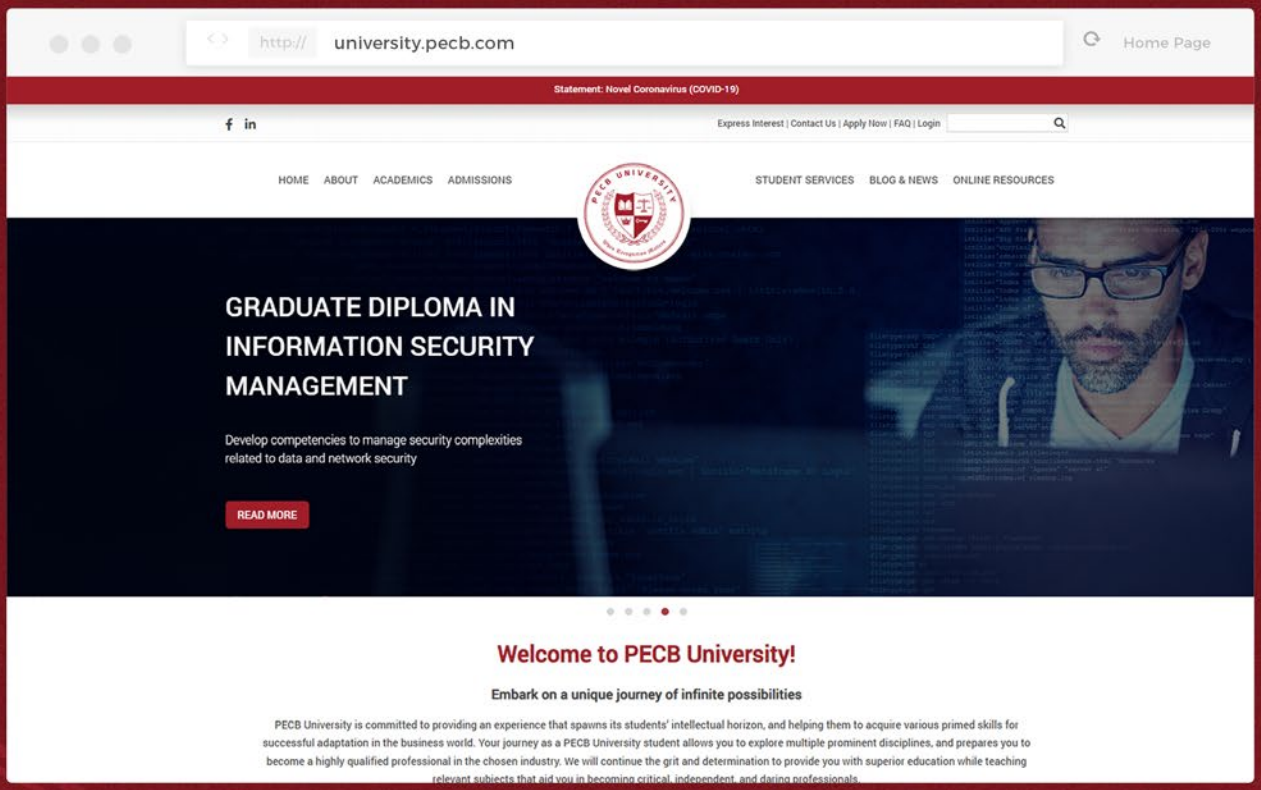
I have been able to maintain an enviable profile, thanks to access to a multitude of online training courses offered by PECB, which has opened a number of unexpected opportunities.

About three years down the line, I cannot help but give thanks to God almighty for all I have achieved so far. As the dreams I had so far have become true, I never rest on my oars and strive to always be the best in all I do and hope someday to consult or be a part of the consulting team for the fortune 500 companies. I most definitely will leave my footprints in the sands of time.

I cannot say that my success story has ended because I am Auphysh. I believe more wins lie ahead of Auphysh and I, because "a goldfish has no hiding place."

A SCREEN NEARER TO YOU

PECB UNIVERSITY WEBSITE LAUNCHED!



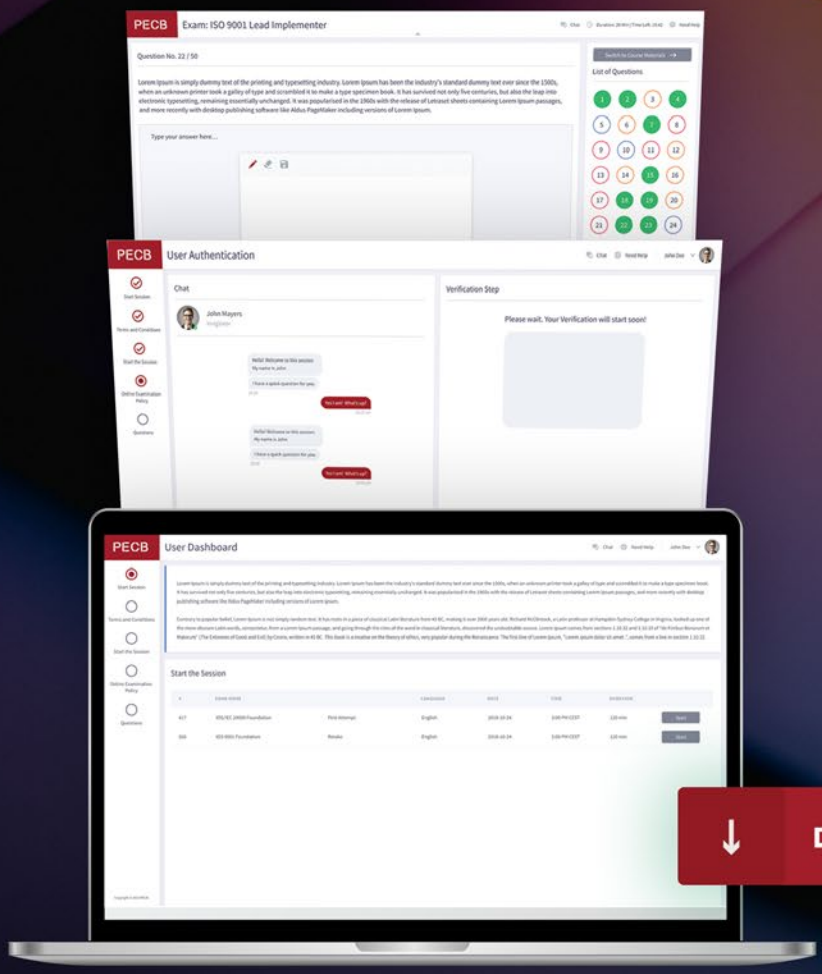
As of March 2020, PECB University has launched its new and improved website, offering a fresh look and user-friendly navigation system, which will serve as a student information hub and resource center to meet all of your needs.

