PECB Insights

ISSUE 30 ISO STANDARDS AND BEYOND JANUARY-FEBRUARY 2021

CYBERSECURITY IN TIMES OF A PANDEMIC: ONE YEAR ON

In This Issue


“Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders.”
RONALD REAGAN,
40TH U.S. PRESIDENT

Cybersecurity in 2021

What Will Underpin Organizations' Cybersecurity Priorities in 2021?

BY ANTHONY ENGLISH

My days working in and then with law enforcement began when personal computers were becoming more mainstream and the interconnection of computer systems around the world began with a USA Department of Defense project (ARPANET) and then a project out of CERN. During this time, I was lucky to have needed an understanding of binary and ASCII as well as a few programming languages in order to work in information technology at all. So, back then, our concerns about bad things being done comprised a short list of threats. Now, as we all know, cybercrime has become a big money-maker for criminals and nation-states alike and it has become a tool in the weapons arsenal of many nation-states as well, and cybercrime tools have become increasingly easy to use such that anyone with limited technical skills can launch cyberattacks.

Fast forward to 2021, and we have, once again, a changing threat landscape: many employees now work from home, either fully or in part, organizations are relying far more on cloud or online services, applications, and infrastructure, nation-states are launching larger and more devastating cyberattacks, social media has become a cornerstone of societal action and also societal disruption, various elements and forms of artificial intelligence are being utilized for defensive and offensive security, and some older forms of cyberattacks based on social engineering have been updated to improve their effectiveness. One common denominator remains, however, the human element in security and, as the saying ascribed to Alexander the Great goes, “Remember: upon the conduct of each depends the fate of all.” Let’s take a look at the crystal ball together and see what 2021 might look like with regards to cybersecurity.

Work from home or remote working is not a new concept, but it has become an essential element of every organization’s business continuity plan and, if you have not yet documented your business continuity plan, then you do need to get on top of that! With a remote workforce, it is always best to have a structured plan that includes: a) secure endpoint devices (either through issuing organization-owned devices that you manage and control access to and/or through the use of MDM or similar software deployed to the endpoints), b) secure communication channels (through the use of secure VPN or similar technology), c) secure document management (through data loss

prevention, forced storage to secure locations only, etc.), and d) continuous security awareness for all organization staff and third-party partners). In 2021, organizations should be investing effort (and probably money) in this new world of remote working because it is not only a new reality during the pandemic, but it can also become a money-saving business model for many organizations (e.g., less bricks and mortar required, less time spent commuting, etc.).

As we have already witnessed in 2021 (e.g., SolarWinds attack(s)), more sophisticated nation-state sponsored cyberattacks are now occurring and they will certainly continue. With the SolarWinds attack, there was an added level of impact due to the pervasive nature of the compromised software throughout government and private sector. In addition, attacks on critical infrastructure (e.g., water supply in town in Florida, USA) which utilize IoT or IoMT (medical devices) have already begun to occur in 2021 and these will continue to be a risk going forward with these attacks mainly being of benefit to foreign nation-states. Here in Canada, there has already been talk about strengthening our cyber defense/offense capabilities due to the new realities of a "gloves off" cyber cold war that we are currently in the middle of (whether any country wants to admit this or not). These types of attacks will continue in 2021 and critical infrastructure and manufacturing where IoT or automated industrial control systems are utilized will have to continue to strengthen their cyber defenses.

> **On the financial front, 2021 has already seen several cyberattacks against cryptocurrency trader or warehouse vendors – I mean, why try to attack the blockchain that runs cryptocurrency if you can instead compromise a password on a cryptocurrency vault that houses the cryptocurrency?**

We have also witnessed how a small, dedicated group of non-professional Wall Street traders can immediately influence stock value on a listed company (e.g., GameStop). Cryptocurrency may be in jeopardy in 2021 as a viable alternative to state-backed currencies; also, trading regulatory bodies worldwide will be looking to protect the stability of exchange-listed companies.

Social media has become weaponized in 2020/2021 with examples such as nation-state elections being disrupted, the rise of online hate groups, the coordination of attacks by private citizens on governments, and the radicalization of citizens of even Western democracies through conspiracy theories launched via and supported by social media. I used to get a chuckle out of memes shared on social media with a photo of someone famous and a statement attributed to that person which that person never really said but, today, this previously humorous activity has become a means for creating disinformation or misinformation. Conspiracy theories will continue to find willing believers in 2021 and this will continue to add a destabilization of the human factor in the cyber-threat landscape because radicalization of citizens (as some nation-states have obviously discovered) can destabilize entire countries. Social media companies will need to continue to tighten their controls over content on their platforms in 2021; however, we have already witnessed some controls being imposed upon social media content from the outside (e.g., Apple, AWS, and Google banning content related to the feeding of misinformation to those who attacked the US Capitol in January) and we have also seen the creation of new social media channels/applications specifically to avoid these types of controls.

On the topic of nation-states, we have seen several successful cyberattacks against nations that appear to have themselves been state-sponsored (e.g., the attacks against systems at uranium enrichment facilities in a certain Middle East country). The latest reports out of US intelligence agencies also describe how some foreign nations are making a fairly large amount of money from state-sponsored cyberattacks against other countries and the citizens of these other countries; this is so lucrative that a certain country near the Chinese border was identified as having funded the development of their latest ballistic missile with funds acquired through state-sponsored cybercrime. 2021 will see this trend of state-sponsored cybercrime continue so the rumored efforts to increase the strength of nation-state countermeasures against these types of attacks will, no doubt, need to be increased this year.

The need for cloud services of all types was mentioned previously in this article as a consequence of the remote workforce reality we now all live in, so the use of cloud will only increase in 2021 and, with this, the need for practical cloud security skills and the need to audit cloud security will both be important this year and going forward. If you are not yet familiar with (or certified in) cloud security best practices (e.g., from Amazon's best practice guidance to ISO

standards, and Cloud Security Alliance frameworks) then you will want to buckle down and get a grip on this information. Every cloud implementation or usage is an opportunity for poor security design or poor security implementation, so 2021 should be your year to get your head in the clouds and learn and apply cloud-specific security.

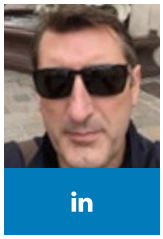
> **Everyone has been talking about artificial intelligence for the last few years and many organizations seem to be misusing this term to describe things that are not actually AI but are instead things like machine learning, deep learning, and similar, but AI as a general discipline has become more pervasive and this will continue in 2021.**

You can even get your hands on machine learning source code today through GitHub that can get you started tomorrow on building your own machine learning-based application or process. I have a friend in Europe who has, along with colleagues, used some AI discipline tools to build an engine to analyze outputs from source code testing tools in order to weed out all of the false positives or informational types of findings to make troubleshooting source code issues far more cost and time effective. Because of the increasing availability of machine learning (and other) toolsets, we will most likely see an increase in AI/machine learning usage in 2021.

We have spoken a few times in this article about state-sponsored activity related to cybersecurity and I wanted to cover another aspect of the relationship between governments and technology: the use of technology as both a societal change engine and also its suppression as a means to stop such change. In 2021, as in some previous years, we have witnessed a nation-state (most recently, Myanmar) undergo a political upheaval, and then, once the citizenry began to resist the change, the government cut off all internet access in the country. Governments have come to understand that speedy communication amongst its citizenry can be used to hold the government to account (and not always in the best way, as we have also seen), so control of access to technology such as the internet has been and will continue to be a risk in the cybersecurity realm on all sides of the security discussion. Control of access to technology for nefarious purposes versus the public good or freedom of speech will, without doubt, continue to be a contentious topic in 2021.

Mobile devices have become an even more important tool in the organizational/work toolbox during this pandemic and the security of these devices has also become increasingly important. Efforts to gain access to these devices and intercept or divert their communications have correspondingly increased during this time of remote working and technologies that promise increased security, such as 5G, have also become a focus for organizations and end-users. Supply chain security especially in technologies like 5G has become critical and will be a vital focus in 2021.

As these pandemic times have demonstrated, nothing is constant except change and, as security practitioners, we must all be adaptable to change. To quote Alexander the Great once more, “There is nothing impossible to him who will try.”, and this applies to both the cybercriminals and the cybersecurity professionals who work to stop illicit or illegal activity. In addition to preparing for the evolving threat landscape of 2021, I think it is equally important to ensure you maintain your personal and professional commitment to ethical conduct when working in any branch of a security career and to instill secure practices at all levels of your organization. Best of luck in 2021!



Anthony English
CEO/CISO at Bot Security Solutions Inc.

Anthony English is a seasoned IT and Security professional with multiple certifications in both disciplines. Anthony has worked in health care, utilities, law enforcement, lottery and gaming, auditing, education, and consulting and has more than 34 years of applied experience. Anthony volunteers on a Standards Council of Canada committee for IT Security, a Cloud Security Alliance committee for securing health care data in the cloud, on ISC2’s CISSP Certification Committee, as a member of the Disaster Recovery Institute of Canada’s Certification Committee, and as a member of the International Association of Privacy Professionals CIPP/C Certification exam committee. Anthony has conducted threat risk assessments, privacy impact assessments, security gap and maturity assessments, security testing (both physical and IT), security audits, built BCP, IRP, and DRP plans and SSDLC’s, and many other tasks during his time in the security field. Anthony holds multiple certifications including: ISO/IEC 27001 Master, PCIP, CISSP, CBCP, CIPP/C, ClCISO, CRISC, CGEIT, ISO/IEC 27032 Lead Cybersecurity Manager, CISM, CISA, and more.

The Role of Leaders in Creating a Cybersecurity Culture

BY DON BAHAM

In Hollywood films, cybercrime is usually portrayed as the modern-day Western where the bad and good nerds shoot code at each other instead of bullets. The reality is far more mundane. Most of the time, data breach incidences occur simply due to negligence or avoidable mistakes by employees.

According to a recent report by the Ponemon Institute and IBM, approximately a quarter of the data breach incidences from July 2018 to April 2019 resulted from human error. The best action to remedy this risk is adopting a holistic approach that can address technology, practices, procedures, and people. Ensuring that all these procedures and practices are well maintained requires an efficient governance model.

This calls for strong leadership from the organization's top levels. Ultimately, all company leaders are responsible for implementing the relevant principles and policies in their teams and departments. Unfortunately, senior executives (even in established companies) still believe that cybersecurity issues are for the IT team instead of a leadership issue.

The company leaders play a vital role in terms of defining the organization's values. They have the influence and authority to prioritize cybersecurity as a critical component of the overall organizational culture. Typically, employee engagement is usually born out of culture and not vice versa. It does not matter the level of commitment or how excellent your strategy is; it will not be successful unless your employees buy into it.

A robust cybersecurity culture can help you avoid data breaches and cybersecurity incidences. But it starts with ensuring all leaders assume their responsibilities.

Leaders Play the Main Role in Creating a Cybersecurity Culture

It is all well and good adopting state-of-the-art, advanced security technology and tools to protect your company data and systems from cyber threats. But if you fail to establish a strong cybersecurity culture, you will still be vulnerable.

Every day, cyber threats get more sophisticated. This explains why nearly a third of businesses in the US have experienced a data breach. Considering these statistics, most companies deem cybersecurity as one of their top priorities.

Companies that make significant investments in cybersecurity mostly base their investments in tech. However, they fail to provide sufficient attention to

the human side of the system, which remains a top cybersecurity threat for most companies.

Often, malicious individuals attack organizations' systems using phishing emails and other similar tactics. This means employees have to be strengthened as the first line of defense. After all, apps, software, and computers do not click on these emails, it is the humans who do it – and this is where you should focus your cybersecurity investments.

Furthermore, it is the personnel who access most of the company's networks, computers, and systems every day, so they have a major role in keeping the IT infrastructure resilient in the threat landscape.

When you implement a cybersecurity culture in the company, the benefits will cover the security posture and the entire organization. The culture goes beyond simply creating and publishing policies without adequate instruction and instructing personnel to change their access details and passwords frequently. Employees do not put the company data at risk intentionally. They only need sufficient guidance and training to handle any incident that comes their way.

That is why company leaders should be at the forefront when creating a security culture. Their role may include raising awareness and explaining to employees the possible cybersecurity threats, their implications, and how to mitigate them. This will allow you to enforce practical cybersecurity approaches and standard procedures that will assimilate with the organization's day-to-day activities.

The board of directors is ultimately responsible and liable for the organization's survival. In the interconnected world of today, cyber resilience remains to be a major part of their responsibility. These organization leaders should consider cybersecurity an enterprise-wide issue, not just the IT department's job. As such, they must guide the management team on the best practices.

Directors should understand the associated regulatory and legal implications of cyber threats and relate this information to their specific circumstances. They should also guide management in creating a robust risk-management framework with an adequate budget and staffing.

How Leaders Can Foster a Cybersecurity Culture

The Covid-19 period has seen a massive increase in reported cybersecurity incidences and data breaches. However, the increase in attacks and vulnerabilities is also a unique opportunity for company leaders. This is the

appropriate time for them to step up their communications and operations to create a strong cybersecurity culture that adequately guides members on the desired behaviors and actions.

High-ranking company executives should personally facilitate enhanced vigilance against opportunistic threats to business data and the company as a whole. They must also ensure employees implement these secure behaviors during these crisis times and beyond.

Here's how leaders can create and reinforce a strong cybersecurity culture in their establishments:

Begin with the Basics

Most companies make the common mistake of skipping the basics. This can lead to lots of confusion among staff, and most may end up making errors that they could easily avoid.

Basic activities like establishing and implementing a firm password policy can have a significant impact. With this policy, you will have an effective defense line, and attackers will have a hard time accessing your network and systems. What's more, enabling two-factor authentication means an additional security layer to the baseline and limited access to accounts.

It is also essential to limit access to systems, software, and data to only the appropriate roles. Once a worker leaves the organization, you should terminate any access to sensitive information or face the risk of exploitation.

Finally, it is vital to limit the types of software employees can download using company devices. This significantly lowers the risk of data breaches and cybersecurity incidences.

Implement Simple Reporting Procedures

Employees may be easily led into thinking that they cannot interact with security and IT departments unless a mistake has been reported. This should not be the case. Instead, management and executive teams must ensure open communication within all the company departments. Staff must also feel confident about reaching out to the responsible groups to report an issue or provide a constructive response when they have committed a mistake.

Leaders should also make junior staff understand that they are free to request any assistance from the teams and gain a more profound knowledge of their roles in maintaining a strong cybersecurity culture. In addition, create

channels where staff can easily reach out to the relevant professionals to report any suspicions, seek guidance, or request additional cybersecurity training.

Engaging Continuous Cybersecurity Training Is Vital

There is no excuse for failing to make cybersecurity training a more engaging experience. Making the training interactive and engaging for your staff is a significant component of a robust security culture.

For instance, you may use real-life examples to show how lousy security hygiene can harm the company, but it should not end there. You should enlighten them on how vital their role is and how they can ensure secure systems and seamless operations.

Make the training fun for your staff. You can organize a competition and reward those who show a deeper understanding of cybersecurity issues. It is also helpful to share stories on how a good cybersecurity culture can transform the company and make the training continuous. Do not force an entire week of training down their throats. Instead, remind everyone to stay vigilant every week while often rewarding anyone who identifies and reports any threat or bug.

Relevance is key. To make the training more useful, you can customize the education program to match different departments' needs since they do not face similar threats. Facilitate cooperation, coordination, and dialogue between teams so that they can share their experiences.

All this will ensure the employees have a deeper understanding of all cybersecurity aspects.

Monitor Post-Training Performance and Behaviors through Metrics

Using fun competitions and games to achieve an engaging learning process can also help you keep track of your strategy's effectiveness. Quick and regular tests and assessments will clearly show how useful the training has been, and you will be certain whether your employees have gained concrete knowledge of the concept. By checking these metrics, you will know how far you have come regarding creating and developing your security culture.

Be creative with the education. For instance, you can assign negative points to underperforming employees or mention their names to motivate them. Of course, this activity is not ideal for all companies, so ensure you choose a strategy that works for your team.

Make It Your Long-Term Objective

Criminals and malicious individuals understand that the best time to attack is during high levels of uncertainty, fear, chaos, and doubts. Company executives must step in and implement the attitude and values that all employees are responsible for the company's security. Leaders must also demonstrate their commitment to ensuring security by improving their activity, updating their staff, and supporting first responders whenever there is a cybersecurity incidence.

Everyone hopes that the coronavirus pandemic ends soon, but maintaining your data and overall company security should be a long-term objective. A security culture where all employees feel personally responsible for protecting the company against cybersecurity threats will protect you from new vulnerabilities and threats for years to come.

The Bottom Line

It is a common misconception that protection from cyberattacks and data breaches is the security and IT departments' work. The truth is, organizations' leaders are responsible for creating and implementing a robust and long-term cybersecurity culture.

With the above tips, you will ensure a robust security culture that will not only protect you from threats during this coronavirus era but for years to come.