Candidates who are certified by PECB are eligible for a PECB University Graduate Certificate.

university.pecb.com

We are excited to welcome you to the new version of the PECB Exams application, built using the latest design trends.

- Brand new design
- Access to training course materials and notes
- New drawing tool for diagrams, graphs, and formulas
- Automatic software updates
- Improved software security



DOWNLOAD NOW

SIMPLE, FAST, FREE

PECB advises you to avoid traveling nowadays due to the ongoing COVID-19 outbreak. However, make sure you add this incredible destination on your travel bucket list.

EXPLORE AUCKLAND

THE CITY OF SAILS

"New Zealand is a land of immigrants, beauty, and valor. The beauty, culture, and nostalgic history of Auckland can hypnotize anyone, and I was one of them. I moved from Pakistan to Auckland in 2008. A visit to Auckland was sufficient for me to decide to live, work, and enjoy life here. Auckland has a subtropical climate, and always sprays rain on people. Whenever you walk in the streets, you will see people greeting you with a smiling face. I call them peopole of God.

Rated as the third most livable city in the world, Auckland is the largest city in New Zealand and home to more than a third of the entire country's population, and is the main arrival point for many international visitors. The city hosts a combination of metropolitan delights and natural landscapes and will sure keep you captivated.

Getting around Auckland

Auckland's international and domestic airport terminals are only 45 minutes from downtown, and you will get the salty whiff of clean air as soon as you land. There are regular transfers, private transport, and busses available 24 hours, seven days a week.

The public transport is a great way to get around. You can take the train, bus, or ferry for visiting the inner or wider region, attractions, shopping centers, and entertainment points. The main transport hub where many bus and train journeys start and finish is Britomart. If you are planning to stay for a longer period of time around Auckland, you can get an AT Hop Card, which is a prepay smart card to get discount for travel on trains, ferries, and busses around Auckland.

The link bus services are very convenient, run very frequently, and get you around the city center and inner suburbs by starting from just 50 cents.

Besides that, you can hire a car, motorhome, or motorbike. In Auckland, you can legally drive for up to 12 months per visit, with either a current driver's license from your home country or an International Driving Permit (IDP). The only disadvantage may be that in New Zealand, people drive on the left, and some might need a bit of adjustment.

Accommodation

Hilton Auckland — With a unique design and ideal location with panoramic sea views, located 300 meters out to sea on Princes Wharf, Hilton Auckland is home to a variety of shops, restaurants, bars, and is within five minutes' walk from the main shopping precinct, the Viaduct Harbor, the ferry terminal, the museum, and the heart of the city.

There are 177 spacious designer-furnished rooms and 10 suites who all have private balconies and decks. You will get a fabulous view of the harbor, and an outdoor lap pool underwater viewing window. For a fine dining experience, the hotel's fish restaurant offers a menu of fresh seafood from the morning's catch throughout the week by New Zealand master chef Simon Gault. The prices range from $350.00 - $1600.00 per night. The hotel has also its business center and meeting rooms, making it very convenient for organizing any business event or conference.

Crowne Plaza Auckland — With a selection of 352 rooms to suit your needs, Crowne Plaza Auckland is located in the heart of Auckland, and it is just a short walk away from the city's attractions such as the Sky Tower, the Civic Theater, and Aotea Center. You can relax during your stay in one of the rooms that come with amazing view and different sizes: Superior Rooms, Deluxe Rooms, Executive Club Rooms, and Suites. Club guests will have exclusive use of the Club Lounge with spectacular views over Auckland Harbor and great benefits like complimentary continental breakfast, and evening drinks, and canapes.

The guests can use all the facilities of the hotel including 10 event spaces for business meetings, conferences, or any other event. In addition, Aria Restaurant and Bar offers delicious food, where you can also watch your breakfast get cooked in-front of you at the live cooking egg station. Whether you decide to use the fitness center, relax in the sauna, club lounge, or business center, Crowne Plaza will ensure you have a good night's sleep with its Sleep Advantage program so that you wake up for a productive day.

IMG: FLICKER / ITRAVELNZ ©

Pullman Auckland Hotel

IMG: FRANKLIN38 ©

Franklin 38

Pullman Auckland — Pullman Auckland Hotel is one of Auckland's largest five-star residential and conferencing hotels with sixteen event venues. This hotel that offers calm, comfort, and convenience for its guests, is situated in the heart of the city with views of the center, harbor, and the historic Albert Park.

Residences by Pullman have won leading awards as "Luxury Apartments of the Year Auckland New Zealand" and "New Zealand Leading Hotel Residence." To have a memorable culinary experience, Tapestry dining is situated on the Lobby Level of the Hotel, and is open seven days a week from 6 am to 10:30 pm. Featuring a unique selection of international flavors and techniques using a fresh locally sourced produce, a meal at Tapestry Dining is perfect for any occasion, business meeting, or simply a casual night out with friends or family. Guests can enjoy a massage with heated stones and exotic wraps after working out at the fitness center. The restaurant has a show kitchen, while the bar offers an extensive wine list.

Stamford Plaza Auckland — One of the finest accommodation's that the city has to offer, Stamford Plaza Auckland rooms surround you with charm and sophistication. Located in the center of Auckland, within close proximity of Queen Shopping District and Britomart Transport Center, the hotel also offers many recreational opportunities, including spa tub, sauna, and an indoor pool.

The rooms (286 in total) are air-conditioned featuring refrigerators and minibars, in-room free WiFi, and LED TVs. Two restaurants, and a business center, including 10505 square feet of space for conference space and meeting rooms.

Franklin 38 — A very quiet place to relax, Franklin 38 is a new Luxury Boutique accommodation with four guest suites, all decorated with contemporary architecture materials and furnishings and individual character. Located in Freeman's Bay, just 15 minute walk to Auckland Central City, a heritage area with Victorian villas.