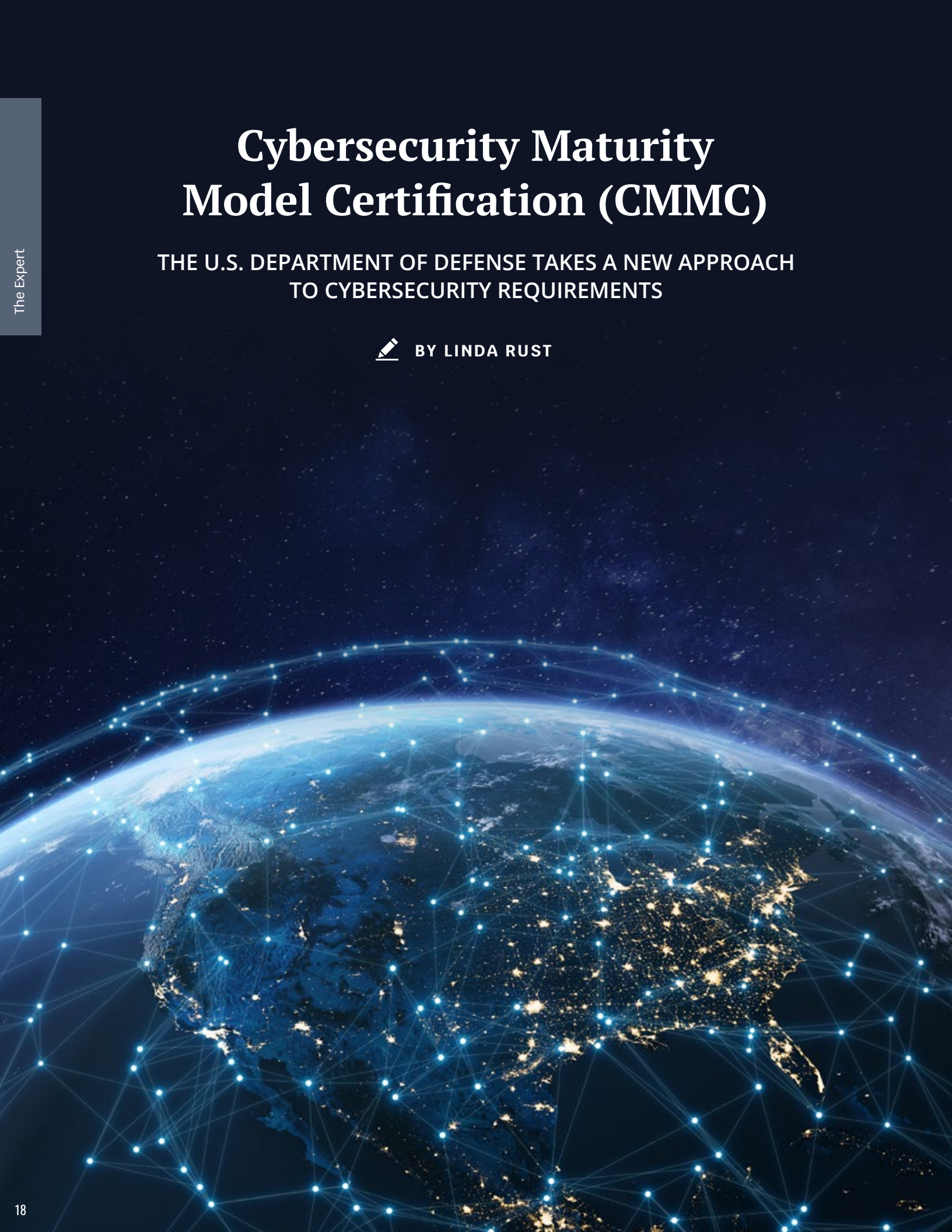
Don Baham
President of Kraft Technology Group, LLC (KTG)

Don Baham is the President of Kraft Technology Group, LLC (KTG). He is responsible for delivering IT strategic planning and virtual CIO services, bringing new solutions to the market, and leading the strategic direction of KTG. Don has more than 20 years of experience in IT with a blended background in technology consulting, information security, and business development. He has a degree in IT Design and Management and several certifications including Certified Information Systems Security Professional, Certified Information Systems Auditor, and Microsoft Certified Systems Engineer. He is a regular guest on Nashville WSMV and WTVF discussing technology and cybersecurity and a member of the Business Journal Leadership Trust and the Forbes Technology Council.

Cybersecurity Maturity Model Certification (CMMC)

THE U.S. DEPARTMENT OF DEFENSE TAKES A NEW APPROACH TO CYBERSECURITY REQUIREMENTS

BY LINDA RUST



What is CMMC?

Cybersecurity Maturity Model Certification (CMMC) is a new cybersecurity standard and a requirement soon to be seen in contracts from the U.S. Department of Defense (DoD) that will affect its entire supply chain, including all levels of subcontractors and those which may be international in location. Estimated to include 300,000 entities, all organizations in the Defense Industrial Base (DIB), including universities and other federally funded research centers, will be required to obtain the new certification.

The Purpose of CMMC

The leader most closely identified with CMMC is Katie Arrington, the Chief Information Security Officer (CISO) for Acquisition & Sustainment (A&S) at the DoD. "Our adversaries are working hard every day to exfiltrate, hack, and breach our supply chain." She said in a keynote in February 2020. "CMMC is about creating critical thinking skills for Cybersecurity, and not another checklist."

"Ultimately, all of you are the base of our national defense. You are the reason we are here," said Arrington at a May 2020 event hosted by the CMMC Accreditation Body (CMMC-AB). "The Department of Defense doesn't build a thing. We buy. We contract with you. You're our national defense. Our adversaries aren't taking a knee during this time (of the pandemic), in fact, they've been extraordinarily aggressive. If there was ever a time and place in our collective history that we needed to stand up and come together, and move forward on this, it's now. Cultural change generally takes a catalyst to happen."

Comparing CMMC to Current Requirements

A summary of the current DoD cybersecurity requirements with a comparison to the CMMC framework is shown in Table 1.

Governance, Framework, and Standards

CMMC is a U.S. Department of Defense Program. The CMMC-AB is the sole oversight body authorized by the DoD to operationalize CMMC assessments and training which are essential to meeting the goals for scaling across the entire DIB. The CMMC-AB is a non-profit organization that has a contract with the DoD. A key requirement of that agreement is the AB must become ISO/IEC 17011:2017 certified. The DoD has also stipulated that subcontractors which conduct authorized assessments must achieve ISO/IEC 17020 certification.

While the DoD does not own standards, it does create and maintain the CMMC model. By defining CMMC as a model, not a standard, the DoD retains the right to update it as

Table 1

Current DoD Cybersecurity Requirements	CMMC
Based on trust	Based on trust with verification
Self-assessment	Third-party assessments conducted by authorized and accredited organizations
Self-attestation of compliance at the time of contract award	Certification must be complete before contract award; three-year renewal cycle
Each company is responsible for its own compliance and to "flow down" the requirements to all of its subcontractors.	The contractor which has the agreement directly with the DoD is responsible to ensure valid certification of all subcontractors at all levels in addition to themselves.
Incomplete implementation of compliance controls may be documented on a Plan of Action with Milestones (POAM).	Compliance tiers from 1 (basic) to 5 (advanced); no incomplete items allowed beyond a 90-day post assessment remediation period
Based on the U.S. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171	Based on NIST SP 800-171 with selected controls added in tiers 2-5 from other respected sources
No process maturity requirement	CMMC tiers 2-5 include progressively higher requirements for process maturity.

required to address the dynamic changes in the cyber threat landscape and the DIB threat surface. This enables the model to draw on respected resources as needed to identify and define controls.

The CMMC framework is a combination of various cybersecurity standards and best practices with NIST SP 800-171 being the foundation. The maturity practices rely primarily on the CERT Resilience Management Model (CERT-RMM) from the Software Engineering Institute (SEI) at Carnegie Mellon University. In addition to standards and the Cybersecurity Framework (CSF) from the U.S. NIST, also referenced are the U.K. National Cyber Security Centre (NCSC) Cyber Essentials, the Australian Cyber Security Centre (ACSC) Essential Eight, along with numerous controls from the Center for Internet Security (CIS), a nonprofit cyber defense organization that draws professional expertise from around the world.

"Any standard that requires your organization to maturely document, implement, and manage an ongoing cybersecurity program will be incredibly useful in passing a CMMC assessment, regardless of who wrote it," posted Ryan Bonner January 2021 on LinkedIn. A respected compliance consultant, Bonner, is among the first 100 provisional assessors approved by the CMMC-AB.

What Is the CMMC Timeline?

The widely publicized full implementation date for CMMC is October 1, 2025, the beginning of the 2026 fiscal year for the U.S. government. At that time, all new DoD contracts and contract extensions are expected to require CMMC certification to be in place prior to the award.

A methodical roll out is forecast for CMMC itself, as shown in Table 2. Intended to test the process while allowing time to create the considerable infrastructure needed to make this work, the throttle on the pace is controlled by Katie Arrington's office; only contracts which they approve may include the requirement language.

Urgent and Compelling Circumstances

While the wheels of regulation usually turn slowly, and CMMC does not go into full effect until 2025, Katie Arrington and her team surprised many DoD watchers in September 2020 by publishing an Interim Rule which made some new requirements effective November 30th, a mere 60 days later.

The unusual acceleration of the rule was made possible by declaring "urgent and compelling circumstances."

Table 2

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	**FY22**	**FY23**	**FY24**	**FY25**
15	75	250	479	479

	Total Number of New Prime Contracts and Sub-Contractors with CMMC Requirement				
	FY21	**FY22**	**FY23**	**FY24**	**FY25**
Level 1	895	4,490	14,981	28,714	28,709
Level 2	149	748	2,497	4,786	4,785
Level 3	448	2,245	7,490	14,357	14,355
Level 4	4	8	16	24	28
Level 5	4	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

The case presented for urgency is the enormous gap between the significant losses being incurred by cybercrime and the lack of readiness prevalent among DoD subcontractors. Among the facts cited are the following:

- Cyber theft of intellectual property and sensitive information from all U.S. industrial sectors is estimated to value $570 billion to $1.09 trillion dollars over 10 years.
- Surveys of DoD contractors and subtractors show engagement in the forms of awareness and implementation of existing cybersecurity requirements, some in place since 2013, as low as 36–54%.

Highlights of the Interim Rule

Intended to bridge the gap between cyber losses and readiness, as well as to remove complacency about current requirements until CMMC arrives, the highlights of the Interim Rule are:

- Define a mechanism for reporting results of self-assessment for compliance with existing requirements beginning November 30, 2020, before award of new and extended contracts
- Increase the visibility of prime contractors' accountability for flow down requirements to their subcontractors
- Announce the contract language for the new CMMC framework and the roll out plan
- Summarize the plan to scale assessment capability via the CMMC-AB

Who Is Impacted?

While the U.S. is clearly the epicenter for this change, there are immediate global implications. Many companies outside the U.S. have DoD contracts or subcontracts. For example, based in Sweden, Saab has a history of many contracts with the DoD and, based on their participation in various public forums focused on compliance with these requirements, Saab is probably in a strong position of readiness.

Research indicates that not all companies are equally prepared. A report from Sera-Brynn says overall implementation numbers are improving, from 39% in 2019 to 53% in 2020, but it is still clear that there is a big gap with smaller companies, especially those with less than $50 million in revenue, struggling the most.

Industry differences are another factor. Manufacturing, aerospace, and technical equipment suppliers are well ahead. At the back of the pack are construction and professional services firms.

PECB an Early Leader in CMMC Training Materials

PECB is among the first 16 Licensed Partner Publishers (LPP) authorized by the CMMC-AB to create materials to train assessors. Enormous emphasis is being put on consistent outcomes across assessments, starting with consistent quality of the training materials.

What's Next?

Katie Arrington believes CMMC "will become a federal standard for the whole of government very rapidly." Indeed, an official from the Department of Homeland Security (DHS) said "it's likely that civilian agencies will naturally benefit from CMMC implementation. Due to that overlap, we aim to harmonize our cybersecurity approaches as much as possible." Meanwhile, the U.S. General Services Administration (GSA) has mentioned CMMC requirements in two contracts worth $50 billion and $15 billion, respectively. Arrington sees an even bigger future, saying, "I think the CMMC will become the basis for a global cybersecurity standard."

in

Linda Rust
Principal and Founder at
SecuriThink Corporation

Linda has a passion to empower commerce and citizens to prevail over cybercrime. Her foundation in the CMMC ecosystem draws on eight years as a C-level consultant to one of the top 50 DoD prime contractors during a period when they significantly matured against relevant standards. She continues to advise that organization which has consistently won a "superior" rating annually from the DoD since 2014, won the Cogswell Award for security in 2016, and the Defense Security Excellence in Counterintelligence Award in 2019. Linda creates hyper-practical strategies that leverage technology investments with essential process and enlisting stakeholders. Her work has earned the support of board directors and the C-suite, engaged thousands of employees in behavior change and aligned information security with the business mission to get results that really matter. With 20+ years of industry experience since earning her computer engineering degree, along with certifications that include ISO/IEC 20000 Lead Auditor, PMP, and CISSP, Linda holds, "Security begins with a mindset."

NEW TRAINING COURSES LAU

PECB Certified CMMC Foundations

LAUNCHING ON MARCH 8, 2021!

PECB is part of the CMMC-AB ecosystem as a Licensed Partner Publishers (LPP) for Cybersecurity Maturity Model Certification (CMMC) and it will be developing training curricula based on the CMMC-AB's Body of Knowledge.

Nonetheless, PECB has decided to also develop a Foundation level training course, in order to help its network understand this new type of certification. **The certified CMMC Foundations training course is not approved by the CMMC-AB.**

This training course enables the participants to understand the structure of the CMMC model including levels, domains, capabilities, processes, and practices.

- **Two days + certification exam**
- **Quizzes, examples, and best practices**
- **No professional experience required**

→ **FIND OUT MORE**

UNCHING ON MARCH 1 AND 8!

PECB Lead Cloud Security Manager

LAUNCHING ON MARCH 1, 2021!

The global cloud computing market size is expected to grow from $371.4 billion in 2020 to $832.1 billion by 2025.

Taking into consideration the global trend and the worldwide increased demand for organizations to adopt a cloud-based technology, we are continuously working to stay ahead of these developments.

This training course will help organizations that adopt cloud-based technologies to ensure that they have a thorough understanding of the security challenges and risks, and can obtain assurances that their cloud solutions provide suitable security and privacy controls while still delivering all the benefits of the cloud.

→ FIND OUT MORE

Insight into Cloud Native Detection and Response

BY SCOTT NICHOLSON

The Managed Security Services (MSS) market has historically been based around a number of enterprise-leading Security Information and Event Management (SIEM) solutions, which enable organizations to harvest and aggregate large amounts of data from servers, networking infrastructure, and systems hosted within the cloud. SIEM technologies and MSS companies then use the data to analyze and identify anomalies and potential cyber-attacks across the networks.

The Problems and Challenges

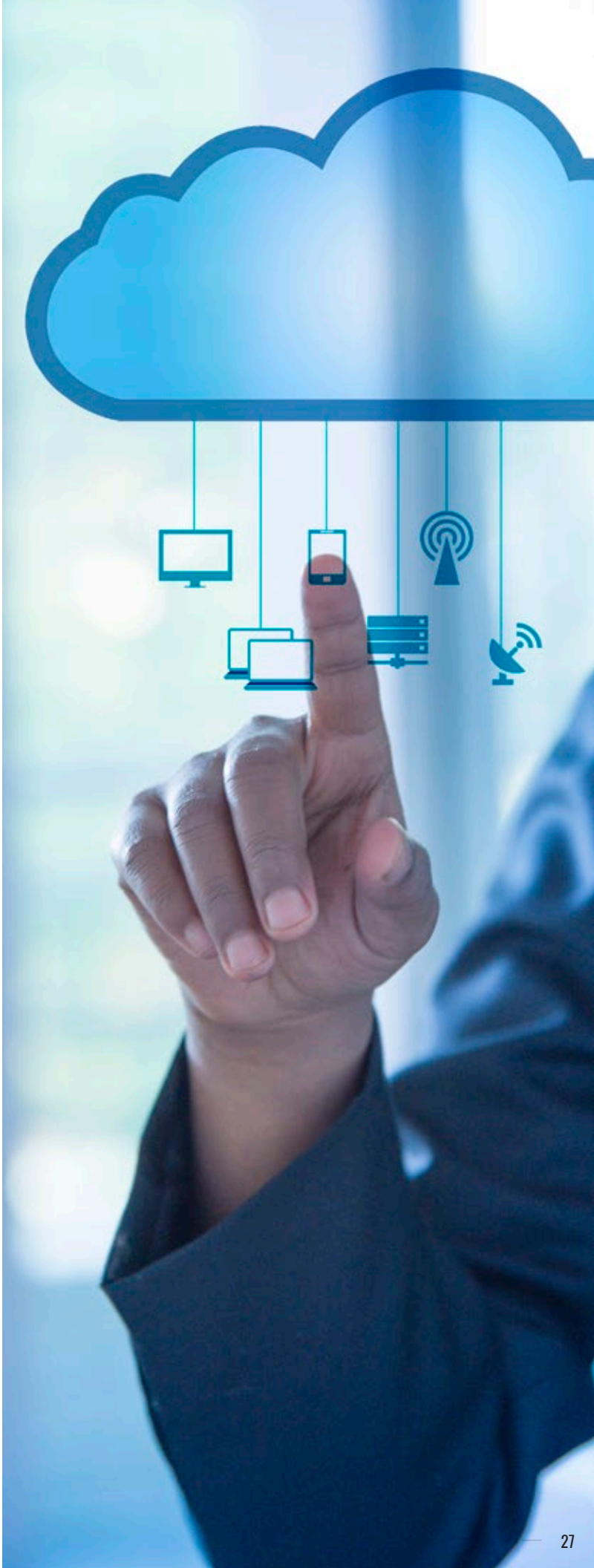
Some of the problems with historic MSS providers and SIEM technologies is that the alerts generated from SIEM technologies often produced a large volume of incidents that required further investigation by IT teams and often deemed to be false positives. SIEM technologies often do not have the full capability to deliver any response or enrichment function to the events, alerts, and incidents generated; high-alert volumes combined with limited business context can often lead to a perception that the MSS is more of a hindrance than adding value to an organization. This is not strictly true but equally a perception that I have often seen over the recent years.

The other thing about SIEM products is the cost. The enterprise SIEM technologies can often be cost prohibitive for organizations and can introduce the concept of a client being tied to an existing MSS provider, due to all the data residing in a third-party SIEM solution. Many have also fixed licensing costs and dedicated hardware that do not easily scale and which contribute to this feeling of being locked in to a provider.

Introducing Cloud Native – SIEM and Managed Detection and Response

Security technologies monitoring public, private, and hybrid cloud environments are no longer something new. However, what is continuing to evolve are some of the public cloud providers such as Amazon Web Services and Microsoft are building their own security technologies, which are often subscription-based licensing models and place the customer in control of their own destiny. These models enable organizations to rapidly scale up and down to meet their own unique needs without introducing additional upfront costs.

> **Do these technologies only monitor the cloud? No, the best thing about some of the cloud native security capabilities is that they can monitor hybrid on-premise IT, multi cloud-based infrastructures, Software as a Services (SaaS) systems, in addition to their deep insight into their own cloud technology.**



My view at this stage is that Microsoft is the leading cloud native provider for managed detection and response capabilities, which comes in the form of Azure Sentinel and Defender Xtended Detection and Response (XDR) capabilities. For that reason, this article focuses on the Microsoft components that could be leveraged for building a cloud native detection and response capability.

Detection and Response for End-User Devices

What is key to an effective detection and response capability is having insight into end-user behavior activity, which often provides insight into initial attack activity. However, visualization and alerting is not enough, MSS providers or internal security teams need to be able to identify, contain, and respond to early signs of malicious activity being undertaken. The MITRE ATT&CK framework is a great way to identify the key Tactics, Techniques, and Processes (TTPs) to proactively identify various attack methods and put in place controls to mitigate them, but when malicious activities do take place, identifying, containing, and eradicating this as quickly as possible is key.

Microsoft's product for this is Microsoft Defender for Endpoint (MDE) which provides increased endpoint protection through attack surface reduction, application control, and network protection. Advanced threat hunting, network isolation, and real-time response across enrolled devices is also possible, making this a key weapon to your detection and response capability. One of the most powerful features of MDE is its ability to leverage signals across all of Microsoft's other XDR technologies and fully automate elements of the incident response life cycle. It is worth noting that this capability is unique to Microsoft. While AWS has great security capabilities, it does not have specific EDR product for end-user devices. However, there are many third-party services available on the AWS Marketplace.