Recently renovated, this place has maintained its original period features. The suite has a wonderful view of the city and upper harbor which you can enjoy from your room or the verandah. All suites have their own tiled ensuite bathrooms with underfloor heating, heated towel rails, NZ natural toiletries and luxurious towels and linen. You can have breakfast prepared by the hosts starting from homemade breads and baking, to eggs of your choice, salmon, and even vegan or vegetarian options are available.

Attractions

Auckland museum — Whether you have an hour spare or the whole day, Auckland Museum is the best stop to gain an insight into New Zealand's compelling story, its culture, and heritage, and war. The museum has served as a place of remembrance for those who have sacrificed their lives at war.

For more, there are a thousands of items on display, including Māori treasures such as rare carvings, whole buildings, and the last great Māori war canoe carved from a giant Totara tree with daily cultural shows.

Wine tasting — Known as New Zealand's "Island of Wine," Waiheke Island is considered the jewel in the Haruaki Gul's crown. Only 35 minutes from Auckland, there is nothing like taking a ferry over to Waiheke, for all of those who love a glass or two of good quality world-class wines, stunning views, and good food. This is the perfect place to escape to for the day, as the architecture of the place is also a must-see.

A native bird of New Zealand, the flightless Takahe.

The Hauraki Gulf — On the doorstep of Auckland city, the Hauraki Gulf is home to a multitude of emerald islands that you can journey to by ferry. The gulf waters are ideal for a cruise. Besides the Waiheke Island, you need to visit the wildlife of sanctuary on Tiritiri Matagi, a place of endangered birds, including the rare Takahe. The summit of Rangitoto, the black lava volcanic island is also a must-see place, which you can visit with a kayak. Discover the historic Manison House on Kawau Island, once home of Governoe George Grey, and sunbathe and swim at Motuihe Island.

Last but not the least, embark on an adventure on the Great Barrier Island, a totally different world from your typical holiday.

In its coastal setting with verdant surrounding landscape, Auckland is a city in which the cuisine is driven by exceptional local produce that is defined by the seasons. But as one of New Zealand's most exciting hubs, it also benefits from the culinary creativity that comes from international influence and a hunger for world-class dining experiences.

Restaurants

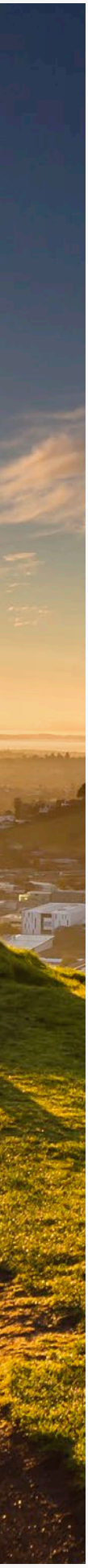
Kazuya — The culinary art of European and Japanese fusion at Kazuya is a feast for the eyes. Kazuya chef uses the unique process of low-temperature long duration roasting for meat, and also traditional Japanese methods for preparing fish so that the guest have a surprising and memorable dining experience. At Kazuya you have fixed-price meals, dégustation options, craft beer selection, and much more.

The Grove — The Grove is one of Auckland's top restaurants, located in the heart of the city, in Saint Patricks Square next to the historic Saint Patrick's Cathedral. Here you can enjoy a unique approach to food and service, of New Zealand and French influence cuisine with degustation dining that changes frequently with seasonality and market availability. The menu changes frequently as it focuses on finding the freshest local ingredients each season; however, specialties like terrine of honey bugs and ripe tomatoes with fennel and tarragon, and Mooloolaba king prawns with samphire can be found at all times. New Zealand and international wines will be served to you for enjoying an amazing journey into the world of wine too.

Sidart — Offers contemporary Indian fine dining using only New Zealand produce. Besides the beautifully presented and tasty dishes here you can find exceptionally good value wine. The Chef's Table experience offers a closer look into the kitchen. Here you can watch dishes being created, and be guided through the menu by our chefs. This is our most exclusive dining experience, starting with a glass of Champagne on arrival, before taking you on a journey of flavors with our Full Discovery Menu. The Chef's Table is available for four to five guests.

The Sugar Club — Located on floor 53 of Auckland's iconic Sky Tower, this seems like the perfect place with fine food, creative cocktails and a well-curated wine list, and a 360 grade spectacular view of the city. The elegant Art Deco-inspired fine dining restaurant and accompanying cocktail bar is the setting for meals of Asian and European fusion cuisine by lauded chef Peter Gordon that champions New Zealand's seasonal ingredients.

Bracu — For a more relaxed meal, Simunovich Olive Estate is also home to a unique restaurant, Bracu, which takes its name from the Adriatic island of Brac, the place where the olive growing tradition began. The menu is on the traditional side with some innovative twists and a commitment to fresh seasonal produce. A meal here is well worth the 40-minute drive from Auckland. The food is cooked from the Estate's own gardens and passionate local producers while you relax on the all-weather verandah or inside the magnificently restyled Kauri villa.