The SIEM Is Dead, Long Live MDR?

Most definitely not, SIEMs are still an integral part of any security operations capability, providing that holistic view that can collect, normalize, and analyze substantial amounts of data to overlay your use cases and alert on the things you care about most. MDR provides the rapid

response capability that the SIEM feeds. It is like a police control room (the SIEM) and the rapid response police officers, only instead of cars they have portals that can instantly make them arrive at the scene – that is what MDR provides, the ability to rapidly be at the scene (the laptop, server, cloud infrastructure, SaaS service). When MDR combines the power of User and Entity Behavior Analytics (UEBA), Security Orchestration Automated Response (SOAR), and highly skilled humans with SIEM technology, this is where it begins to disrupt in comparison to more traditional SIEM implementations.

Amazon GuardDuty is the AWS native threat detection service and the dashboard summary with some key areas highlighted can be found here.

Azure Sentinel is Microsoft's native SIEM solution and has very powerful SOAR capabilities and for me is the leader in cloud native SIEM solutions, bringing in all end-user behavior, devices, applications and both on premise and cloud infrastructure. It also leverages Artificial Intelligence and Microsoft's own threat intelligence feeds, while supporting integration into other threat intelligence capabilities.

If you are going to leverage Azure Sentinel and part of your cloud native, detection, and response capabilities, be sure to connect the multiple data sources. By leveraging Azure Sentinel connectors you can integrate things like the range of Defender XDR security capabilities, Office 365, Azure Active Directory, and Microsoft Cloud App Security.

> **When combining all technologies together, it is an extremely powerful capability that can also leverage a proportion of your existing licensing costs where Microsoft E5 licenses are already in use, reducing your overall costs.**

In general, Microsoft will not charge you to consume alerts from its own security products which is another additional benefit.

Fusion Technology to Deliver Multi-Stage Attack Detection

If you want to leverage some powerful capabilities to identify complex combinations of potentially malicious activity across the kill chain, then look no further. Enabled by default is Fusion, this low-volume, high-fidelity rule is pre-built within Azure Sentinel and can detect multi-stage attacks across the MITRE ATT&CK Kill Chain, leveraging machine learning. Again, when it comes to enhancing your detection and response capabilities, this type of capability gets you off to a great headstart.

Scheduled Queries

This detection method in Sentinel involves leveraging Log Analytics using Kusto Query Language (KQL) and this can be a very effective way of building upon several great out-of-the-box templates Microsoft already has, in addition to a Sigma rule capability converter. You can schedule the queries to periodically run and view previews to ascertain the potential volume of data the rules could create. There is then the ability to map entities, enabling you to utilize them in an investigations graph.

Microsoft Security

Microsoft security detections essentially consume alert and incidents from other Microsoft Security products such as the Defender XDR suite of technologies.

Machine Learning and UEBA

These are essentially the secret sauce Microsoft detections that leverage proprietary machine learning (ML) algorithms. These are behavioral detections that pull and correlate data across a wide variety of data points to uncover malicious activity.


AIU 1,822 12,349,000
EJK 3,680 238,681,000
HPL 1,062 85,678,000
KEE 485 8,369,000
NAH 8,569 189,301,000
QOP 6,602 102,698,000
TIK 890 24,697,000
WIG 6,280
AHD
350
300
250
200
150
100
50
A
02
01
B
30,000
25,000
20,000
15,000
10,000
5,000
0
OPI
TDS
PPO
FNV
JIO
JIF
J01
K02
M03
A04
D05

Considerations for Cloud-Native Detection and Response

There is no doubt in the value that having a cloud native capability for detection and response can deliver an effective capability to protect, detect, contain, and respond to threats. Where companies such as Microsoft provide much of this in their existing licensing models and the benefits that also derive from cloud such as no hardware costs and subscription based price models, you can also see the ROI benefits. However, there are some considerations you need to be aware of:

Log Data – How much and for how long?

While some licensing is already included for products such as Azure Sentinel, you may have to pay for log storage costs. This is not just relevant to Microsoft, it is relevant across all SIEM products, which often use this as part of their pricing model but "sometimes free" doesn't always mean "completely free". Key decisions around how long data is retained for and whether it is retained in stock from hot to cold and bucket to blob, it all needs careful consideration and ideally before you commence your journey.

Sometimes less is more when it comes to log ingestion

Many organizations want all log data, across all devices and this can really hike up your costs. Analyze log data sources and consider what actual benefit it contributes to use case detection. Ask yourself, what type of things are we trying to identify within this log data? This can be a valuable exercise in ensuring you only ingest data you care about, as not all data is equal, and data storage can be expensive.

Do not end up with a SOAR head, iterate automation

Automation of response is a very powerful and efficient way that can enable your security operations team to focus on the more complex of threats and move more into a proactive, threat-hunting approach to security operations. However, do not go automation crazy as this can often lead to issues impacting user-based or IT operations. I would recommend having an automation roadmap, driven by your analysts. In my view, the security analyst can often be neglected, and they are the ones with all the knowledge of what is going on across the organization. Consult them, listen to them, and work to develop a list of potential automation opportunities. This will yield the best results and get your teams feeling like part of the solution. Equally a good Managed Security Service Provider (MSSP) should have a great library of automation opportunities for you to leverage.

Summary

There is a growing number of MDR products in the market, which all bring a raft of qualities and capabilities to an organization. Anyone operating a traditional SOC/SIEM approach has to evolve into having a detection and response capability, so that attacker dwell time is minimal, and a response can be delivered as quickly and effectively as possible. This capability not only builds effective response times but equally can reduce administrative burden on IT departments, having to investigate a mass of alerts, often turning out to be false positives. Having these capabilities in a way that can maximize existing technology investments and reduce technical debt is clearly making some of the cloud-native solutions like Microsoft a compelling proposition. However, do not think because the user interface is friendly and there is a lot of "click and go" capability that you do not need experts with the necessary technology and security operations expertise. Technology is only a small proportion of effective detection and response, it is the processes, development expertise, and the ability to interpret, investigate, and act upon results where the real value is obtained and expertise is needed. Whatever you decide to do, spend the time to plan out your journey, capture what you are trying to achieve your "Why?" and go into a process of building this capability with a clear vision. You can always adapt your approach as you move forward and things evolve but trying to deliver without a clear vision will not yield effective results.

Scott Nicholson
Director at Bridewell

Scott has a wealth of experience in information security and as Director, he is responsible for the strategic direction of Bridewell's services, driving the business strategy forward, as well as overall service delivery. With extensive experience in delivering large-scale transformational projects in highly regulated environments, Scott plays a pivotal role in Bridewell's continued growth and success, forming strong relationships with industry bodies including the NCSC. Under Scott's leadership, Bridewell was one of the first organizations in the UK to gain accreditation on the Civil Aviation Authority's (CAA) ASSURE scheme and has an industry leading 24x7 Managed Detection and Response service.

Scott has been part of the Bridewell team since 2015 having previously spent ten years working within the police service, as well as several years at IBM and Rackspace. He is passionate about cybersecurity delivering tangible value to clients, developing others and is also a published author and regular guest speaker for industry events.

Keeping Cybersafe

New guidance on cybersecurity frameworks just published

As our world gets increasingly digitalized and interconnected, the threats of cyber-attacks rise with it. Organizations need resilient and secure systems and processes in place to protect them, and an effective solution is a cybersecurity framework. Two new ISO guidance documents have just been published to help organizations ensure the best possible frameworks and keep them cybersecure.

Developed in collaboration with the International Electrotechnical Commission (IEC), ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection – Cybersecurity framework development guidelines,* specifies how to create or refine a robust system to protect against cyber-attacks.

Recognizing that many different cybersecurity frameworks exist, with highly diverse lexicons and conceptual structures, this technical specification intends to simplify the task for both creators and users by providing an internationally agreed minimum set of concepts and definitions that everyone can agree on. This then frees up valuable time for combatting the real threats to cybersecurity rather than getting entangled up in the concepts and terminology.

ISO/IEC TS 27110 is complemented by ISO/IEC TS 27100, I*nformation technology – Cybersecurity – Overview and concepts,* which defines cybersecurity, establishes its context in terms of managing information security risks when information is in digital form, and describes relevant relationships including how cybersecurity is related to information security.

Dr. Edward Humphreys, Convenor of the ISO working group of experts that developed the documents, said the new guidance will help industry players be more effective in managing cyber-risks that are pervasive across our digital world.

“The IT security sector invests significant amounts of time and resources into complying with disparate regulations which, in the environment of finite resources, takes valuable time and resources away from actual cybersecurity activities. This will help to maximize resources to deal with combatting real-time cyber threats,” he said.

“Differences exist within individual countries and across global environments. These new technical specifications aim to provide clear guidance that will help organizations create a cybersecurity framework that is flexible in use while allowing for compatibility and interoperability across frameworks. This will contribute to alleviating these differences, while meeting stakeholder requirements, and create coherence across the industry.”

ISO/IEC TS 27110 and ISO/IEC TS 27100 were developed by joint technical committee ISO/IEC JTC 1, *Information technology,* subcommittee SC 27*, Information security, cybersecurity and privacy protection,* whose secretariat is held by DIN, the ISO member for Germany.

What Lessons COVID-19 Taught Us about Employee Upskilling and Reskilling

BY LUNDRIM SADIKU, PECB

No matter how much one insists that we must go back to "normal" and have a state of "business-as-usual," I'm afraid that is not really possible at this point. But that's not an inherently negative thing! In fact, the pandemic has shed light on the growing need for employee upskilling and reskilling.

With major changes in our personal and professional lives happening so rapidly, it is interesting to see how the pandemic has altered the paradigm for upskilling and reskilling efforts.

While reading about employee training, I found interesting data that hinted to certain trends that had started even before the pandemic hit.

For example, I did not know that more than 375 million workers worldwide will have to change jobs or improve their skills due to automation and AI. And I did not know that employees value learning opportunities and career advancement more than job security or salary increases.

The World Economic Forum (WEF) lists some major benefits of training employees so that they can conduct their job better or switch jobs within the company. It is much cheaper for a company to provide training for existing employees, than to fire and hire new employees. Furthermore, trained existing employees are more productive than newly-hired employees, and they are much more likely to stay in the company longer than those who do not receive any training. Finally, salary growth is shared between companies and their employees after training (as a result of increased productivity).

Where to begin?

Having talked about the benefits of upskilling and reskilling, what should companies focus on in light of the pandemic?

The first and probably most urgent need is to help employees feel comfortable in their new work stations (i.e., their homes). This and the fact that more than 90% of all jobs requiring digital skills in the next two decades make it clear that it would be a very wise decision to help employees gain digital and technological literacies.

Given the ever-growing importance of technology, it is not a coincidence that two-thirds of all employees surveyed in a study declared that learning how to work with intelligent technology in the next five years is very important.

There are already several major organizations that have understood the benefits of upskilling and reskilling. Those companies are taking steps by allocating budgets reaching billions of US dollars for creating highly skilled employees and eventually retaining their existing workforce.

In addition to technical skills, employees, especially the ones who are new relative to the existing workforce, need help and guidance in improving their interpersonal or social skills. Given the remote workstation, improving social skills is a top priority.

Moving on to something more advanced, in 2020, the world witnessed a massive move to e-commerce and digitalization of sales even in countries that were reluctant to make such a move in the pre-pandemic era. In the US, for instance, e-commerce constituted a third of total retail sales. Germany or Switzerland saw an increase of e-commerce penetration as well, thus defying pre-pandemic predictions. The increase of e-commerce penetration has huge implications for businesses.

First of all, existing employees and/or new employees need to have specialized skills to ensure smooth business proceedings online. Second, e-commerce requires that valuable information be exchanged between companies and their customers, thus creating the need for effective information security management systems. Third, the supply chain has been affected by the pandemic – obviously! Since many organizations are not aware of what happens in the lower levels of their supply chains, the issue of being able to predict what risks come with contractors becomes ever more pressing.

Speaking of risk management, a report shows that disruptions lasting for a month should be expected by any given organization every 3.7 years.

It seems to be abundantly clear that something in the way of risk prediction and managing did not go quite well. Just to be clear, nobody is to be blamed! What I am suggesting here is that risk management must be given careful attention in the future. Therefore, any professional or team of professionals need upskilling to stay on top of the game.

How to use PECB's training courses?

Many of the areas touched upon in this article, such as information security, risk management, business continuity, privacy management systems, and so on are covered by PECB training courses.

PECB's globe-covering network of more than 1,500 resellers offers a wide range of training courses. You can consult our database by clicking here: PECB – Training Resellers List.

For all clients interested in self-study opportunities, since 2020, some of PECB's training courses are available online as well! Explore more about our eLearning platform by visiting our website or following us on LinkedIn for updates.

PECB's training courses aim to equip clients with the skills and knowledge to meet the requirements of the latest international standards in a particular field.

PECB training courses and other resources (such as PECB Webinars, PECB Insights, and so on) help you implement and audit information security management systems; improve your risk managing and business continuity skills; know best practices in outsourcing, supply chain security management systems, and so on.

World Economic Forum recommendations

Reaping the benefits of employee upskilling and reskilling requires commitment from all levels of an organization. The WEF lists four aspects that will help organizations foster learning in the workplace.

The first important factor for an organization is to make lifelong learning a norm in their day-to-day business. This change of attitude is a stepping stone that enables employees and organizations to explore creative solutions to new challenges. Teaching literacies (such as digital, financial, and so on) is just one way to begin. Fostering the culture of learning and continuous improvement is the way to continue.

Second, organizations should start early, WEF suggests. Since there is a trend for jobs to become less defined and more fluid, employees have an increased sense of independence in their workplaces. This would mean that the responsibilities are also higher since the employees set their own daily agenda. So the earlier training starts, the better it is for employees who want to use new skills to function with minimal supervision.

Inclusivity is the third factor brought up by WEF. They see bridging the gaps that exist within an organization and beyond as crucial in nourishing the sense of belonging.

Finally, the WEF sees upskilling and reskilling of employees as an undertaking of multiple stakeholders, not just shareholders. This means that the needs of not only the board of directors, investors and so on, but also those of employees and the society at large need to be taken into account when training employees.

What to focus on in the future

Writing about future trends is probably the most exciting part of writing an article. I mentioned e-commerce and digitalization earlier, and those two areas are definitely here to stay.

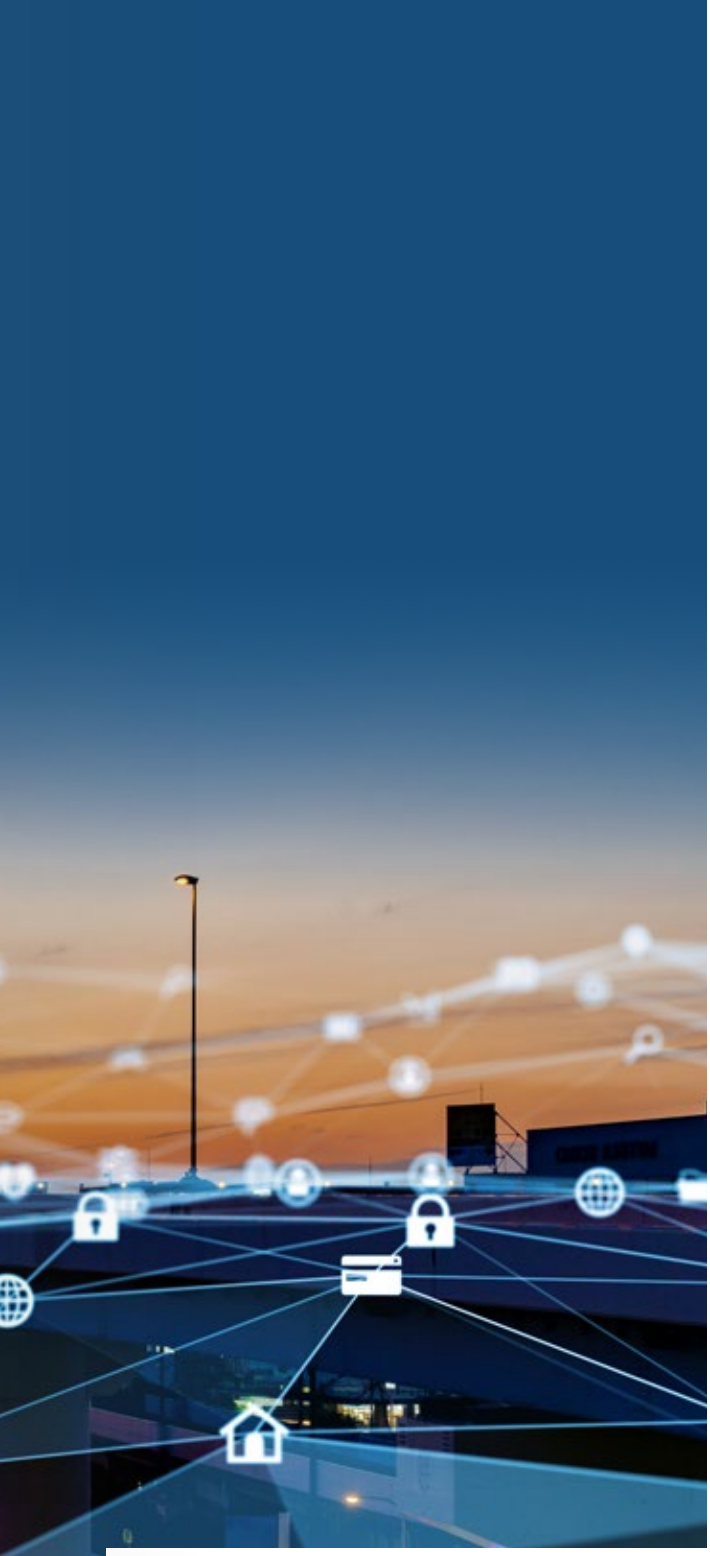
But another pressing issue is the environment. With billions of dollars allocated for green policies, businesses and governments across the globe are looking for ways to make their work more efficient and environmentally friendly, aiming at carbon neutrality by the second half of this century. Trends like these really set the tone for employee upskilling and reskilling. There are some industries that will either cease existing or change their business model entirely, therefore there will be a significant portion of workforce in need for new skills and new jobs.

Employers, training providers, and so on, need to make use of this trend and meet the new training demands, which I see as ever-increasing.

Do We Really Need a New, Next Generation of Breach Detection?

Finding the “bad guys” sooner has never been more important.