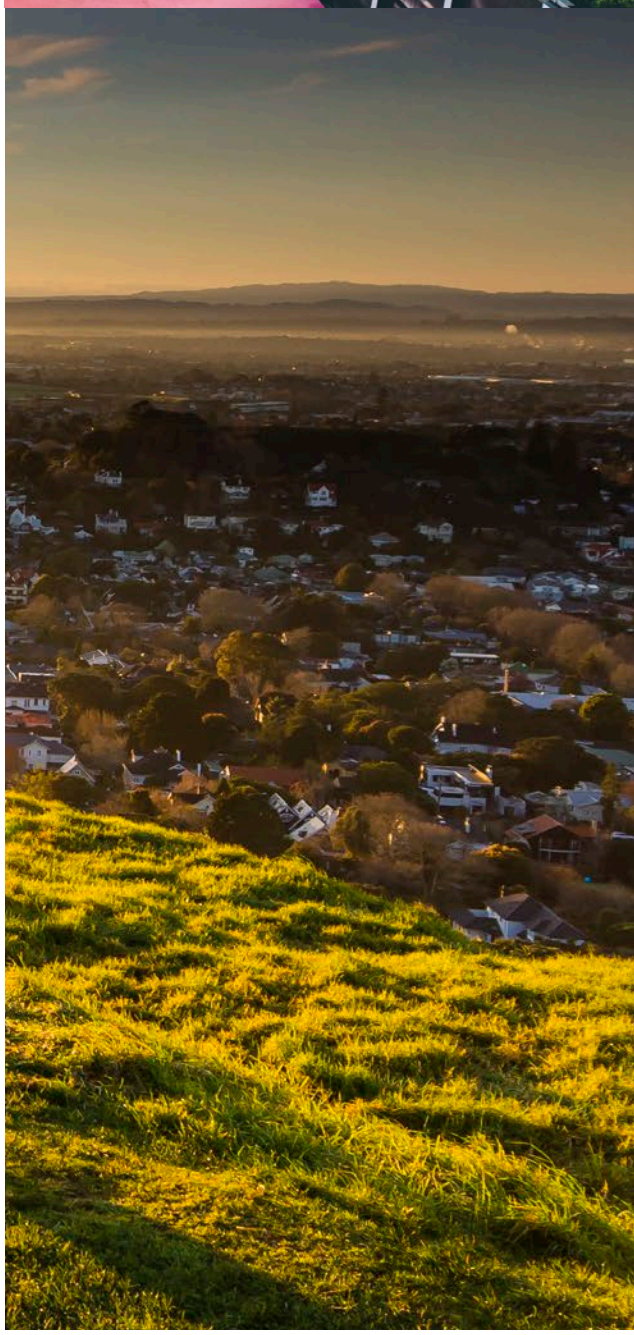
Business

Auckland generates nearly 40% of the country's GDP and is a major skills, production, and research and development hub for Asia-Pacific. Besides being strategically located, Auckland is also connected, as the business hours are complementary to key regional markets and markets in Europe, Britain, and the US east coast. With the country's largest airport, seaport, and freight operations, Auckland is also the main logistics hub in and out of New Zealand.

Auckland is considered to be the economic center of New Zealand and an innovation hub of Asia-Pacific. According to the IFC World Bank — Doing Business Report 2020, New Zealand was voted, for the fourth year, the first out of 190 economies in the world for ease of doing business. This evaluation is done based on a number of indicators such as "starting a business" to "resolving insolvency" and "protecting minority investors." For more, New Zealand has been ranked as number one for "ease of starting a business" by the Doing Business Report, for the twelfth year in a row.

There are available websites and resources that make it simple to register companies and help understand the steps and obligations to starting a business. For more, it is very easy to run your training courses in Auckland, as the best hotels are there to accommodate your requirements in order to have an immaculate training.

All these factors make New Zealand, and especially Auckland, a favorable place to start thinking of making business: a business-friendly and stable environment coupled with an easy lifestyle and a great place to raise a family.



About the Author

Rizwan Ahmad
Director at Cianaa Technologies

Dr. Rizwan Ahmad is an information security professional with more than 20 years of experience. He is currently the Managing Director of Cianaa Technologies, a certified QSA for PCIDSS, certified ISO/IEC 27001 Senior Lead Auditor, and also possess attorney law certificate. He is an expert for information security and produces work in New Zealand standards. He also holds and represents New Zealand in joint IT Governance committee IT-30. He contributes to object management group, ITU-T, and ISO internationally.

Cybersecurity Maturity Model Certification vs. NIST Framework Models

BY ARDIAN BERISHA, PECB

After you finish this read, the first key takeaway that you should acquire is that when you read through the CMMC requirements, you can notice that the model is a more "good IT hygiene" approach, meaning that its practices are associated with people, processes, and technology. Hence, the more mature your IT as well as cyber practices are, the less of a threat you pose from negligent acts that are directly associated with implementing and managing technology solutions. If your organization does not possess a valid CMMC for a certain level, you result in not meeting the minimum requirements to bid on or even participate in a certain contract from the Department of Defense (DoD).

The second key takeaway that you should obtain is that CMMC can be considered as a tool from the US Government in terms of using it to implement a tiered approach to audit contractor compliance with the NIST framework (based on five specific levels of maturity expectations). Since January 1, 2018, DoD contractors are required to comply with NIST 800-171. In the past two years, DoD dealt with a very low rate of NIST 800-171 compliance in line with the Defense Industrial Base (DIB). At that point, CMMC was initiated to adjust that systemic issue of low rate compliance by both primes and their subs. In addition, when NIST 800-171 was firstly launched, the DoD did not accept any form of third party audit for the NIST compliance, and that is exactly what CMMC was launched to do, ensure compliance with the NIST framework.

Breaking Down Technicalities — CMMC vs. NIST Framework Models

Even though CMMC and NIST SP 800-171 are linked in the technical nature and share a joint goal — the protection of Controlled Unclassified Information (CUI) — they are not the same. Here are the main descriptive differences and similarities between CMMC and NIST:

1. CMMC primarily originates from NIST 800-171 which itself has the same mapping to the previous NIST 800-53. Adding to that, CMMC adds a few more controls in the new NIST 800-171 and most of these controls are based on the existing NIST 800-53 controls. Thus, only the CMMC Levels 4 and 5 controls fall outside of the previous NIST 800-53.
2. Complying with the current NIST SP 800-171 requirements would presumably fulfill the Federal Acquisition (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) requirements too.
3. CMMC has five levels of maturity compliance, which depend on the sensitivity of the information in any contract that is given, whereas NIST SP 800-171 has only one basic level with an additional level of supplement for advanced protections (NIST SP 800-171B).
4. CMMC is a contractual requirement, whereas the NIST framework is a regulatory requirement.
5. CMMC requires a third party compliance assessor while the NIST framework only requires self-documentation and attestation.
6. NIST framework assesses the cybersecurity controls of your organization, on the other hand, CMMC also assesses the company's maturity of cybersecurity practices as well as processes.
7. Last but not least, the CMMC framework combines and unifies a variety of cybersecurity standards including, but not limited to: NIST SP 800-171, NIST SP 800-53, ISO/IEC 27001, ISO/IEC 27032, AIA NAS9933 into one merged comprehensive cybersecurity standard.