BY RICK RUSCH



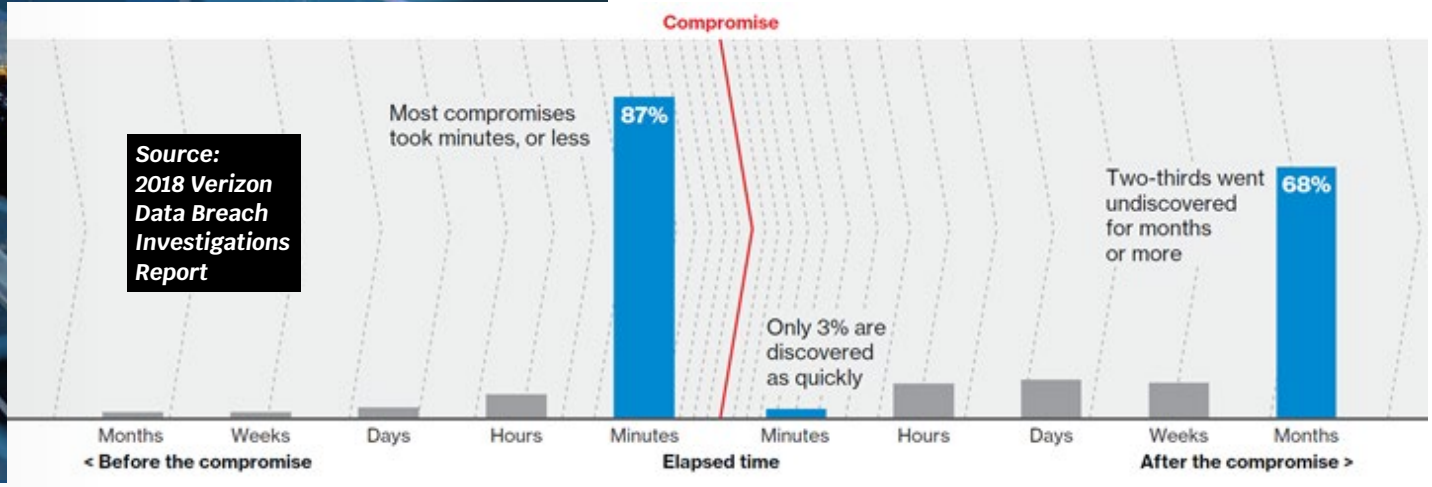
Historical Perspective

To understand the need for the next generation in breach detection, we should go back just a few years. In 2013, very few governments or businesses put much discussion into cybersecurity other than putting anti-viruses on their computers and getting a dedicated firewall on the company network at the advice of their IT department. AV and a first-generation firewall should be more than adequate for a layered defense. What was hidden until late 2013 was the massive Target breach and some sobering statistics from an annual Verizon Data Breach Investigation Report. In that report, there were a few statistics which point to the need for breach detection in a serious way. The breach is only detected by corporate internal IT staff 6% of the time. A breach goes undetected for an average of 210 days. The time to hack into a corporate network, in 75% of the cases, took under 15 minutes. Is it any wonder that breach detection has not been promoted more aggressively by cybersecurity experts?

Fast forward to 2020. We have had 7 years to better perfect our detection, right? Well, the criminals have had 7 years to find much more sneaky ways to hide on our computer networks. The stats bear out who is winning the war of attrition. In 2020, the average days to detect a breach have decreased only 4 days in 7 years, to 206 days. The costs of breaches have increased steadily over the last 2 decades, so it is inevitable that breach detection needs to step up to the next generation to counter the hackers. Although the graphic presented below is from the 2018 Verizon Data Breach Investigations Report, it graphically shows the battle we have at hand.

Current Breach Detection Methodology

There are several technologies in use now that should reduce dwell times for hackers on government or corporate network systems. Most of these have been around quite some time, particularly in enterprise environments.



Source: 2018 Verizon Data Breach Investigations Report

One such technology is known as an SIEM (Security Information and Event Management). Don't ask me the proper pronunciation of the acronym as no matter how I say it, I am immediately corrected by the nearest systems engineer. The idea is quite sound, gather in all the logged actions taking place on every PC, networked device, and server in the environment, and review them by a security professional every single day. Given that there are literally millions of actions recorded in the logs every day, this is quite a daunting task.

This is where the SIEM tool comes into play. Parse down the meaningless actions (at least as far as finding a hacker in the environment is concerned) and allow the security professional to review only about a dozen of actions that should be investigated. The problem is that there's no Red Alert Deflector Screen that pops on to protect your network. We will have to wait until the 24th century for this, I'm sure. (Geeky Star Trek reference) If you only have a single professional tasked with reviewing these actions, they will quickly get fatigued with tracking down false positive alerts. There are also vacations, sick days, and a myriad of other reasons this task is nearly impossible for a single person. A Security Operations Center (SOC) monitoring an SIEM is almost always desirable. The cost of an SOC & SIEM combination has made this option cost-prohibitive in the past, but given the rise in cybercrime and the detrimental effects after a breach, the cost may well make much more sense in the Boardroom and Government offices.

Next Step to the Next Generation

The business problem becomes how to reduce the cost of this very labor-intensive process and at the same time increase finding the elusive hacker while diminishing false positives that take time away from real threats. Just as Ransomware was a brilliant leap forward for criminal organizations to use instead of just adding more hackers, the solution is automation. Through machine learning and artificial intelligence, the machine can be trained to see certain patterns which MUST take place for a hacker to plant his flag inside a network. They need to keep some way to regain access to the same corporate network. Even if the attack is automated itself, through AI or scripted, the fact remains that the human hacker will need future access. The hacker will also need time to perform reconnaissance on what level of access they have, where they can travel within the network, and most importantly, how to increase their authority to have full access to all data, both on premise and in the cloud.

New vendors are taking advantage of this machine learning and creating agents for PCs that are similar to SIEMs, but which are specific to looking for the hidden hacker on your network. They often have an SOC behind them to perform the analysis and investigations needed to determine if an anomaly is a real threat or simply a false positive. The cost is significantly reduced since they are only looking for that needle in the haystack and not pins, thimbles, and other pieces of thread to go into the needle.

One More Security Tool, Is It Really Worth It?

For full transparency, I should admit we use two different breach detection tools working within our internal network. So, obviously, I believe they are worth the investment. But let's look at it just based on the evidence at hand. Given the statistics of the hidden hacker threat, is there a reason as to why it isn't worth it? Enterprise level breach detection does not have a small price tag, but neither does the cost if you really have a breach and the hacker has 6 months to go through your entire network. That single action could put your business out of business.

When I perform vulnerability assessments, the largest gap I see is the lack of serious security awareness training, but followed right behind it is no breach Detection at all. So, yes, I believe it is well worth the investment with today's Advanced Persistent Threat. I would not use these tools without the experts in the SOC. These folks work 24/7 and understand the threats intimately. Without the proper expertise in interpreting the data, the value is lost.

> **Are these tools perfect? No, but this is one layer of protection that has been missing from way too many networks, both government and corporate. This is the tool IT doesn't even know they need, YET.**

Conclusion – There's No Silver Bullet

No matter what defenses we create or how diligent we are at doing all the little things associated with a defense in depth, we will get outsmarted sooner or later. The SolarWinds Orion debacle should be the best example of this. When I give presentations on cybersecurity, I often use the analogy of a thief breaking into your home. Given enough desire and tools, no matter your defenses, the determined thief will gain access to your house. The best approach is to better protect your critical data, focus on its defense, and understand you are going to lose the battle elsewhere. Just don't lose the war.

Rick Rusch
CEO and Founder at Secure ERP, Inc.

in

Rick Rusch is the founder and CEO of Secure ERP, an Indianapolis based Cybersecurity & IT services firm, and refers to himself as a Cybersecurity Evangelist. Although he has worked in Information Technology for over 30 years, Rick has been focused on cybersecurity since 2015, educating business owners about the unprecedented dangers in the age of hackers and ransomware. Rick has been passionately speaking and writing on cyber risk and mitigation for over 6 years to organizations, conference attendees, and business executives, just like you. Rick is the proud father of two grown children, enjoys travel photography, and has degrees in accounting and computer science and is a CPA. Additional information may be found at www.secureerpinc.com.

UNLIMITED LEARNING OPPORTUNITIES

Now available in the eLearning format!

ISO/IEC 27001
Lead Implementer

IN ENGLISH

ISO 31000
Risk Manager

IN ENGLISH

→ SHOW ME MORE


#BeyondClassrooms

What Will the Cybersecurity Landscape Look Like in 2021?

BY JASON IKEGWU

2020 was a significant year for individuals and businesses alike. It was a year in which all aspects of our lives were drastically affected, exposing our collective fragility and increasing feelings of fear and uncertainty.

The COVID-19 outbreak forced people's lives to move online, both at work and in person, and digital transformation accelerated. Technology helped to maintain social and emotional well-being and helped many organizations stay afloat. However, this new reality has also led to an increase in the number of cyber-attacks. As cyber-attacks increase and new cybersecurity trends continue to emerge, organizations must take a proactive IT security stance to keep their operations safe. They must become more agile, flexible, and collaborative as they strive to protect their critical assets and infrastructure. They need to increase their digital security initiatives, change strategies, and educate employees about cybersecurity.

The year came with an optimistic outlook considering the current strides in developing vaccines for COVID-19. As businesses seek to transition to a new normal in 2021, we will examine some of the projections and expectations in the cybersecurity landscape and what will underpin organizations' cybersecurity priorities in 2021.

1. There will be an increased demand for remote working security.

As organizations embrace remote and smart working, remote access to corporate environments brings quite significant constraints for enterprises to protect and ensure secure access to their networks.

There is an urgent need for organizations to reimagine their cybersecurity approaches and evolve counter measures of protecting teleworkers in the emerging future of work.

In 2021, there will be increased adoption of remote and smart working models and organizations must proactively embrace the zero-trust architecture to combat remote working threats.

2. Multi-Factor Authentication (MFA) will be critical.

Nowadays, there are daily occurrences of authentication attacks and cybercriminals have perfected measures of using stolen usernames and passwords on underground forums to compromise organizations, using password spraying and credential stuffing attacks.

Over time, cybercriminals have perpetuated the act of syphoning billions of credentials from breached interactions and systems across the dark web and underground forums.

These databases, paired with the ease of automating authentication attacks, suggest that no internet-exposed service is safe from cyber intrusion if it is not using multi-factor authentication (MFA).

MFAs will be mandated as authentication requirements by regulators in many countries in 2021 and will be used to enforce and maintain security levels.

Organizations should therefore make adequate preparations for implementing different variants of MFAs to cope with the emerging trends and challenges.

3. The challenges around cloud security will increase.

Even though organizations were gradually migrating to cloud prior to 2020, the advent of the COVID–19 pandemic accelerated cloud adoption and empowered remote working and online collaboration.

This rapid migration and adoption of cloud opened up new security threats and vulnerabilities across different computing systems. Even though the traditional cloud technology was premised around functionality and convenience and not security. Cybercriminals are exploiting these gaps to perpetuate all kinds of havoc, including espionage and cross country cyber-attacks.

To protect its information assets, organizations will have to focus efforts on improving cloud security initiatives. Prevention and detection strategies will be crucial for all organizations, large or small, to protect themselves against these threats. Expanding the cloud's use will require organizations to improve the visibility of their cloud presence, assets, and vendor relationships to manage risks.

4. The adoption of technology-driven security tools will be rapid.

Today's most effective cybersecurity measures center around insight and response. The mechanism for providing spontaneous response and data-driven insights rests on technology. These technologies, including automated security tools and advanced machine learning

technologies, support decision-making and provide alerts on risky thresholds in tackling threats and vulnerabilities.

> **In 2021, the use of technology-driven security tools will be at the center of cybersecurity implementation.**

With growing data privacy awareness and the adoption of the GDPR globally come greater scrutiny from clients and consumers, who demand their sensitive information be kept safe. Legacy technologies built on static rules can simply not stand up to this pressure, and we are instead going to see even greater adoption of intelligent security technologies that use contextual machine learning to keep data safe.

Organizations will need to make conscious efforts to create security strategies and implement same with intelligent technology driven security tools and advanced machine learning technologies.

5. There will be an increase in ransomware attacks.

COVID–19 brought some social challenges, including latent economic exposures across the globe. Individuals who hitherto were dedicated to specific employment relinquished these jobs or earned less than required. Of course, this increased the number of cybercriminals who attack databases and block user accesses to demand ransoms before providing access to legitimate users. These ransomware attackers will be targeting corporate entities, holding company's databases in exchange for crypto-currency or other forms of financial compensation.

The greatest challenge with ransomware attacks is not only the reputational dent on the organization but also the transit data accumulated by the attackers such that even when the accesses are restored, the attackers can still use the retained data to blackmail the organization, make financial demands, and publicly expose the organization.

Ransomware is becoming more technically advanced and sophisticated. In 2021, ransomware attacks will be the most rampant attack across organizations. A number of entities will be targeted and compromised. Organizations therefore must prepare for ransomware prevention and recovery. Networks should be segmented and components hardened. Disaster recovery, business continuity, and data recovery plans should be in place and tested periodically.

6. New forms of 5G vulnerabilities will emerge.

5G technology will be one of the greatest drivers and revolutions of this decade, enabling the fastest and broadest connectivity for humanity. As the adoption of the 5G technology set in as the standard form of cloud-based data transfer and communication, more vulnerabilities, compromises, and new cybersecurity threats will also emerge.

In 2021, the 5G broadband will provide cybercriminals and hackers the capability to inject data packets across networks using high-speed data transfers and conduct corporate espionage with limited interference without these companies knowing. Organizations will need to prepare specially for the 5G technology adoption and provide higher levels of security scrutiny and monitoring. Training and awareness will be supreme in this crusade to provide the capacity and know-how within the organization.

7. The number of Advanced Persistent Threats (APT) groups will continue to grow.

There have been increased hackers and cybercriminals' activities across the clear, deep, and dark web using Advanced Persistence Threat (APT), with new groups emerging every day. The dark web for instance allows cybercriminals and hackers to have access to sensitive information and corporate networks, transact on stolen credit cards, etc. More actors are joining the foray and these groups are continuously growing across different sectors and interests.

This year, organizations will increase the digitalization of their processes using social media, web sites, mobile phones, and cloud. It is important that they keep a tight control over their digital footprint and keep track of it in real time and control all activities within the outlying borders of their extended organization.

8. Smart phones and mobile devices will be a target in 2021.

The proliferation of mobile connectivity across many networks in itself is a major cybersecurity challenge. Such mobile devices are being used directly to connect to corporate networks even in this remote working era. The attention in 2021 will be on mobile device attacks. The presence of advanced spyware and vulnerabilities in many mobile software applications will give cybercriminals access to valuable data. Organizations should create comprehensive cybersecurity programs to include accurate inventory to protect their information assets including nontraditional assets such as BYOD, IoT, mobile, and cloud services.

9. Organizations will pay more attention to cybersecurity.

With the expansion of remote working and increased adoption of digital transformation triggered by the COVID–19 pandemic, executive management has seen the reality of cyber risks and the implications to business continuity. This has elevated cybersecurity conversation to a board room agenda and most organizations are giving adequate consideration to information security as a strategic component of the business strategy.

In 2021, many organizations will be very deliberate in managing cybersecurity, including appointing the Chief Information Security Officer (CISO) as a C-suite within the executive management.

10. Cybersecurity automation will increase.

Cybercriminals have devised several ways of stealing and accessing corporate databases and networks and these techniques are being improved daily. Cybersecurity automation simplifies the response from organizations in providing a faster pace to response and an efficient mechanism for containment.

With the growth in the number of cyber-attacks and the increasing accuracy of cybercriminals in gaining access to systems, cybersecurity automation is a safe and effective solution to prevent cyber-attacks and data breaches.

In 2021, the focus of cybersecurity automation will include automation of threat correlation, automated enforcement of MFA on ANY resource, authentication sequence, vulnerability scanning, Penetration Tests, security patch management, traffic logs, etc.

Conclusion

In 2021, organizations will deal with the effects while striving to stay secure as online dependency grows. These suggestions and recommendations are not only plausible but should also be anticipated. We looked into the drivers of cybersecurity's near future and how organizations will have to adapt as threats and technologies exert their influence. It is pertinent that organizations and decision-makers frame a proper and strategic response that can withstand change and disruption.

Organizations need to be proactive in managing cybersecurity initiatives, including beefing up cybersecurity programs, implementing cybersecurity systems, managing vulnerabilities and risks, testing incidence response and business continuity plans.

Jason Ikegwu
Associate Partner at Phillips Consulting

Jason is a Partner at Phillips Consulting (pcl.) responsible for Digital and Technology Consulting. He has extensive experience in developing and implementing effective cybersecurity, digital, and technology governance and processes for top organizations in Africa. He is the first indigenous Payment Card Industry Qualified Security Assessor (PCI-QSA) in West and Central Africa and has conducted security assessments and implemented sustainable payment ecosystem infrastructure in over 20 countries. Jason is a business leader and certified trainer with over 45 professional certifications in cybersecurity, digital operating model design, project and program management, IT governance, risk management, agile, data analytics, platform management, and business innovation.

Cybersecurity in Healthcare: How to Manage Security Threats

WHAT EVERY HEALTHCARE ORGANIZATION SHOULD BE DOING NOW

BY ANGELA RIVERA

Healthcare has always intrigued me, not just as a career choice but as a patient. The amount of technology to support the patient experience, improve clinical outcomes, and support value-based care is enormous. While COVID-19 has forced healthcare institutions to pause on many planned initiatives to focus on getting us through this immediate global healthcare crisis, unfortunately, the need to focus on cybersecurity has never been greater. In healthcare, cybersecurity is so much more critical, as an incident is not just about losing or exposing personal information or losing money due to an intermittent shut down, it is a matter of life or death. A non-planned downtime can delay critical treatment or leave clinicians uninformed about a patient's history that could ultimately determine the outcome of care. An example of this was in September 2020 when a woman in Germany ended up dying after having to be diverted from the nearest hospital because it had been shut down due to a ransomware attack.

This criticality of keeping healthcare operations running optimally is what also makes it a prime target for hackers. The more sophisticated the industry gets with the use of technology, the more opportunities there arise for the hackers to be destructive. In the U.S. for example, the Health and Human Services Office of Civil Rights publicly reports any disclosed breaches affecting over 500 patient records. In 2020, the number of patient records exposed from reportable breaches affected more than 20 million patients. The majority of these breaches were a result of hacking of a network server or email. For more, data breaches due to attacks in the healthcare are expected to triple in 2021.

Unfortunately, the industry is very challenged in keeping the pace with the adaptability of today's cyber criminals. While there is a heightened focus by healthcare executives to invest in cybersecurity with the healthcare industry expected to spend $18 billion in 2021 on cybersecurity, that is not nearly enough and most security executives in healthcare even admit much is spent to recover after an incident rather than to prevent one.