CMMC controls

▼	**CMMC Level 1**	**17 controls**	
▼	**CMMC Level 2**	**72 controls**	**(includes Level 1 controls)**
▼	**CMMC Level 3**	**130 controls**	**(includes Level 2 controls)**
▼	**CMMC Level 4**	**156 controls**	**(includes Level 3 controls)**
▼	**CMMC Level 5**	**171 controls**	**(includes Level 4 controls)**

What are the costs of noncompliance with NIST 800-171 and Cybersecurity Maturity Model Certification (CMMC)?

Termination of contract: It is rationally expected that the US Government will terminate contracts with its contractors in case of noncompliance with DFARS/NIST 800-171 regulatory requirements.

Criminal fraud: If an organization claims that they are compliant knowingly they are not, that is a direct misrepresentation of material facts. Hence, this is considered as a criminal act as any other activity intended to deceive through a false claim of some fact, which then results in the legal detriment of the person or the organization who relies upon the false information (False Claims Act).

Contract lawsuits: Prime contractors, as well as subcontractors, could be exposed legally to contract breach lawsuits. The instance of a breach, in this case, can be for a DFARS/NIST 800-171 would be regarding the negligence on behalf of the accused party by not being able to maintain a specific code of conduct.

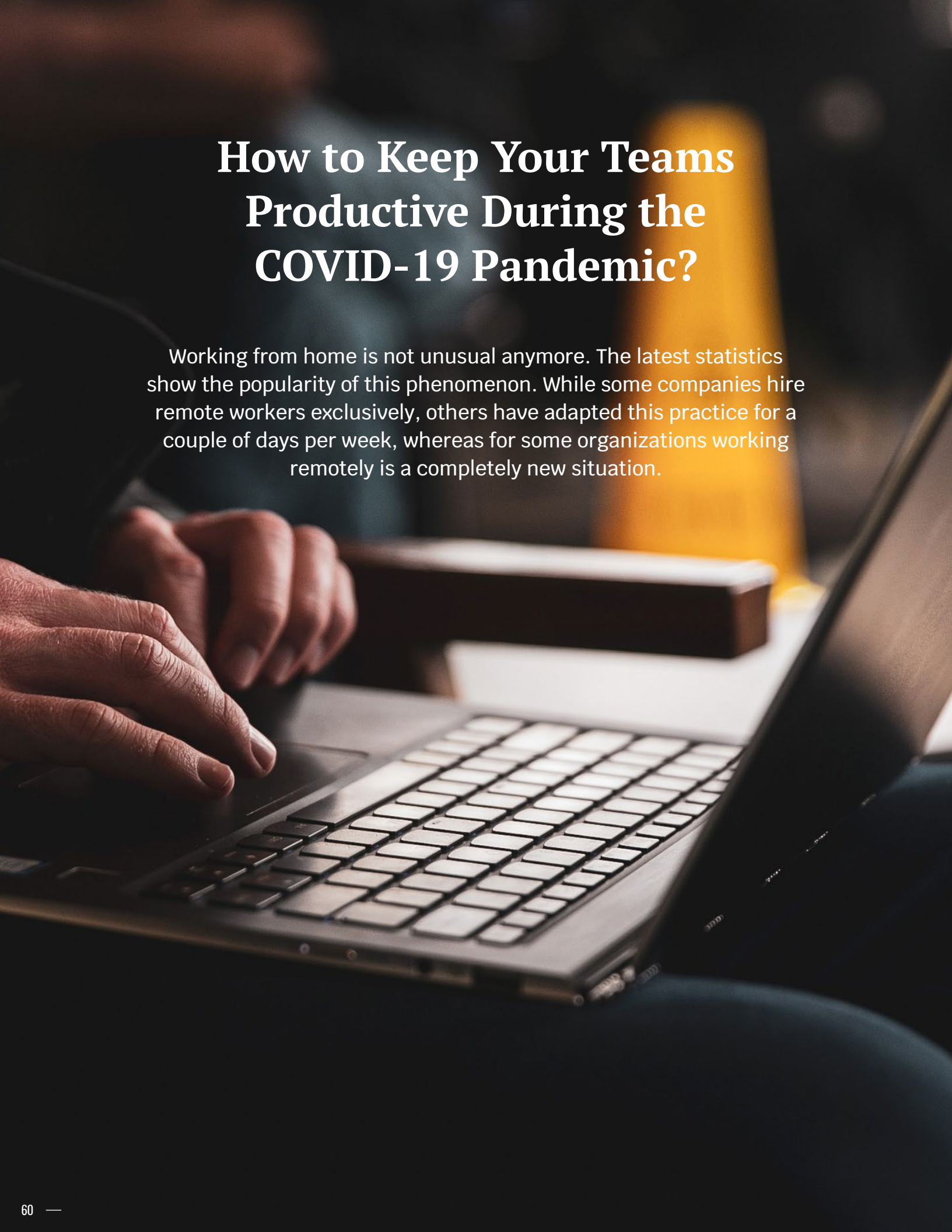
As a final thought, the responsibilities that are linked with CMMC compliance spread far beyond just your cybersecurity team. Having a clear idea of who manages CMMC controls can payoff significantly as you gradually prepare for your CMMC audit since these are not principally "cybersecurity" controls and many of them are managed by the business process owner or the IT asset managers. We can argue that data and process owners and IT managers have more control compared to the cybersecurity team when we take a look at the realistic roles as well as responsibilities for CMMC controls, so this is a highly significant part to keep in mind while addressing CMMC audit preparations with your stakeholders.

All in all, in most cases, it is highly recommended that the best course of action that you can take is to retain a trusted third party to assess, mitigate, as well as construct the CMMC certification process which would also help you comply with the NIST regulatory requirements. Moreover, by doing so, you would not only attest compliance but also maintain the basic cybersecurity position during the life cycle of the certification and recertification too.

One of the most crucial steps towards successfully completing an audit with the controls mentioned in this article is to have appropriate documentation in place, which you can use as a real proof that you are doing what is required.

How to Keep Your Teams Productive During the COVID-19 Pandemic?

Working from home is not unusual anymore. The latest statistics show the popularity of this phenomenon. While some companies hire remote workers exclusively, others have adapted this practice for a couple of days per week, whereas for some organizations working remotely is a completely new situation.



As the number of people working from home is expected to grow exponentially in the face of COVID-19, many companies have prioritized the safety and protection of their employees by having everyone carry out their tasks from home. However, due to the sensitivity of the situation, another layer of stress is added. This is when companies' support and assistance comes to place.

Take a look at some ways you can make sure that your employees remain at the top of their game and keep being productive while working from home during this period of uncertainty.

Make sure that your employees have the right equipment

This is probably the primary and most important aspect of increasing productivity while working from home. Equipping your teams with proper communication channels and new technologies, allows both the employees and employers be on the same page. In order for tasks to be carried out efficiently, employees also need to have proper access to internet, and the right devices to work and complete tasks (e.g., computers, tablets, laptops, internet access equipment).

Provide access to all the information they need

Besides coronavirus-related materials, your employees need to have access to other information that is crucial to perform their daily tasks. That is why you need to ensure that the folders containing any type of information needed are easily found and accessible by everybody at all times.

Internal communication

Social isolation can greatly impact your team, so it is important you reinforce communication. This can be done by sharing essential and timely information with employees. As you adapt your processes, strategies, and policies due to the pandemic situation, make sure you share them with the entire company. Thus, your employees will feel more involved and connected to the entire team.

You can also develop a plan for communication and provide the tools and software needed for team interaction. Make it a habit to continuously share informative materials related to the virus, the measures to be taken, and the best practices to be adapted so as employees stay safe even at their homes. Above all, your employees need to be informed first about any pandemic-related decision that the company takes.

Most crucially, you need to inform employees on network security, protection of confidential information, network capabilities, and encrypted access to the company's network.

Encourage dedicated workspaces

A very important aspect of being productive while working from home is the space one uses. You should encourage employees to have a safe and dedicated workspace, free from distractions, where they can focus on their work and do not deviate from productive work hours.

Give emotional and steady support

In order to have alignment of goals and tasks, as well as improve communication across teams, make usual check-ins through video calls or texts. By having online daily meetings, your team can talk about what they have achieved the previous day, what they want to achieve for the day ahead, concerns, ideas, and so forth. Keep in touch with the teams, ask for suggestions, and discuss the progress. You can use these calls to simply keep their spirits high. Also, support them by asking for whatever they need while they work from home.

Advise employees on taking care of their mental health and encourage them to prioritize their physical health. Tell them to get up, stretch, and refocus during short breaks. This can be as easy as sending out a daily reminder on the communication channels you use or via email telling your team to get up for 15 minutes.

A change of working environment can lead to increased productivity for some, but on the other hand, can lead to a dip in productivity for others. As this is a stressful situation for everyone, extend some grace to yourself and your teams by helping them to be more productive, have an improved mental health, and be more creative in their thinking and work.

Keep learning

As the health crisis caused by COVID-19 is reaffirming the need for access to learning resources, everyone should make use of this time to pursue new interests or upgrade their competences. This could be easily achieved by attending, for instance, any of the many PECB training courses that are going to be delivered online, finely tailored to meet your needs.

PECB e-Learning Dynamic Training:

Your Modern Destination for Learning!

Learning has never been e-asier! Learn and become certified at the comfort of your home!

Stay tuned...


1:22/11:43
PECB

PECB advises you to avoid traveling nowadays due to the ongoing COVID-19 outbreak. However, make sure you add this incredible destination on your travel bucket list.

WHEN ALL THE ROADS LEAD
TO THE ECLECTIC CITY OF MALMÖ...

The Grandeur of Malmö, Sweden

BY HEAR IT FROM LOCALS

Malmö is a coastal and largest city of Skåne County in southern Sweden. It is also the third largest in Sweden, after Stockholm and Gothenburg. Lying at the eastern end of popular Öresund bridge (largest road and rail bridge in Europe), this city is closer to Copenhagen in Denmark than Sweden's capital Stockholm. Malmö is one of the most diverse and multicultural cities in Sweden, credit for which also goes to the universities of Malmö and Lund. It has a young population with almost half of them under the age of 35. The Swedish brand IKEA has most of its' headquarter functions based in Malmö and after the integration with Copenhagen brought by the Öresund bridge in 2000, the city has seen some major transformation.

Winters in Malmö are about snow, ice, and freezing temperatures but much milder than the cities in the north. However, if you are visiting Scandinavia for northern lights, consider visiting Malmö for its annual Christmas markets.

When to visit Malmö

The best time to visit Malmö is for sure during spring and summer time i.e., from April to August. We have a central beach just a short walk from the inner city, lots of nice parks to hang out in, many restaurants and bars with seats outside, beautiful nature just 30-60 minutes away, etc.

Transport

There are special flight buses that take you from the airport to the central parts of Malmö. The other option is taxi, but since the flight buses go often, I suggest you take one of those.

When you want to travel around in Malmö you can use city bikes. Malmö is not that big so you can take the bike anywhere. It is also nice to take a bike tour to the countryside of Malmö. Malmö is a great city to bike in!

We also have buses that can take you everywhere, green buses are for journeys within the city, while yellow buses take care of regional journeys. Use trains if you want to visit Copenhagen (just 30 minutes with train) or other cities around Malmö. You can check Skånetrafiken for information about both buses and trains.

Top four must visit places in Malmö

Pildammsparken

Situated right in the city center, Pildammsparken is a beautiful, big park of woodlands, perennial gardens, and a lake which once supplied the entire city with water. Spread out in an area of 111 acres, the park is an ideal location for hanging out with friends, power walking, or running. The park also has an outside gym, jogging track, ponds for bird watching, and boat riding. Its iconic bridge is a wonderful piece of engineering and architecture. The park is free to enter and stays open 24 hours a day, every day of the year. If you are visiting Malmö in the warmer months, attend one of its outdoor events organized in the Pildammsteatern amphitheater.

Turning Torso

Designed by the Spanish architect Santiago Calatrava, Turning Torso is a residential building with 147 apartments of slanting windows, curving walls, and oddly shaped rooms. Inspired by a sculpture (Twisting Torso) and built using nine stacked cubes, Turning Torso is the tallest building (623 feet tall) in Sweden and entire Scandinavia. It is located in Västra Hamnen, and is only two miles away from the Malmö Central station. They also sometimes organize guided tours in the building, keep an eye on their website to know when.

Malmö Saluhall (Malmö Food Hall)

Is a culinary heaven brought to life by siblings Nina Totté Karyd and Martin Karyda. This refurbished warehouse is a perfect place to eat and shop locally produced food with its many restaurants and boutiques. You can also find Scandinavian crafts and flower arrangements there.