Healthcare is complicated, but the core best practices for maintaining a secure environment are the same whether you are a small physician practice, a rural community hospital, or a large integrated delivery network.

Make no mistake, even the largest and most well-funded healthcare organizations have gaps in their security program and opportunities for improvement. The key for any organization is to focus on a few high-level priorities no matter where you are in your security journey. Do not try to tackle too much. For some reading this, this concept may sound basic, yet having managed a team that conducted hundreds of assessments per year from across the U.S. health industry, its most recent annual report of a full year's worth of assessments representing 278 facilities indicated that, "79% scored less than a "C" in terms of conformance with NIST CSF".

> ***Note:*** *The National Institute of Standards and Framework's Cybersecurity Framework (NIST CSF) is a standardized security framework for critical infrastructure in the United States and heavily adopted in the healthcare industry.*

In that same report, the category of hospitals and health systems specifically showed a 3-year trend of 50% conformance to NIST CSF. Unfortunately, healthcare organizations are having a hard time keeping up as threats get more sophisticated. So, for this article, I will focus on a few key recommendations that healthcare organizations of any type, size, and complexity can do to evolve their cybersecurity program.

I know you have heard it many times, but when it comes to improving their cybersecurity posture, organizations must focus on the best practice triad of "People, Process, and Technology."

People

In healthcare, we rely so heavily on the people who work in the healthcare environment to keep assets and data safe. There are the clinically trained doctors and nurses who deliver direct patient care and have access to patients' Protected Health Information (PHI) through electronic health records, or the non-clinical staff managing scheduling, registration, and billing who have access to a patient's financial information, or environmental services staff or porters who may be logging into or have their RFID name tags connected to systems that track room, bed, or equipment availability. We cannot forget the HR department staff who may have access to all of the employees' personal data that can be very valuable to a hacker. Unfortunately, all of this access makes people the weakest link for any organization.

From a hacker's perspective, people usually provide the easiest route into an organization. Taking advantage of the high rate of human error through phishing attacks or compromising emails can sometimes create the biggest challenges for a healthcare security team. While it seems basic, security awareness and training are highly impactful and often forgotten or accomplished through a one-time training upon hire or only annually. Security awareness training should be continuous and here are some tips to keep security top of mind:

- Educate your team on what they should be looking for in a phish and extend advice to outside of work. Training your staff on not only how to protect the organization's assets but also their own security away from the office offers more opportunities to get their attention. Making it personal helps build a culture of security they will carry over to the workplace.
- Encourage your team to speak up and ask questions without fear of repudiation for a mistake. This will make employees feel more comfortable to report their mistakes like falling for a phish. The sooner the security team is made aware of the situation, the better.
- Focus on access management. Larger healthcare systems tend to do fairly well at identity management, even implementing advanced technologies such as retinal or other biometric scanning solutions; however, it can all be for naught if there is not a strong focus on access management. Based on the size of the organization, it can be a heavy task requiring lots of input from end users, but authorizing access only to the systems that are critical to a particular role will reduce the attack surface of a potential hacker or an employee's human error or malfeasance.

- Continuously assess your security awareness effectiveness through periodical phishing and social engineering exercises. These can be done internally or outsourced, depending on the size and complexity of your organization and how advanced your team is getting at recognizing a phish. Long gone are the days when the phish was misspelled or the request was ridiculous like asking to wire funds to a foreign country. Today, many hackers spend time getting to know who the leaders in an organization are and are making the requests seem fairly realistic. So, performing periodic assessments combined with continuous training and empowering employees to question a request can significantly reduce potential penetration into your network.

Process

Through my experience as an Executive Vice President of a healthcare-focused cybersecurity, compliance, and privacy consulting company, it was interesting to find that healthcare organizations of all sizes still lacked some of the basic policies and procedures to effectively safeguard their organization. Some organizations have invested in good technologies but have focused too heavily on relying on the technology to solve their challenges. Often it is a failure in process and not the technology that causes the issues for an organization. A good example of this is with medical device security. There are many valuable tools in the market that identify the vulnerabilities of network-connected devices through continuous scanning, but there is so much more needed to run an effective medical device security program. From procurement to destruction of devices, organizations should have effective policies and procedures to address best practices to reduce the risk posed by medical devices. This requires collaboration between many departments (IT, Security, and Clinical Engineering to start) to implement an effective program. While not an all-inclusive list, examining how you are doing in the following areas is a good place to start.

- **Asset Management**

  Inventory management practices
  Ensure that all devices are accounted for and that the security team stays aware of any additions and changes. This is an area where larger organizations have more challenges as individual departments or divisions may procure and install devices without involving the security team.

  Medical device procurement
  Establish third-party security requirements that must be met before a new device can be purchased. Meeting a minimum criterion as established by your Risk Management Committee should be integrated into any procurement decision.

  Secure asset disposal
  Develop a specific protocol that all departments must follow before disposing or selling of assets to ensure that all data is removed from the device. And if you outsource this task to a third party, ensure that you receive certification and/or third-party validation of the sanitation.

- **Vulnerability Management**

  Develop a process to prioritize your vulnerability management based on risk levels. Most medical devices are serviced by the clinical engineering department based on a set service schedule recommended by its manufacturer based on install date or life stage of the device. However, the criticality of the device and identified security vulnerabilities should be taken into consideration. While it is understood that many devices are very old and may not be able to be patched (those should be segmented), devices that can be patched should be moved up in the service schedule when high and medium-risk vulnerabilities are identified.

Technology

IT, compliance, and security executives are approached by thousands (yes, thousands) of security product companies out in the market. With the daily barrage of notices of ransomware attacks, breaches, etc., these security companies find it easy to use fear, uncertainty, and doubt (FUD) as a sales approach to persuade and pressure business leaders to purchase security tools giving them a false perception that they will be safe. Do not get me wrong, there are very valuable tools in the market, but before you buy, make sure you take a breath and evaluate the people and processes you have established to maximize the purchase and truly reduce your risk. At my last company, we often found that our clients had purchased security technologies that either were not fully implemented, or they did not have the staff to timely remediate the identified vulnerabilities resulting from those tools. Knowing your risks and not fixing them can create additional liability to your organization. But do not hide your head in the sand, because not trying to determine your risks can be considered negligent.

The majority of breaches occur on end-user systems (laptops and desktops) so at minimum, your security tools should include endpoint security and email protection software with 80% of effort focused on maximizing the effectiveness of these tools. Combined with this is effective and complete vulnerability management based on the important information that comes from these tools such as prioritized vulnerabilities and misconfigurations on your most critical assets. The key word here is "complete" as many organizations struggle here as they either do not have the trained staff or the budget to hire a team to tackle these never-ending vulnerabilities. For those parents out there, it is like laundry. As soon as you have finished all of the laundry, your kids have already filled their hampers with more to clean. It is never ending. Unfortunately, these activities are where organizations will find the most value from their security program so if you cannot do this on your own, investigate firms that can support you here.

As mentioned above, executives are inundated with news and FUD around breaches and attacks which can be very overwhelming and make it difficult for organizations to know where to focus. Regardless of where you are in your security journey, revisit the basics by starting with your assets — all of them (hardware, software, and data) — and ensure you are maintaining an up-to-date asset inventory. It serves as a useful mechanism in assisting in the development of a comprehensive, enterprise-wide risk analysis, to help organizations understand all of the places that ePHI may be stored within their environment, which will not only help comply with government standards (i.e., U.S. HIPAA Privacy and Security regulations), but also prioritize any necessary security tool improvements, or administration (people and process) tasks such as policy and procedure development and training, that is necessary to strengthen your security environment. This is actually an area where a tool purchase can be very helpful to stay organized. Depending on the organization's size and complexity, the cost of these tools can be fairly inexpensive. Prioritizing your efforts with the most critical life-sustaining systems and data (PHI and employee data) in mind should get the most attention. Avoid taking a blanket approach to securing your assets equally, because no matter how much money organizations pour into their security program, it is impossible to secure all of your assets equally. Your assets are not equal. You will be better served by taking a tiered approach to cyber health governed by business priorities.

Bottom line, focus on the basics, do not get rattled by all of the FUD you are getting from the industry vendors. Once you have stepped back and taken a fresh perspective at your environment encompassing people, process, and technology, re-prioritize your efforts to truly make an impact in your environment. If you want a way to clear your mind, check out this new and quick comic series e-book from my teammates at Cyvatar "8 Epic Cybersecurity Fails."

Good luck!

Angela Rivera
MBA, FHIMSS

Angela Rivera is a passionate executive with more than 25 years of experience in the healthcare technology industry with significant focus serving the healthcare provider industry. Ms. Rivera currently serves as a member of the Board of Advisors and Health Sector Lead for Cyvatar, a transformative cybersecurity company offering cybersecurity-as-a-service with measurable outcomes. Ms. Rivera also served as Executive Vice President of Operations for CynergisTek, a Best in KLAS healthcare-focused cybersecurity, privacy, and compliance consulting firm. Prior to CynergisTek, Ms. Rivera served for 17 years at Computer Task Group, an international IT solutions and services company. Ms. Rivera serves as an advocate for the advancement of women in technology and currently serves on the Board of Directors for Women in Healthcare Information Technology (WHIT) and was named "Women in Healthcare IT to Know" by Becker's Hospital Review in 2018 and 2019.

Walid Charfi's Career and Success in Cybersecurity

How PECB Certifications were a determining factor to the recognition of my 20 years of expertise which lead to the founding my own consulting firm – W.A. IT ADVISORY.

I am writing this article and the challenge is becoming more severe as we observe the impacts of the pandemic on businesses in particular and nations in general. Maybe a post-pandemic success story will extend the lessons to learn from the professionals and the companies proving a success to jump from survival mode to a stable or evolutive mode.

Praise be to God who helped me achieve all the successes in my career. All my gratitude to my kind honorable parents who raised me and who did not spare any effort encouraging me and giving me life and ethics lessons, so that I am the man I am.

This is how I begin my success story. In fact, my beginnings were multiple, and the successes were several, so let us commence with the time I obtained my national diploma of Engineering in Computer Sciences from one of the finest universities, and a pioneer in teaching computer sciences in Tunisia, which I call "the Faculty of Science of Tunis". My choice of engineering studies was not random, and it was to me a firm conviction ever since I got my high school diploma in 1995.

First Choice in My Career

To me, the year 2000 stands out as the year in which I started my career. That year had a great global impact on the history of computers. Everyone does remember "Millennium bug", we ITs, were the real stars of year 2000. That year marked the beginning of the global awareness on IT and its threats. I remember that the summer of 1999 was a particular occasion to take a key role in the "Caravane 2000" national campaign to conduct an awareness program about ultimate risks in the south region of Tunisia with my colleague and our teacher in internship co-organized by the Tunisian Government and the Computer Science Department at the university.

By July 2000, I had to look for my first job, and as usual, I was not the man to pick the easiest job. Most of my peers begun working as software developers, and at that time, these companies were mass recruiting and offering a very respectable salary. The choice seems obvious, but I focused on selecting a new challenging job with the highest added value specialty.

So, I joined the French company "NEUROCOM" which is specialized in information and network security. I kept endeavoring with the information security realm since then, and thankfully my success in it was sprawling. Yes, this is how I describe my successes, mostly because I was successful in all my assignments which I started as a diligent young engineer and then as an auditor keen to perform my duties in the best professional way possible and attempted a higher level with the next exercise.

Teaching Experience and Career Path Advice to Students and Young Professionals

All along my career I have also been a university teacher and had many related roles along the way. I was simultaneously the teacher in the classroom, the researcher in the laboratory, and the mentor and coach to my students with their projects and trainings.

My teaching experience is still the most delighting to me as it was very enriching to my personality at various plans. It is always very satisfying and overwhelming to sense my students' regard and admiration, whenever we meet again by coincidence or they try to reach me on purpose. I never estimated the care that I used with my students, more than a strict obligation and a responsibility toward them. Nevertheless, I feel proud when they express their sincere gratitude and recognition and I feel way prouder of them when seeing that I succeeded to positively influence them. That feeling makes me regain faith in that "good seeds, with proper care, will last as a long strong tree".

Here, we reach an important stage of my journey as a trainer. In this role, I succeeded combing pedagogics and intensive experience in cybersecurity, governance, risk management, and auditing information systems. As per the same personal approach, I endorsed this aspect of my profile by the most prestigious and significant certifications including, but not limited to, "COBIT5®", "NEXUS CSX®", and several technical certifications issued from CISCO, Microsoft, Huawei, and LPIC.

Information Security and Information Systems Auditing

After being involved in computer security audit missions as a young computer security auditor during my first experience, the label of auditor in computer security engraved, and I became recognized in Tunisia among the first auditors specialized in IT security since 2002. Therefore, following the initiative of the Tunisian government and after the creation of the information security agency "ANSI" and the publication of a 05-2004 law, I was selected to be part of 40 auditors who successfully passed the Information Security Expert Auditor Certification. This national certification is required to conduct audits as required by the 05-2004 law that obliges public and private organizations in Tunisia to annually conduct an information security audit. In 2010, I received recognition from the national security agency as they appreciated my audit reports in information security related to the mission I have directed for financial institutions and companies in different fields of activity (oil and gas, industrial, etc.).

Since 2005, I was invited as a speaker in national and international professional and scientific events. I have also presented some researches between 2006 and 2008 related to Wireless Sensor Networks recently known as IoT (Internet of Things) published in IEEE Conferences proceedings and international journals. From 2009 until now, my conference activities mostly focus on Cybersecurity and IT governance like HSSE Conferences, Cybersecurity Forums, Conferences and CTF, ISACA events, etc.

I was honored to be ISACA's Tunis Chapter President from 2018 to 2020. It was a continuity of my achievement as the founder of the first chapter of ISACA in the North African region since 2013. The roles that I have in the chapter and my contribution to make ISACA frameworks and certifications known in local universities, the improvement of academic and professional membership in addition to the assistance of students to launch the students groups. It was the association role that I played with several associations mainly the technological communities: IEEE and ISACA.

PECB Certification, the Success Factor

The greatest recognition of my expertise was by successfully passing the examinations and obtaining PECB certifications: "ISO/IEC 27001 Senior Lead Auditor","ISO/IEC 27001 Senior Lead Implementer", "ISO/IEC 27032 Senior Lead Cybersecurity Manager", and "ISO/IEC 27005 Senior Lead Risk Manager". After that, I have been recognized as "Certified Trainer" by PECB.

PECB Group Inc. is a certification body which provides education[1] and certification under the standard ISO/IEC 17024 for individuals on a wide range of disciplines and helps professionals and organizations to show commitment and competence by providing them with valuable education, evaluation, and certification against rigorous internationally recognized standards. It provides training courses for ISO/IEC 27001, ISO 9001, ISO 22301, and ISO/IEC 27701.

As a PECB Certified Trainer, I successfully organized and delivered PECB training courses to a wide spectrum of learners. I contributed in developing the skills and industry-specific knowledge of students, junior and senior professionals also managers and executives. I accompanied them to obtain their certifications which was the recognition of their efforts and the confirmation of what they have acquired as knowledge and skills during my trainings. I am proud of each one of them. The successes and accomplishments of whom attended my trainings is mine and increases my comfort to the quality of the coach and mentor that I aim to be. This worldwide recognition by earning PECB and ISACA certifications offered me the opportunity to be mandated by the Tunisian Accreditation Council — TUNAC (The National Council of Accreditation) as an assessor to conduct missions and supervising management systems auditors and participating in certification bodies' assessments based on ISO/IEC 17021-1 and ISO/IEC 27006. I was also invited by TUNAC to train assessors in the topics of information security management systems implementation and audit and explain the requirements of ISO/IEC 27001 and ISO/IEC 27006.

W.A. IT Advisory Founded to Promote Training and Advisory in Governance and Cybersecurity

Training is the professional service that I enjoy the most, among all the services that I deliver to businesses. All along my career I got involved in many missions in which I engaged my expertise to add value to companies and institutions. I worked on raising their overall

[1] Education refers to training courses developed by PECB, and offered globally through its network of resellers.

performance, promoting their digital transformation, and increasing their information systems and networks' security and resiliency.

Driven by virtuous beliefs and principles, combined with hard work, this is my formula to double success, as I had to endeavor on both education and professional services. This combination maxes success indicator and candidates to reach records in every life or career project.

Here I am, after 20 years, looking at that young engineer in systems and networks security growing to an expert auditor and a PECB certified trainer, owner of his own governance and cybersecurity consulting firm "W.A. IT ADVISORY".

Strategic Vision after PECB Recognition and Partnering

I introduce you to my business that I recently founded "W.A. IT ADVISORY" which is a PECB partner in Tunisia, North Africa, and the Sub-Saharan region. It provides training courses of ISO/IEC 27001, ISO 9001, ISO 22301, and ISO/IEC 27701. It also provides training on a decent variety of other management systems standards, as well as standards' guidelines such as ISO/IEC 27005 in risk management and ISO/IEC 27032 for cybersecurity management program and other guidelines related to quality.

I am proud of and trust that our partnership with PECB is a successful strategic direction and I am considering developing more and more in the information security management realm by accompanying businesses to certify their management systems, and to certify their staff as well, partnering with PECB.

Additional partnerships were concluded in the last 2 years with a specialized firm in cybersecurity and investigation, Nuix Company, with distributors in IT and Security solutions, Ozone and Ingram Micro. Other partnerships are in progress with editors of vulnerability scanning and threat detection solutions and editors of Data Historian and Operations Management Systems for industrial Systems supervision. All upcoming partnerships will be published soon in our website.

Me and PECB agree passionately on that we should move "Beyond Recognition", and here I want to express my recognition to all the people around me who inspire me... my wife with all the sacrifices and continual encouragement, my brother and sisters with their cheer, my son and daughter with their inspiration, and my friends and colleagues who contributed so much to my success. I also address my distinguished recognition to my first school, the "Boy Scouts", which taught me "Life" and shaped the core of who I am.

PECB ANTI-BRIBERY 2021 CONFERENCE

MAY 17-20, 2021

Over four days, with three sessions each day, more than 30 panelists will participate in inspiring discussions related to different topics about anti-bribery and COVID-19, blockchain, artificial intelligence, whistleblowing, and more.

This year's first conference will be held virtually and will include sessions in three languages: English, French, and Spanish.

→ REGISTER NOW FOR FREE

For further information, please visit the following link
or contact us at events@pecb.com

Artificial Intelligence Tools in Cybersecurity

BY ENDRITA MUHAXHERI, PECB

Cybersecurity continues to be a hot topic. According to a World Economic Forum report, the global spending on cybersecurity has now reached $145 billion a year, and by 2035 it is expected to exceed $1 trillion.