Bar deco cinema Spegeln

Spegeln is a cinema with a bar deco salon and a bar where you can order food and drinks that you can enjoy during the movie. Get your noncommercial movies fix here! Movies shown here are generally in Swedish but have English subtitles.

You can get a nice view from the roof top bar and restaurant Kasai in the Sky and also Malmö Live's sky bar which is located at 25th floor of Live Hotel. Panoramic city views from all sides is the main attraction of this sky bar.

IMG: MALMO SALUHALL ©

Day trips for nature, culture & history

Apart from crossing the Öresund Bridge which is Malmö's most remarkable sight, you must also check out the following:

Bokskogen in Torup

Bokskogen in Torup is around 20 kilometers from the city of Malmö and can be reached within 25 minutes. It is a beautiful big forest with lots of running and walking trails. It is a very popular place to relax and hang out. Torup Castle was completed around 1540 and is one of the best preserved medieval castles in Sweden.

Österlen

Österlen is a beautiful south eastern part of the Swedish historical province of Skåne. It is known for its fantastic scenery of rolling fields and fishing villages. There are many cozy cities in Österlen to explore. It is a tourist destination with its beautiful environment, many cultural monuments, small towns, and farmlands. During spring time you can visit the Österlen art festival.

Lund

The town of Lund is known for its historic and impressive Roman cathedrals. It is also well-known as a university city. Lund University is a public university, often ranking among the world's top 100 universities.

The squares like Lilla Torg (small square) and Stortorget (large square) attract a lot of tourists. Further down from Lilla Torg is the city area Gamla Väster located between Stortorget and Kungsparken. Like the popular Gamla Stan in the city of Stockholm, Gamla Väster is very cozy and colorful. However, in Malmö's Old Town, there are almost no stores. The charm of this street lies in its small historical buildings, art galleries, boutique hotels, and cafés.

Holidays and events

Konstrundan Österlen

Konstrundan is an art festival with art exhibitions and local artists. It takes place every year during Easter. Hundreds of artists, who are members of ÖSKG, open their ateliers and galleries for visitors at the same time, all over Österlen. You can recognize artists from ÖSKG by their road sign which is a popular yellow and orange circle. Buy art and products directly from them during this event which goes on for ten days.

Malmöfestivalen

Is a city festival that takes place in Malmö with lots of food stalls, concerts from famous Swedish artists, music, culture, and much more. It is actually Sweden's oldest festival, rich in traditions and for every generation. The festival is organized for one week every year in August, right in the heart of the city.

Shopping

Möllan is a trendy and an ethnically diverse neighbourhood of Malmö city. It has many second-hand shopping boutiques. Read this guide by Blonde-Gypsy to know more about Möllan.

If you want to shop from the big chains you can go to the big mall Emporia at Hyllie which lies between the city and Copenhagen airport. One of the biggest shopping centers in northern Europe, the Emporia mall houses two hundred shops.


IMG: FLICKR/MARIA EKLIND ©

Food

Malmö is the most diverse city in Sweden with lots of restaurants and food from all over the world. I like the tapas restaurant Vibliotek and the Mexican street food restaurant — Eatery Social.

> **Typical Malmö and Sweden food are egg cake, meatballs, and herring.**

You can also use the "Karma" app for food delivery or orders. In Sweden, Karma has over 250,000 users and more than 1,000 eateries which offer their surplus food at much lower rate to minimize food waste. Among them are groceries giant Hemköp, Scandic hotels, Wayne's Coffee, and many more. Through this app you can check on the nearest places available, place your order, pay, and pick up later. However it is only available at Apple's store in Sweden and UK.

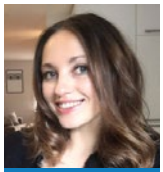
Cultural centers for art, drama & music

Malmö Konsthall is one of the largest art galleries in Europe built as an open space consisting of wood, glass, and concrete. It has a huge art collection and is the ideal excursion for museum lovers.

Malmö is often considered as Sweden's best city for street art. During the Artscape international street art festival, held in 2014, artists from all around the world painted in Malmö. Artscape also ran a series of free workshops and invited the public too to participate. As a result the Seved neighborhood has brightened up with a number of graffitis, also Norra Sofielund and Möllevången. Check out this wonderful guide on street art of Malmö to know more.

Rent a bike, you can pay with card (almost) everywhere. Remember that Swedes are very good at English, so communication is not a problem at all. Malmö has something to offer for everyone, from old-world to modern cosmopolitan vibes, making it one of the most eclectic cities in Scandinavia.

About the Author



Maria Busck
Blogger

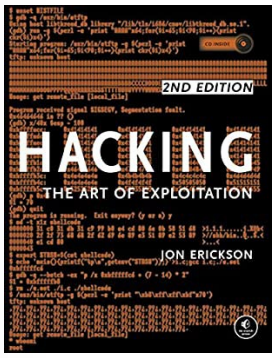
Maria Busck is a 30 years old Swedish blogger who originally hails from Hudiksvall in northern Sweden but now lives with her partner in the district Gamla Väster in Malmö. She blogs about everyday life, fashion, and hypothyroidism. Her hobbies are exploring new restaurants in Malmö, going for walks, hanging out with friends, attending different networking events, etc. Maria works with marketing and communications at an IT company and also runs her own company as an influencer.

Make Cybersecurity Books Fiction Again!

Curious to know what to look out for so that you do not fall prey of cybercriminals? Take a look at some cybersecurity must-reads that will help you develop your skills and support your career!

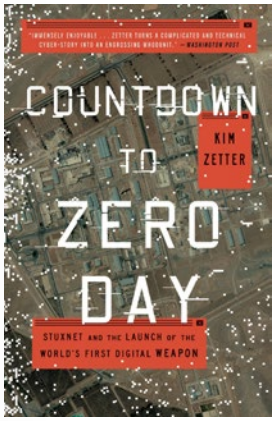
Cybersecurity is a quickly evolving industry, and new technologies are day by day bringing new threats that require new skills. The development pace is so fast that it is very difficult to step back and look for fundamentals. As you stay up-to-date with the latest reports on threats, data breach communications and cases, and developments in the cybersecurity field, it is time to deepen your knowledge as a professional and add these cybersecurity books to your library.

This selection of books are among the most famous and informative with topics ranging from history and law to penetration testing and social engineering.



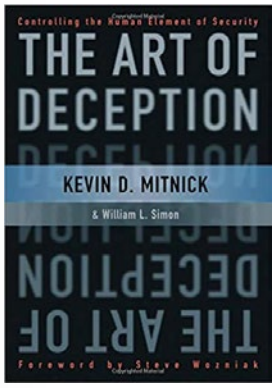
Hacking: The Art of Exploitation (2nd edition)
by Jon Erickson

The second edition of "Hacking: The Art of Exploitation" shows the art and science of hacking in a way that is accessible to everyone with the fundamentals of C programming from a hacker's perspective. It provides a holistic approach of problem solving, hacking techniques, programming, as well as network communications. For more, there is a LiveCD which provides a complete Linux programming and debugging environment (without compromising or modifying your operating system). Tons of knowledge you would not want to miss!



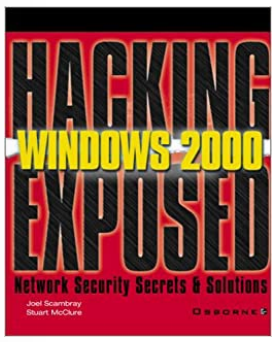
Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon
by Kim Zetter

Countdown to Zero Day introduced the world to the most sophisticated technology of the time and warfare in the digital age. Stuxnet proved to be unlike any other malware that had ever existed, since it was the first attack that reached beyond computers; it did not intend stealing information from the targeted computers but rather caused physical destruction on the equipment controlled by those computers, in this case an Iranian nuclear facility. Check out this book to learn everything regarding the planning, execution, and discovery of Stuxnet, the so known world's first digital weapon.



The Art of Deception
by Kevin Mitnick and William L. Simon

Are humans the weakest link in the security chain? Authors of "The Art of Deception" introduce us to the modern world threats posed by the human factor and how lack of vigilance can make even the most sophisticated security systems worthless. What is really intriguing about this book is its perspective, that of both the attacker and the victim. The book unfolds some true stories of successful attacks, narrated by the world's most famous hacker, Kevin Mitnick, the reason they were successful, what could have been done to prevent them, thus attempting to increase information security awareness.



Hacking Exposed: Network Security Secrets and Solutions
by Joel Scambray, Stuart McClure, George Kurtz

The Hacking Exposed series, also known as the bible of hacking, has become the ultimate reference for all security professionals. This book has proven to be a great resource for network securing providing guidance from experts renowned worldwide, with many examples of hacker attacks and tools. As it has been said "the best way to protect a system is to understand all the ways hackers can break into it," and Hacking Exposed is the right address for grasping such knowledge.

TAKE THE CHANCE TO ADVANCE

Status	Training Course	Language	
New!	Introduction to Pandemic Preparedness and Response FREE	English	→
Updated	ISO/IEC 27001 Lead Implementer	English	→
Updated	ISO/IEC 27001 Lead Auditor	English	→
Updated	ISO/IEC 27032 Lead Cybersecurity Manager	English	→
Updated	ISO 22301 Lead Auditor	English	→
Updated	ISO 50001 Foundation	English	→
Updated	ISO 14001 Introduction	English	→

Where Quality Meets Excellence!

PECB has been awarded the Best Cybersecurity Education Provider Gold Award (North America, between 100 – 499 employees) by the Cybersecurity Excellence Awards.

"We have been awarded the Best Cybersecurity Education Provider and the Cybersecurity Educator of the Year awards in the 2019 Cybersecurity Excellence Awards, and winning the 2020 award means a lot as it is a showcase of the continued hard work that the PECB team and network does every day to make sure that we provide the best quality of training materials and education. This recognition speaks for itself and we are extremely delighted to receive it."

Eric Lachapelle — CEO at PECB

For more information, take a look at the press release.

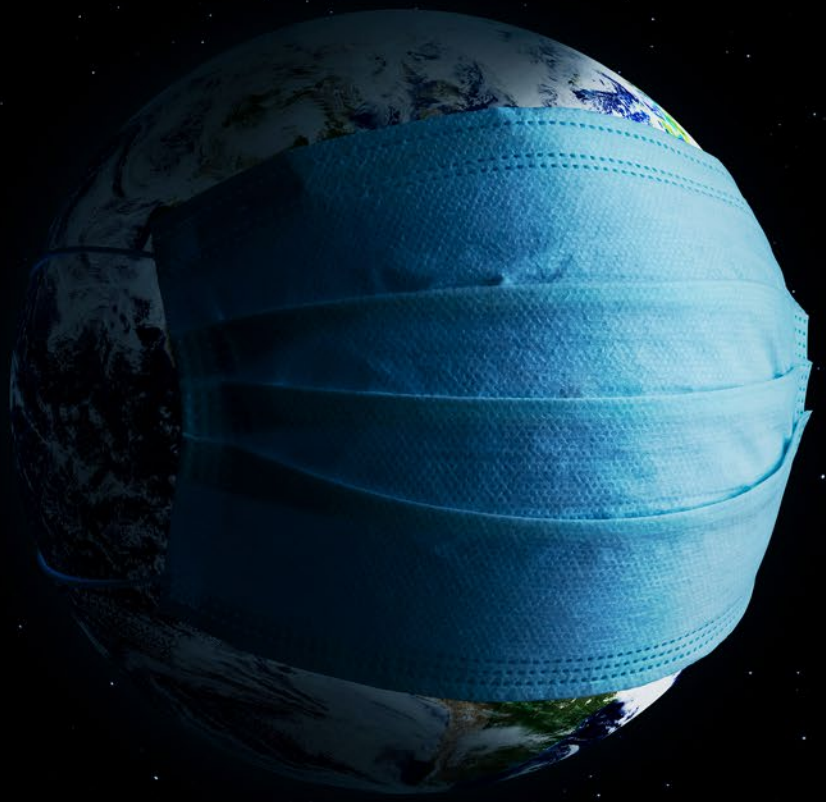
SPECIAL THANKS TO

PLATINUM PARTNERS

GOLD PARTNERS

Note that PECB Partners are listed as per the credits acquired from January 1, 2019 to December 31, 2019.

Human health and planetary health are indissolubly related to each other. To protect one, we must shield the other!



KEEP YOURSELF AND YOUR ONLY HOME SAFE!