As cyber threats become more complex, AI for cybersecurity has become necessary and is becoming a game-changer. Therefore, organizations are massively investing in Artificial Intelligence in order to help cybersecurity professionals identify potential threats, take protective measures, and accelerate response time. By analyzing large quantities of data, AI manages to speed up response times and enhance under-resourced security operations. In this article, we present four cybersecurity AI tools, which you might find useful and start using them in the future.

IBM QRadar Advisor with Watson: By using the cognitive artificial intelligence of IBM, this tool helps reduce the duration of incident investigations. It performs an automatic incident investigation, detects threats with higher risks and it prioritizes the list of investigations based on the greatest risks. In addition, this tool provides insights about users and critical assets. The more details and information you have during an incident investigation the better, that's because it allows an organization to save a lot of time and effort.

In addition, by using external threat intel feeds, Watson provides great feedback. This is done by applying cognitive reasoning, which helps in identifying the possible threats and connect threat entities related to the original incident such as mistrustful IP addresses, malicious files, etc. Depending on the edition you select, this tool also meets the requirements of ISO/IEC 27001.

Targeted Attack Analytics (TAA): Developed by Symantec by employing AI and Machine Learning, this tool is used to discover hidden and targeted attacks. These hidden cyber-attacks, if not treated, will give hackers access to systems. TAA reveals suspicious actions at each endpoint and gathers information to define whether each action has hidden malicious activity. This will allow users to identify the threat and take the necessary actions. It's free of charge for existing Symantec Advanced Threat Protection (ATP) customers.

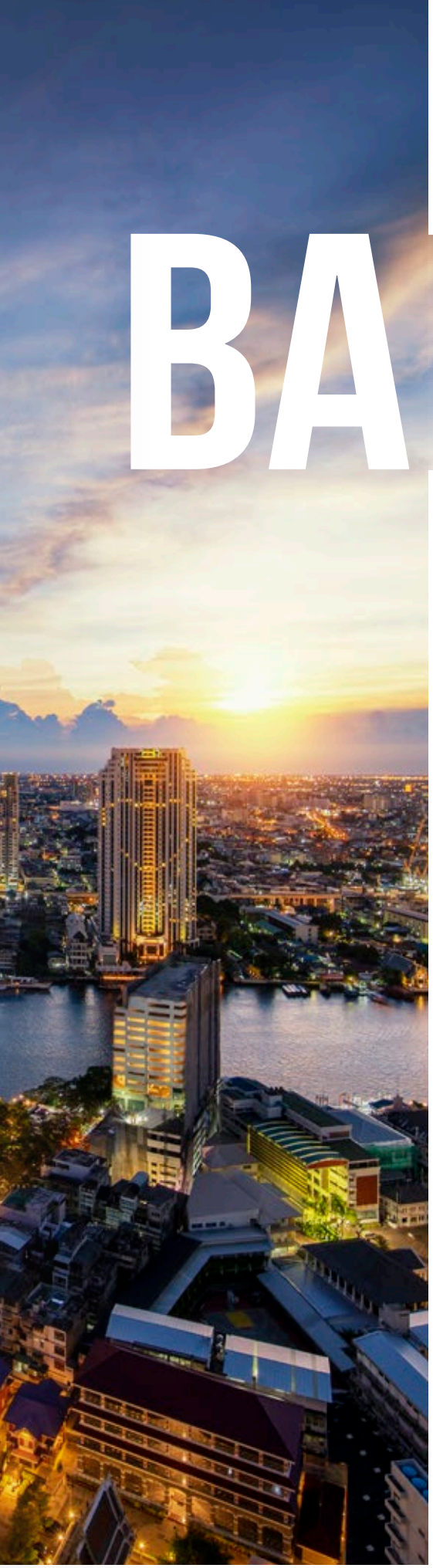
Sophos' Intercept X tool: This tool is integrated with a deep learning neural network, which helps protect against different malware attacks. It has different specific defense measures, including network threat protection and malicious behavior detection, scanning of files in real-time, data loss protection, etc. Its predictive approach allows users to protect against both known and unknown threats. From detection of malware to ransomware protection, it is packed with layers of robust security. Moreover, it has good reporting features including alerts sent to the admin if there is something wrong with the tool. This tool has no free version, however, a 30-day free trial is available.

The usage of deep learning technology makes this tool more adaptable, functional, and powerful against unknown and complex threats. Deep learning is used for the purpose of outperforming endpoint security solutions that use traditional machine learning or signature-based detection alone.

Cognito: Developed by Vectra, this tool is an AI-driven threat detection and response system inside the cloud, data center, IoT, and enterprise networks. In real time, it gathers, identifies, and prioritizes the biggest risks and responds with automated alerts to the security employees, which allows them to respond in a timely manner. Moreover, it quickly identifies hidden attackers through a combination of machine learning techniques. It has no free version, however, it offers a free trial and you can request a 30-minute demo.

Due to their ability to analyze a much greater volume of data compared to security professionals, organizations should consider adopting these new technologies in order to accelerate growth and stay ahead of threats. AI is one of the tools that will impact most areas of cybersecurity. That is why organizations should keep Artificial Intelligence on top of their cybersecurity strategies.

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.



BANGKOK

The City of Angels

Ranked among the world's most visited cities, Bangkok is an affordable place that always has something new to offer. It is a perfect mix of culture, food, shopping, and nightlife. There is never a dull moment in this place, and once you visit it, you will understand.

Known for its tropical climate, myriad of attractions, restaurants to explore, and friendly people, the best time to visit Bangkok is from November until February. If you happen to visit Bangkok during these times, please make sure to check the travel guidelines and gain information on travel restrictions, since they change very often due to the situation with the pandemic.

The Peninsula Bangkok Hotel

Getting to Bangkok

Suvarnabhumi International is approximately 30 kilometers east of the city. It takes around 30 minutes (depending on the traffic) to reach Bangkok's Central Business District (CBD) from the airport. The cheapest and fastest way to reach to the city center is through the Airport Rail Link City Line which costs 45 Baht per person. It leaves every 15 minutes, and takes 25 minutes for the whole distance, including the stops. You can then take a taxi from your stop to your final destination. The other convenient option is taking a taxi. Taxi lines are located on the ground level of the airport. Taxi trips will cost around 300-500 Baht (around 8-14€).

Where to Stay

Bangkok is a popular tourist attraction and therefore has a lot of accommodation options for all budgets.

Luxurious

The Peninsula Bangkok – Known for its great location, you cannot go wrong by booking here. Located along the bank of the Chao Phraya River, this hotel offers a classical design and great views of the Chao Phraya River, with delicious food, excellent service, and great amenities. It is around a 45-minute drive from the Suvarnabhumi International Airport. The Grand Palace and Wat Arun Temple are within a 20-minute ride from the hotel.

Mid-Range

Avani and Riverside Bangkok Hotel – Similar to the previously mentioned hotel, Avani offers great views of the Chao Phraya River. It is a gem in the BKK city with stunning views and very attentive staff, who will do their best to make your trip a memorable one. The rooftop bar and restaurants offer a great selection of food. The rooftop infinity pool located on the 26th floor is another bonus. The hotel offers a free shuttle boat that runs frequently to the first river taxi stop which is very helpful.

Budget-Friendly

Vera Nidhra is a small boutique hotel with a positive ambiance. It is a convenient place to stay and it offers a warm, friendly, and comfortable feeling. Popular landmarks are not far from this hotel and the Iconsiam shopping center is very close too. The staff is really helpful and friendly and helps you in experiencing your trip itineraries to its fullest.

Working, Relaxing, and Exploring the Best of Bangkok – How You Can Spend a Day in Bangkok

Grand Palace

King Power Mahanakhon building

Iconsiam Shopping Mall

6:30 – Start your day early with a happy and healthy ride and cycle in the Bangkok Sky Lane – a 23-km cycle track. A must for cyclists of all levels and ages and a great way to see the airplanes up close as they take off and land. Bring your ID for free registration.

8:30 – Get back to your hotel and have some breakfast. We recommend choosing the hotel near BTS Skytrain station for the ease of moving around Bangkok. If you are looking for a luxurious stay, consider Siam Kempinski Hotel Bangkok. With stylish and spacious rooms, multiple pools, and three restaurants offering an international buffet breakfast and modern Thai cuisine, this hotel is known for its amazing service and convenient location.

10:30 – Visiting the Grand Palace. Situated at the heart of Bangkok, and known for its history and beauty, the Grand Palace is comprised of more than 30 buildings and is a top tourist and visitor attraction. It is an amazing experience you cannot miss. Open from 8:30 a.m. until 3:30 p.m., the price per person is 500 Baht (around 14€).

12:00 – Having lunch at 80/20 Eighty Twenty, a restaurant which was recommended by Michelin guide. A place with an excellent and innovative menu, a relaxed and energizing atmosphere, and attentive service. A unique Thai food experience.

14:00 – After having a great lunch, treat yourself with a foot massage of your choice in Khao San road. It is a great way to prepare for the rest of the day. Another option is to spend your afternoon reading and enjoying afternoon tea or coffee at the coffee shop at Bank of Thailand Learning Center with a view of the Chao Phraya River.

17:00 – Catching Bangkok skyline atop Bangkok SkyWalk at Mahanakhon Building, the tallest building in Bangkok. This is a must-do experience. On level 78 you can enjoy cold drinks, clear your remaining works for the day, while catching a sunset view across the Bangkok skyline.

18:30 – Enjoy a fine dining experience and have a Thai & Italian fusion meal and a nice cocktail while overlooking Chao Phraya River at Fallabella River Front – a terrace restaurant located on the top floor of the Iconsiam Mall.

20:00 – After you enjoy the great food at Fallabella, reward yourself or your loved ones by shopping at Iconsiam, one of the largest shopping malls in Bangkok. Once you step inside Iconsiam the first impression is WOW. With a lot of high-end stores as well as local products, movie theaters, restaurants, lounge spots, and more, this impressive mall simply has it all.

Attractions

I mentioned earlier that visiting the Grand Palace is a must. After Grand Palace continue your visit to the Wat Phra Kaew know as the Temple of the Emerald Buddha. It is a great sight to see, both because of its history and its beauty. In order to avoid the biggest crowds and heat, come early to the temple. There are plenty of beautiful temples to walk around. The highlight of this visit is sitting in the room with the emerald Buddha. Be cautious and respectful inside the temples, the rules are clearly written down on the walls.

After that you should visit:

Wat Pho, also known as the Temple of the Reclining Buddha, makes an excellent addition to your palace tour. Located not far from the Grand Palace, it is one of the oldest Buddhist temples. It is breathtaking and enormous, an absolute must-visit. When inside, you are given a bag for your shoes and you walk around barefoot. The entry fee is 200 Baht (around 6€) and it takes around an hour and a half.

Wat Arun, located on the other side of the river from the Grand Palace and Wat Pho, is one of Thailand's grand historical landmarks. Known as the Temple of Dawn, this temple is partly made up of colorfully decorated spires and is absolutely splendid at sunset. Once on top, the views are surreal. I suggest you take a boat to visit the temple. The recommended time to spend here is around 1 hour and the entrance fee is 100 Baht (around 3 €) for foreigners.

Wat Traimit, also known as the Temple of the Golden Buddha, located in Chinatown, is another beautiful temple you should visit. It is hard to take your eyes off the Golden Buddha. The extremely shiny Buddha weighs 5.5 tons. Admission to the temple complex is free. Visiting the museum costs 100 Baht (around 3 €) for adults and 60 Baht (around 2 €) for kids.

Chinatown – Bangkok's Chinatown is the largest Chinatown in the world. Once you visit it you realize what makes it so unique. I suggest you spend at least 1-2 hours here. If you are interested in traditional Chinese food, you can find small places where you can buy delicious food. The mix of Chinese and Thai cultures makes this part of the town

Wat Pho Temple

Wat Arun Temple

Lumpini Park

unique and attractive, with stunning temples, exotic street foods, and more.

Chatuchak Weekend Market – This is the largest market in Thailand. Crowded streets, lots of sellers, the smell of street food, all make it a destination you should not miss. It is open on Friday, Saturday, and Sunday. Here you can find anything you can think of, including food, pets, and pet accessories, clothing and accessories, handicrafts, souvenirs, art, etc. Even though it is massive and it looks hard to navigate, there are signs and maps in English and tourist advice booths.

Lumpini Park – If you are interested in visiting a green space, this park in central Bangkok is the answer. It is opened from 4.30 a.m. until 9:0 p.m. and has an outdoor gym, paddleboats, and playgrounds. A great place with refreshing surroundings to get some peace and tranquility away from the noise and bustle of Bangkok life.

Cafés and Restaurants

After a long day of walking around, a coffee break is all you need.

ROAST Coffee & Eatery is a popular café with a nice ambiance, excellent service, and amazing food, including waffles, pancakes, a lot of drinks, desserts, burgers, etc. Their coffee is great too. I suggest you try the Iced Espresso Latte. If you plan to go on a weekend, make a reservation or go early because it is always full.

Shugaa is an awesome place with interesting plates and a creative menu, as well as a unique interior design. Everything here is homemade, delicious, and beautiful. These desserts are works of art. Without a doubt, I recommend stopping by if you are in the area. The icing on the cake would is the warm service provided by the staff.

The Best Places to Eat

They say that Bangkok is a food lover's paradise. It is not just the flavor of the food that makes it interesting, but the vibe of the areas that sell the best street food too. Apart from the Fallabella that I already suggested, here are some other suggestions:

Raan Jay Fai is known for her Michelin-starred street food and is a bucket list experience. The woman running the business turned 75 in 2020 and still has a lot of energy. Considering that you have to wait long to get seated, try to avoid peak times, or book in advance. I suggest you try the delicious crab omelet. Even though eating here might be a bit pricey, it is worth every baht.

The Deck – Even though street food is the best, there are also some luxurious restaurants that offer a panoramic view of the skyline of the city. The Deck by the River Restaurant is located directly on the bank of Chao Phraya River and you can enjoy the view over Wat Arun (the Temple of the Dawn). With excellent service, great food, and a view beyond words, this place should be visited.

Partnership with PECB: A Source of Success

ACinfotec has established a partnership with PECB since 2011 and conducted the first PECB training course in the same year. Now, it is the only Gold-level partner that delivers PECB training courses to the Thailand market. All classes are led by a consultant team with hands-on experience in the field, making participants get useful and practical advice they cannot find from other training providers. In October this year, we will celebrate the 10th anniversary of ACinfotec and PECB partnership with new training courses, updated services, and promotions to customers.

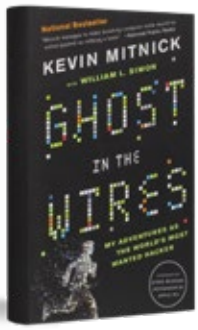
Sasawat Malaivongs
Business Director
at ACinfotec

Mr. Sasawat is a well-known pioneer of the ISO/IEC 27001 industry in Thailand. He has contributed to mapping Thailand as one of the key countries with organizations successfully achieving the ISO/IEC 27001 certification. He holds the ISO/IEC 27001 Master credential and many other certifications from PECB. He is currently managing the security and privacy consulting services of ACinfotec.

Best Cybersecurity Books to Read in 2021

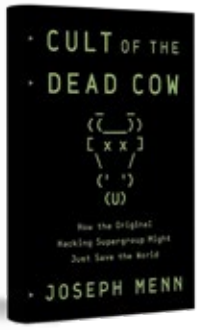
It is no news that cybersecurity is everyone's responsibility and not just an IT department's problem. Due to the incredible speed of the advancements in the cybersecurity field, new job opportunities are flourishing. That is why cybersecurity skills continue to be on top of the lists as technology in-demand skills.

If you are interested in entering this world of opportunities, these books will be a great source and will introduce you to the information you need to get started and be ahead of the game. This article will take you through the top books that you should read in 2021. These books are packed with insights from real-world situations and examples that will teach us what to look out for so that we are equipped with the right information and prevent ourselves from falling prey to cybercriminals.



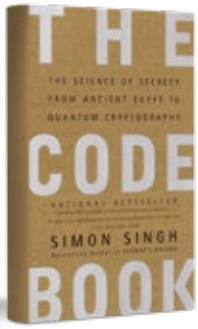
Ghost in the Wires: My Adventures as the World's Most Wanted Hacker by Kevin Mitnick and William L. Simon

Ghost in the Wires is a fascinating book covering a very important topic: Social Engineering. This book has been written by the world's most wanted hacker, in a way that most people can understand. It presents thrilling true stories on how he got started, his successes, betrayals, and lessons learned. It provides an understanding of social hacking and insights on the rise of information technology, which will help you understand a hacker's mindset. Kevin and his co-author provide valuable insights on how to be aware of the security risks of today's digital world.



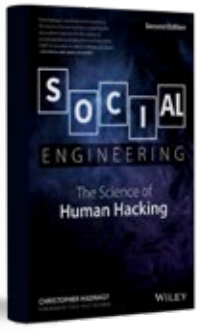
Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World by Joseph Menn

Cult of the Dead Cow is a highly informative book, suitable for non-IT readers too, which engages readers that are interested in the history of computer hacking at the beginning of the internet. The author does a very impressive job in telling the story of one of the most influential hacker groups, Cult of the Dead Cow. Readers will have the chance to explore the deeper impacts of the early hacker culture as told by people that lived it. It provides insights into how companies, governments, and criminals came to hold immense power over individuals and how they fought against them.



The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography by Simon Singh

This is a perfect book for individuals that like science and history. It is an interesting introduction to the world of cryptography where the author offers a glimpse of the codes and cryptography world, from ancient text to computer encryption. The author provides portraits of the remarkable personalities who wrote and broke the world's most difficult codes as well as technical and mathematical explanations.



Social Engineering: The Science of Human Hacking by Christopher Hadnagy

It is known that targeting a human is sometimes the easiest way to gain access to computer systems, because it is easier to only ask for access than to hack into something. This is a well-written book and perfectly combines useful knowledge together with actionable techniques. In this book, the author explains the most used methods, and the psychology behind each interaction, which in some cases fooled even the most experienced security employees. Packed with examples, personal stories (successes and failures), and the latest methods, this book shows you how to identify, predict, and avoid social engineering. By gaining a thorough understanding of this book, you will be able to protect yourself as well as your company from potential cyber attacks.

Privacy in the Twenty-First Century – ISO/IEC 27701:2019

A continued commitment to achieve privacy by design and comply with the new requirements

BY AL MAHDI MIFDAL

Information security can make or break an organization. From moment to moment, millions of bytes of data stream across data networks, protected by security. However, as we know now, not all security is foolproof. The world of cybersecurity is always in flux. It is a constant arms race between malicious users and cybersecurity professionals. Data privacy is one's (or a consumer's) understanding of their rights regarding how their personal information is being collected, used, stored, and shared. Information privacy is the relationship between the collection and distribution of data, technology, the expectation of privacy by the public, and the legal and political issues surrounding them. Data and information privacy protection relies on effective cybersecurity implementation by organizations to secure personal data both when in transit and at rest. For businesses, especially, it is beneficial to have an international standard that focuses on privacy. ISO/IEC 27701:2019 is that standard.

This standard demonstrates why improved privacy protection in a tech-driven world is crucial. Organizations need to protect not only their own data but that of their customers as well. When ISO conceived of this certification, the impetus was to help businesses have a framework to establish a Privacy Information Management System (PIMS). But what is ISO/IEC 27701, and what does it require for a company to attain certification?

Introducing ISO/IEC 27701

The ISO/IEC 27701 standard was published in August of 2019 as an extension to the ISO/IEC 27001 and ISO/IEC 27002 standards. The standard was prompted by concerns that personal data was not conforming to privacy expectations. As with most other ISO standards, continual improvement is a core aspect of ISO/IEC 27701. However, unlike other ISO standards, there is no demand for organizations to cover all the bases for them to be compliant with it.

In this way, most security professionals consider ISO/IEC 27701 an "add-on" rather than a standard on its own. Primarily, it deals with personally identifiable information (PII) and how an organization handles it. ISO itself notes that the standard deals with accountability and responsibility for managing PII, both from controllers and processors.

> **For a business to successfully be compliant with ISO/IEC 27701, it needs to understand the context in which it uses PII and how its processes may become vulnerable. Before an organization can realize ISO/IEC 27701 in its entirety, it must first pinpoint the difference between controllers and processors.**

Controllers vs. Processors – What's the Difference?

When one inspects the ISO/IEC 27701 standard, it states that the standard applies to both controllers and processors. In context, the controller is any entity that provides the reason for the collection of PII. A processor may or may not be a separate entity that processes that collected PII. The law considers both entities as unique individuals. If a processor is to hire another individual or company as a sub-processor, the standard also applies. ISO/IEC 27701 is in force regardless of the business's sector and factors in the GDPR, ISO/IEC 29151, ISO/IEC 27018, and ISO/IEC 29100 standards. Specific requirements outlined by the ISO/IEC 27701 standard that apply to both controllers and processors are as follows:

Record Keeping: Most ISO standards require extensive record-keeping and ISO/IEC 27701 is no exception. Organizations must have a written record of PII transactions, including those between jurisdictions and disclosures to third parties.

Internal Processes: In addition to documentation, the organization looking at certification needs to adopt strategies and policies regarding how they deal with specific incidents, such as security breaches, for example.

Training: Tech Republic notes that more than 40% of all corporate security breaches come from staff. Training is, therefore, a requirement to ensure that team knows the risks associated with their behavior.

Oversight: Organizations must have an individual responsible for ensuring that the guidelines of ISO/IEC 27701 are followed throughout the organization. They are responsible for developing, maintaining, and monitoring the current and future performance of the security system.

Risk Analysis: Organizations have to perform a risk analysis to verify any PII processing risks within the company's existing processes.

Confidentiality: At the heart of ISO/IEC 27701 is confidentiality. Businesses must have a confidentiality agreement in place that each individual or entity accessing PII needs to understand and sign.

Requirements Related to Controllers Only

While the abovementioned requirements apply to both controllers and processors, a subset of requirements apply just to controllers. These are:

Privacy by Design/Default: Controllers are required to adopt processes that rely on privacy by default and privacy by design. Privacy by design refers to designing technology that addresses privacy as one of its core concerns. Privacy by default means that controllers should assign a high-default security value to PII.

Individual's Rights: Empowering the individual is also high on the list of considerations for ISO/IEC 27701. The standard allows individuals the right to access, erase, and correct their PII if they so choose. They are also entitled to object to or restrict the use of their PII by organizations if they want to.

Requirements in Processor Contracts: Controllers need to have a written contract in place with their chosen processors which address certain items such as limiting the processing of PII to the specific reason it was collected and requiring processors to state if breaches of security occurred that may have impacted the protection of the collected PII.

Privacy Policies: All organizations must have a privacy policy in place which outlines how the entity will collect, process, and use the data. Processing can ONLY be done within those tightly defined parameters.

Requirements Related to Processors Only

Processors have to maintain the ISO standard on behalf of the controller. In essence, the controller is the processor's client. There are a handful of requirements that only apply to processors outlined in the ISO/IEC 27701 standard. Among these are:

Disclosures and Transfers: If the processor intends to transfer PII between jurisdictions for any reason, they are required to inform their clients of that decision.

Subcontractors: Processors can only hire subcontractors that conform to the terms of the customer contract. Anything that applies to the processor should also apply to the subcontractor.

Assisting with Individuals' Rights: The controllers are required to ensure that the individuals' rights are respected. The processor has a requirement to help ensure that the controller can do so.

Limitations to Processing: As the controller is only allowed to use the PII for a specific purpose, the processor is only allowed to process the PII along those guidelines.

Benefits of ISO/IEC 27701

Since ISO/IEC 27701 is based on ISO/IEC 27001, a company must first fulfill the requirements of this standard. As mentioned before, ISO/IEC 27701 can be considered an extension to the ISO/IEC 27001 standard. Entities that

decide to conform to ISO/IEC 27701 will create documentary evidence related to their handling of PII throughout their business processes. This documentary evidence will further serve to make it easier for business partners to understand how the company handles PII processing.

As with other ISO standards, third-party accreditation offers stakeholders peace of mind. To acquire ISO/IEC 27701 certification, a business needs to conform to the requirements that apply to its data processing and handling. While this may not be every requirement listed on the standard, it does cover all the essential needs associated with how a business processes PII. A third party must certify that the company conforms to the requirements at a certain level of competency for accreditation.

ISO/IEC 27701 is also extremely rigorous in how it deals with privacy. Most jurisdictions are playing catch-up with privacy laws, and ISO/IEC 27701 offers a global standard that a company can refer to that may surpass any local legislation. Because of the complex nature of ISO/IEC 27701, businesses benefit from a standard that is in tune with the concerns of individuals about how their data is being collected and used. One of the more progressive local standards that the standard references is the GDPR from the European Union.

ISO/IEC 27701 and the GDPR

Immediately, when one looks at Article 42 of EU's General Data Protection Regulation (GDPR), the terminology stands out as familiar to ISO/IEC 27701. Terms such as controller and processor also exist here and carry the same meanings as in the standard. The standard (so far) lacks the formal backing of the GDPR, and without that, compliance with the standard will not necessarily mean compliance with the GDPR. Businesses within the EU will also need acknowledgment of their certification from at least one supervisory body.

For businesses with problems with allowing access to their PII for remote teams, this might be an excellent time to consider getting ISO/IEC 27701 certification. Additionally, companies that conform to the standard are more likely to get the nod from clients as caring about their customers' personal data. While there is not any official link between the GDPR and ISO/IEC 27701 as of yet, they both have the same goal in mind. Businesses may not want to leap into certification with both feet just yet since there is not any supervisory body that presently recognizes the standard. However, with such a close relationship with the GDPR, it may only be a matter of time before the EU starts recognizing and asking for this certification as a prerequisite for doing business.

Breach Management and Control

Organizations that comply with the ISO/IEC 27701 standard will have measures in place to deal with breaches. The standard is flexible enough to be used in any jurisdiction and allows for contacting the requisite personnel to report the violation. By following the standard, a company can have peace of mind that it is doing everything possible to ensure its data privacy. The ISO standard serves as a guarantee that the organization is ready and willing to act in case a breach does occur. As any security professional can attest, it is impossible to foresee when and where a violation will happen most times. An organization, therefore, simply needs to be ready to deal with the fallout and mitigate any potential damage that may result.

Another close similarity between the GDPR and ISO/IEC 27701 is breach management. ISO standard's incident management controls are almost the same as GDPR's. There is one glaring exception, however, and that is the notification window. The GDPR has a standardized 72-hour window for companies to report a data breach, while the ISO standard does not include this window. However, there are workarounds for this shortcoming of the standard. Organizations can still fulfill the GDPR requirement by having a system that allows them to notify a regulator independently of the standard. In this way, the standard retains its usefulness outside of the EU but still has a failsafe in place that a company can use if they operate within the extended European state's boundaries.

Acquiring ISO/IEC 27701 Certification

For organizations looking for a pathway towards certification, there are a few significant steps that the company must take:

1. Understand ISO/IEC 27001:2013
This standard deals with establishing an information security management system (ISMS) which will be the basis for getting ISO/IEC 27701 certification.

2. Establish a management framework
The management framework outlines the requirements an organization must meet to comply with ISO/IEC 27701. A company cannot seek ISO/IEC 27701 certification unless it already conforms to ISO/IEC 27001.

3. Perform a risk assessment
Where are the risks in your system? A risk assessment is a crucial step in figuring out where your data is most vulnerable. The organization must have a security baseline set up and then perform its risk audit in reference to that baseline.

4. Implement risk-management controls
Dealing with risk requires figuring out the best way to manage them. The organization should document its intention to address its risk and complete a Statement of Applicability report and a risk treatment plan. These reports are crucial as documentary evidence of risk assessment and mitigation.

5. Train employees
As mentioned before, employees are one of the weakest points of entry into a corporate system. Extensive employee training must be undertaken and documented.

6. Pinpoint the processes that apply to ISO/IEC 27701
As noted before, since ISO 27701 doesn't require businesses to conform to every aspect, companies need to pinpoint which procedures apply.

7. Ensure the processes conform
The organization must go through the guidelines outlined in the standard and deal with any issues they encounter.

8. Monitor and review
After a single cycle, the organization headed by the ISO/IEC 27701 champion should outline the information they collected and review it to see where the system can be improved.

9. Implement changes
The organization should be able to discuss and develop relevant changes to improve the organization's handling of PII, and those changes should be implemented in the relevant processes.

10. Seek external certification
Audits by a third-party are necessary for an organization to achieve final certification.

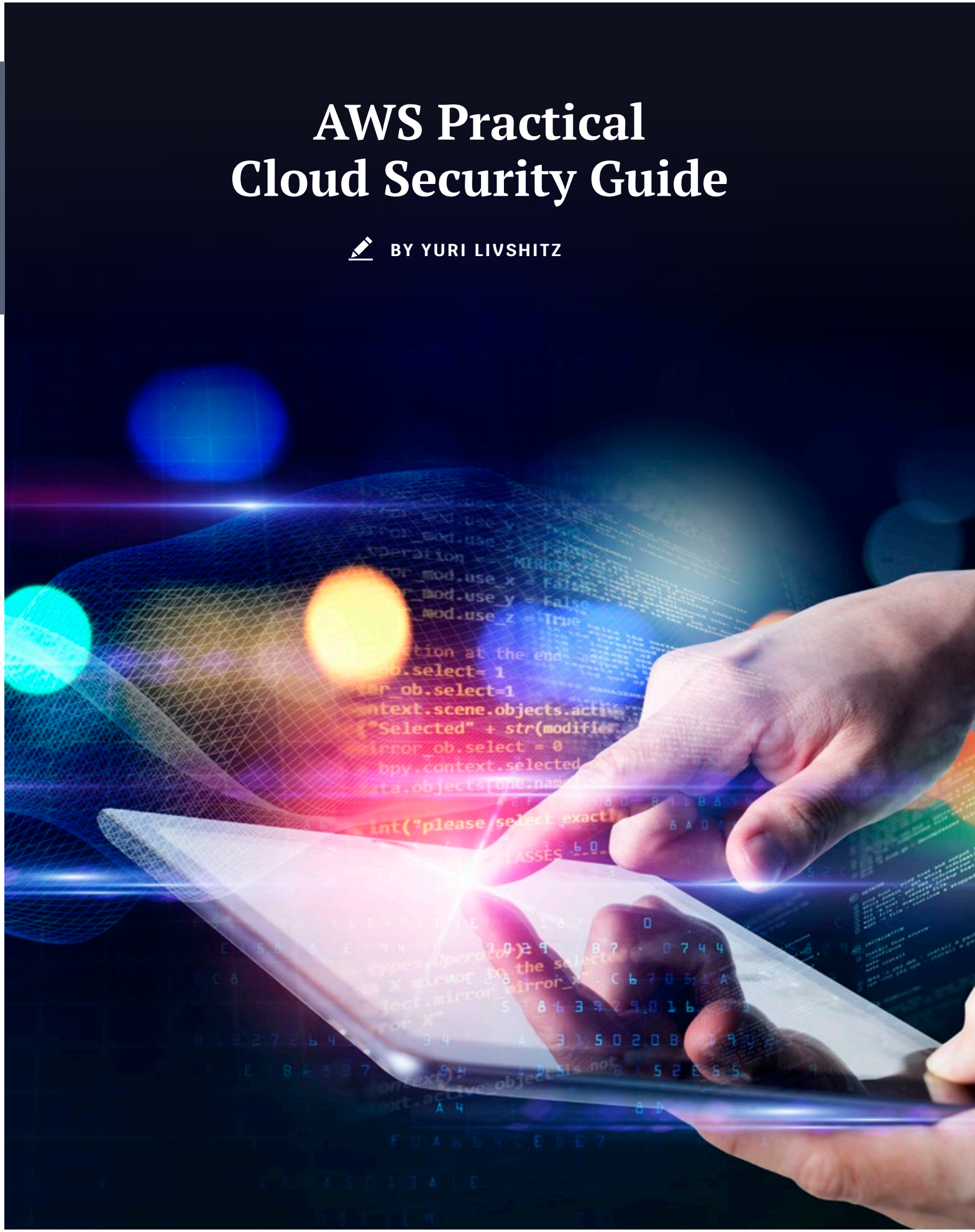
The ISO/IEC 27701 certification works on the principle of constant improvement. It is still a relatively new standard, and many businesses have not realized how important it can be as a selling point. However, with so many users concerned about what goes on with their PII, it may become even more vital to twenty-first-century businesses.

Al Mahdi Mifdal
Principal, Privacy and International Assurance at Coalfire

Al Mahdi Mifdal is an information security subject matter expert with over 12 years of senior information security compliance and consulting expertise for fortune 500 companies, cloud service providers, Silicon Valley start-ups, and international companies in the healthcare, technology, and critical infrastructure sectors. Al Mahdi has extensive experience managing a wide range of consulting projects (Risk Management, Critical Infrastructure Protection, Security Operations Center Design, etc.) and compliance assessments (PCI, SOC, ISO/IEC 27001, HIPAA, etc.). He currently serves as the Global ISO Assurance Practice Principal at Coalfire Systems and manages ISO assurance services and programs for clients worldwide. Al Mahdi has earned several industry-recognized certifications, including the Certified ISO/IEC 27001 Master, CISM, CISA, and PCI QSA.

AWS Practical Cloud Security Guide

BY YURI LIVSHITZ



My introduction article about cloud security best practices will focus on AWS cloud security. The core information in this article can be extended to other cloud technologies like GCP and Azure.

Amazon Web Services (AWS) is the most-used cloud infrastructure provider today. With multiple cloud-based services, large organizations rely on it every day to provide services to their employees and contractors, and applications to customers. Companies like Netflix and LinkedIn base their core service infrastructure on AWS.

Recently, numerous cloud-related attacks occurred in multiple large companies. The need to protect AWS cloud services is paramount. Company investment in AWS has to include a detailed security approach, so, it is essential to verify that all parts of AWS are proactively protected.

Security CIA Triad

A common way to explain cybersecurity needs and requirements is via the CIA triad. Different organizations can emphasize some parts of the triad as more important for their business needs. However, every company has to maintain key factors of the triad as described below.

Confidentiality

It is crucial in today's world for companies to protect the sensitive and personal information of their employees from unauthorized access.

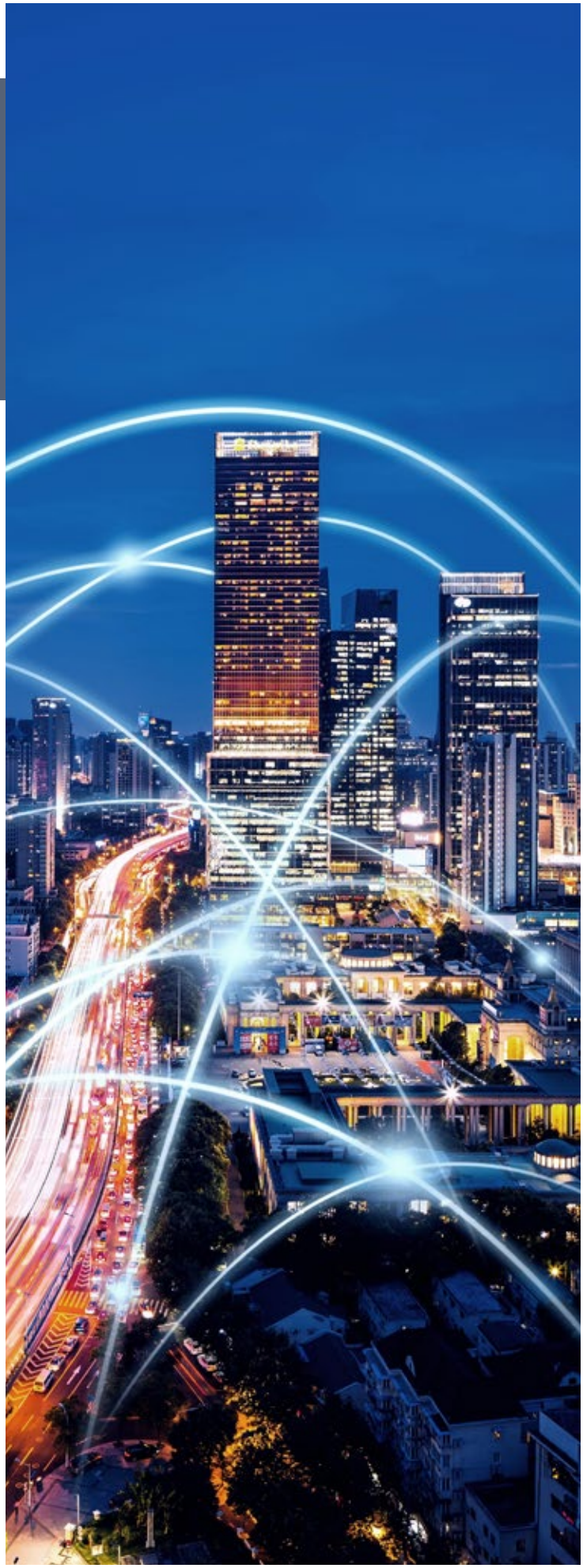
Information confidentiality is dependent on being able to set proper access levels to your data. Doing this requires segregating the information into data sets that are organized based on need-to-know access and sensitivity level that information actually has. You need to also examine the amount of damage if confidentiality is breached. Some of the ways to manage confidentiality include access control lists, volume, file encryption, and data classification.

Integrity

This component of the CIA triad is designed to protect data from alteration or destruction by unapproved parties, and it ensures that when an authorized person makes an unwanted change, the change can be reversed and damage prevented.

Availability

The last component of the CIA triad is related to the availability of the data. Authentication mechanisms and systems have to function accurately for the information they protect and ensure it is available when it is needed. Modern computing resources have architectures that are specifically designed to improve availability.



DDoS protection measures and systems specifically address availability-related challenges related to volumetric distributed attacks. My explanation of cloud security best practices will follow a reference to the CIA thread as a methodological framework for holistic cloud security.

Building AWS Cloud Security

Your AWS environment security requires risk prioritization and risk management based on your organization's use of the AWS services available and the detailed risk footprint these services create as a result. In order to create a security baseline, follow the list below:

Know your responsibilities

AWS uses a shared responsibility model where AWS is responsible for the availability of computing, storage, and more. You are responsible for your data, company applications, users identity, and – most importantly – overall environment security.

Know your risk

In the case of AWS, the risk is about exposure. Since most use cases of AWS are internet-facing, you need to understand your potential risk. Performing a risk scoring may be necessary to comprehend where you may be exposed and what security service may be necessary to protect your AWS investment. Remember, risk assessment is a pivotal first step in any security program.

Limit access via IAM

Start with a properly configured IAM strategy that utilizes defined roles to ensure that users only have access to the bare minimum resources they should. Use 2FA as much as possible, separate accounts, and never allow employees to use service accounts for manual admin tasks. Following these requirements will improve the integrity and confidentiality of your environment.

Think "defense in depth" security

Threats are evolving, requiring that your security strategy uses several tools and methods. Products that assist you with the protection, prevention, detection, and remediation of AWS security necessitate implementation across infrastructure, identity, storage, and endpoints.

Use external vendor solutions from AWS marketplace if needed. This can provide you with more granular security and better visibility. Solutions by multiple security vendors are available in the AWS marketplace. Fortinet, Pal Alto Networks and Checkpoint, and Splunk are just a fraction of hundreds of vendors available.

Focus Areas of AWS Security

Identity and access control

AWS environment access requires a combined approach. A central user identity store is used with the ability to manage user identities, along with single sign-on (SSO), multi-factor authentication, and detailed access to AWS resources.

Infrastructure

If your environment is exposed to the internet, you need network firewalls, web application firewalls, and encryption in transit. Use base-security services like EDR to protect your AWS environment as a whole.

Threat detection and remediation

A large array of threat intelligence exists today. Threat intelligence can be used as the basis to detect threats. Network-level intrusion detection and host-level detection are necessary parts of the strategy with AWS implementations.

Data classification

The need to understand where your sensitive data is stored is the first step for its defense. Mapping critical data is pivotal for a successful defense strategy. Data located in S3, EC2 instances, EBS, RDS, and more, all contain critical, protected,

sensitive, or otherwise valuable data. Data classification requires automatic discovery and classification data based on its content. This requirement relates to the confidentiality part of the triad.

Vulnerability management

It is your direct responsibility to perform assessments of and fixing vulnerabilities found on virtual resources within AWS that your company deployed. This requirement relates to the integrity part of the security triad.

Penetration testing

AWS tests its infrastructure in a rapid way. There are multiple core services (AWS EC2 and AWS RDS) against which customers can perform their own penetration tests without approval from AWS. Selected types of tests are prohibited by AWS or require a separate written approval process to pass with AWS. This requirement relates to the integrity part of the security triad.

AWS Native Security Services

AWS Firewall Manager and Amazon WAF are centralized configuration and management of rules used to block traffic and traffic patterns synonymous with malicious activity. AWS supports the encryption of data that is available across most AWS storage and database services. Consider utilizing AWS KMS – Key Management Services to supervise encryption keys and their use. This requirement relates to the integrity part of the security triad.

Data classification

Use Amazon Macie to identify sensitive data such as personally identifiable information, providing visibility into how this data is accessed. Maice is limited in scope to data residing in S3. This requirement relates to the confidentiality part of the security triad.

Monitoring and auditing

Two key services provide this requirement: Amazon CloudWatch collects data via logs, metrics, and events across multiple AWS services. AWS CloudTrail detects AWS account activity and API access.

AWS Inspector service can provide vulnerability management functionality by looking for vulnerabilities and providing automated security assessments on EC2 instances.

The technologies mentioned relate to the confidentiality part of the security triad.

Identity and access management

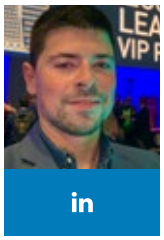
AWS offers multiple solutions designed to meet the needs of organizations that are in different levels of security maturity. Important services for IAM are AWS Identity and Access Management (IAM), AWS Multi-Factor Authentication, and AWS Directory Service. IAM AWS services provide highly secure and centralized access to AWS resources. IAM services can integrate with on-premises identity systems, such as Active Directory and OKTA style cloud-based identity management solutions to offer SSO access to multiple applications and infrastructure services outside of AWS.

Amazon GuardDuty can monitor AWS accounts and analyze network and account activity for anomalous behavior. GuardDuty uses rule sets and machine learning to alert on abnormal activity. GuardDuty identifies threats within AWS and can either address them with Amazon Lambda or route findings into third-party event management SIEM application. This requirement relates to both integrity and confidentiality parts of the security triad.

DDoS mitigation

Amazon Shield detects and responds to DDoS attacks to reduce the time to mitigate and reduce the scale of attacks. AWS customers can enjoy AWS Shield's Standard level service for free. For more sophisticated requirements, external CDN and DDOS services by Akamai, Imperva, or Cloudflare can be used. This requirement relates to the availability part of the security triad.

As a final word, remember that cybersecurity might be complex and costly, but in the long run, it pays off as it allows safer business operations. In addition, investment in security creates a competitive advantage for your organization.



Yuri Livshitz
CISO of Clarizen

Yuri Livshitz is the CISO of innovative SAAS company Clarizen. Yuri has more than ten years of cloud security experience, which he acquired while working for IATA and PayPal. Yuri has substantial cybersecurity experience with an emphasis on cloud security and Kubernetes security.

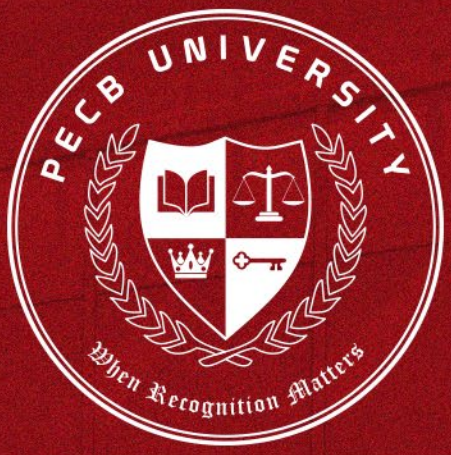
He originally studied cybersecurity at Technion and received CISO certification. Yuri is a certified CISSP, GCIH, and provides consultancy and forensic services to some of the largest VCs and international companies.

Transfer Your PECB ISO Certifications Towards a PECB University Degree!

All of PECB University study programs share the same modular structure; this allows students to easily transfer from one study program to another.

For more, the vast majority of PECB training courses are equivalent to those offered by PECB University. Therefore, the certifications obtained by PECB can be easily transferred to PECB University courses!

See the brochure to find out more, or contact PECB University directly at university.studentaffairs@pecb.com.

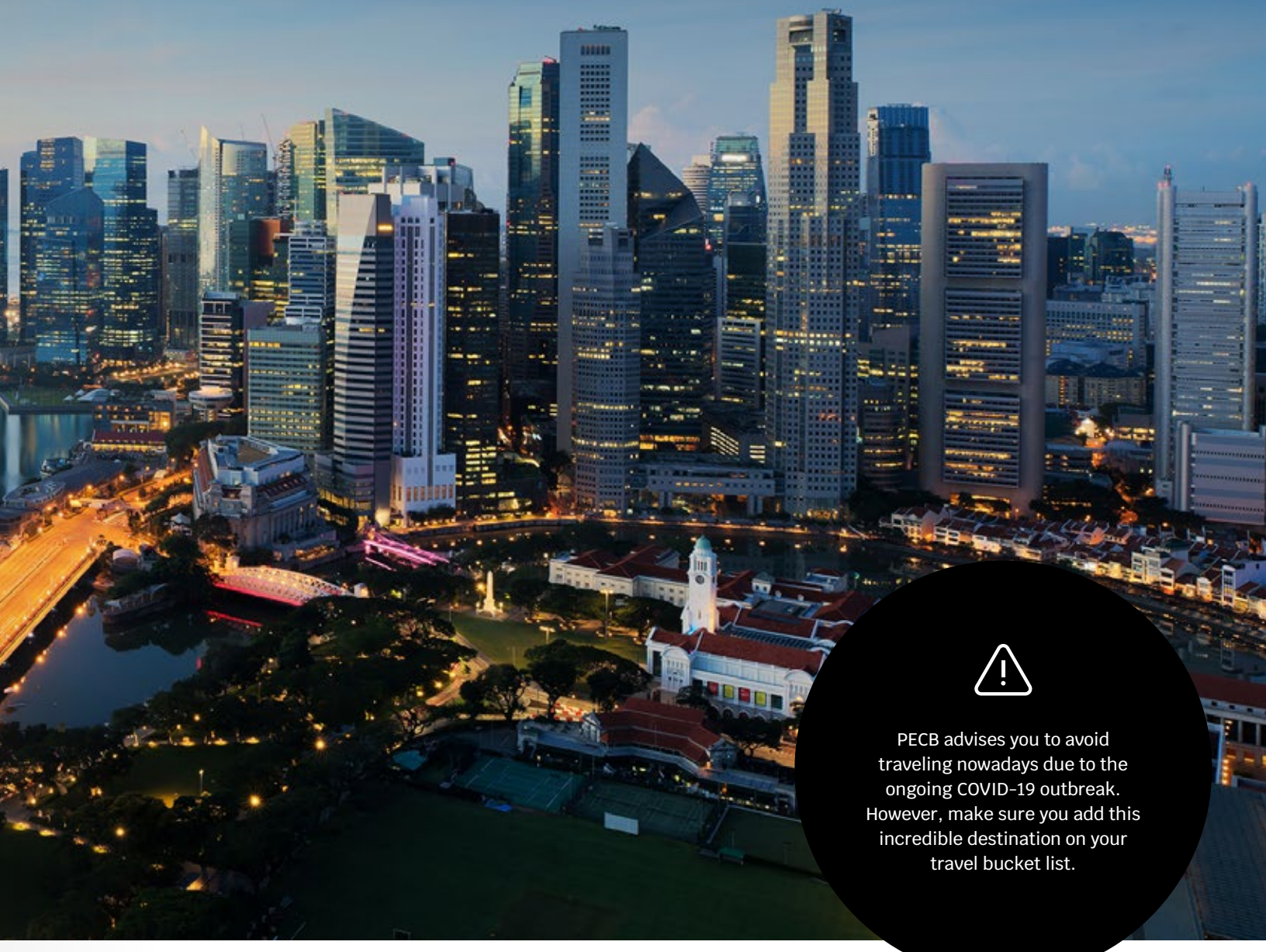

PECB UNIVERSITY
When Recognition Matters

SINGAPORE

THE LION CITY, AWAITS YOUR NEXT TRAVEL!

If you are traveling to the Lion City soon — congratulations, you have come to the right place!

Singapore is one of those cities that stays with me long after I bid my adieu. Apart from the obvious tourist attractions, I found out much more about Singapore through a local. It helped me to get a good perspective of the city and appreciate it in all its glory. So, before we talk about the itinerary, let me give you a brief idea about Singapore by answering the frequently asked questions about traveling to Singapore.



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.

ARTICLE BY THEROVINGHEART.COM / INSTAGRAM

Is Singapore a Planned City?

Singapore is one of the most well-planned and well-organized cities in the world. By definition, it is THE ideal city. Everywhere you go, the road is lined up with trees on both sides – it's easy to understand why Singapore is called the Garden city. A colossal S$10,000 is fined on anyone who accidentally or not, cuts down trees for personal or commercial purposes.

What's the Population of Singapore?

With just over 5.5 million population (2019) in around 720 square km area, barely crowded roads surprised me. In comparison, the city I was coming from, Bangalore, had a similar area, but over twice the population.

Unlike a lot of highly populated cities, it was possible to enjoy driving within city limits. I soon found out why.

Is Singapore Expensive to Live?

"The lesser number of cars on road attributes to the fact that buying a car is considered a luxury," my relative who lives in Singapore told me once. "A steep entitlement fee is paid to the government alone that costs as much as the car," he added.

No wonder Singapore is one of the most expensive places to live in! On the other hand, they have a very efficient public transport system, be it metro or buses, which makes it convenient for the locals. That's one of the reasons why Singapore isn't an expensive place to travel.

What Are the Official Languages in Singapore?

English, Chinese, Malay, and Tamil are the official languages of Singapore – rightly emphasizing a blend of different cultures there. Singapore relies heavily on overseas imports for everyday necessities – including diary since the land area is not adequate to practice agriculture.

What's the Ease of Doing Business in Singapore?

It is hassle-free to start a business in Singapore. From the time of conceptualizing the idea, it hardly takes a week's time to literally start working on your own business. Due to this, the city is ideal for startups.

Now that we have a brief idea of the garden city, let's start planning our itinerary. But before that, let's decide where can we make ourselves at home, shall we?

Is Singapore Safe to Visit?

Due to its stringent laws and regulations, Singapore is one of those cities where you don't have to worry about your safety. It's constantly rated as one of the top safe cities around the world.

I've even heard of multiple stories where tourists left their luggage in the cabs, and the cab drivers diligently returned it to the rightful owners.

If you are traveling solo, with friends, or family, rest assured that Singapore is as safe as it is clean.

Singapore 5-Day Itinerary

While Singapore is not blessed with natural landscapes, the advent of cutting-edge technologies has made it one of the top tourist destinations in the world. Marina Bay Sands is one of the most photographed buildings in the world.

I found myself in Singapore on a family trip in 2015. It was our first trip abroad, so it will always remain special. We made extensive plans and almost every hour was accounted for. You can use this as a template for your future trip to Singapore. It covers all the main attractions – iconic buildings, parks, museums, thrill rides, nightlife, and more! We stayed close to Little India, a hotel which is now shut down, but I have some hotel recommendations for you at the end of the article.

Most of the below attractions are popular ones, and there would be huge waiting lines at the counter. You get discounts when you book tickets online. So, I would suggest having confirmed tickets before visiting the below attractions at least for the popular ones.

Here's a gist of Singapore itinerary for 5 days. As an Indian family of 4, we spent around Rs. 45,000 (S$835) per person including the flight tickets.

Art Science Museum

Singapore National Museum

DAY 1

The best way to start exploring Singapore would be to get a perspective of the city and its origins. What a better way to do it than understanding the history and culture of Singapore. Take your time roaming the streets and align better with the city. We have a light itinerary for the first day, and intentionally so.

Art Science Museum

Visit the Art Science Museum for some spectacular sights. This museum is clearly one of the most instagrammable locations in Singapore. Short of a bucket list item!

Duration: A minimum of 2 hours

Singapore National Museum

If you'd like to know more about the history of Singapore, pay a visit to the National Museum of Singapore. It has some cool and contemporary art pieces too.

Duration: A minimum of 2 hours

If you have time to spare, you can head to Singapore zoo for a night safari or river safari, if you'd like. Book your tickets for Night Safari here.

DAY 2

On Day 2, let's head to the bird park, followed by a visit to the world-renown Gardens by the Bay. And then cross the road and walk over to Marina Bay Sands for the brilliant views from the 57th floor. It's quite a packed day today, so keep up!

Botanic Gardens

Gardens by the Bay

Jurong Bird Park

For ardent bird lovers, Jurong Bird Park is a must-visit in your Singapore itinerary. It is one of the largest free-flying aviaries in the world. Inside the campus, at Pool's Amphitheatre, based on weather conditions, the park hosts high flyers show every day at 11:00 a.m. and 3:00 p.m. This includes, and is not limited to, parrots, hornbills, macaws, yellow-naped Amazon, and flamingos as stars. It's a fun and interactive show. Make sure you catch it!

Duration: 2-4 hours

Book tickets for Jurong Bird Park here.

Singapore Botanic Gardens

Stop by at the massive and over 150-year-old garden. Apparently, Singapore Botanic Garden is the only tropical garden to be honored as a UNESCO World Heritage site. If you have time, you can visit the garden on Day 1 after a visit to the National Museum, or you can make time for it on Day 2.

Duration: A minimum of 2 hours

Gardens by the Bay

Visiting Gardens by the Bay, a park spanning 101 hectares, is nothing short of fantastic. It is an integral part of a strategy by the Singapore government to transform Singapore from a Garden City to a City in a Garden. It transcends you to a different dimension with the cloud forests and flower domes. These resplendent man-made trees offer a feast for the eyes. Additionally, the park has proven extremely popular among event planners. I happened to witness a very extravagant reception happening in one of the halls there.

Travel Tip: There are daily light and music Garden Rhapsody show at 7.45 p.m. and 8.45 p.m. at Supertree Grove. It's a brilliant show designed by an award-winning Lighting Designer, Adrian Tan. That promises to whisk you away to a mythical enchanted forest. And, best of all, it's free! So, it is ideal to visit Gardens by Bay during dusk. In addition, there are some seasonal shows that you can be privy to. Check out the official site for more details.

Duration: A minimum of 4 hours

Book tickets for Gardens by the Bay – Flower Dome and Cloud Forest now.

Marina Bay Sands Sky Park

At night, visit the iconic Marina Bay Sands. The viewing deck is located on the 57th floor. Consequently, it offers a scintillating and mind-blowing view of the Singapore skyline. From Singapore flyer or Gardens by the Bay or Fullerton hotel, to whole the commercial district of Singapore, it shows the major skyline of Singapore. So, definitely include it in your Singapore itinerary. Ideally, visit during the night for the best views.

Duration: 2 hours

Book tickets to Marina Bay Sands now.

DAY 3

Let's spend Day 3 on Sentosa Island – Asia's leading resort destination, and a premier resort island getaway. Afterward, let's try a thrilling adventure!

A Day at Sentosa Island

Sentosa Island has a casino with free entry for foreigners, while it costs S$100 for Singaporeans. If you aren't planning to play, you can visit it if you'd like. Highlights at Sentosa Island include, and not limited to, Underwater World and Dolphin Lagoon, Sentosa SEA Aquarium, Adventure Cove Water Park, and Wings of time. It will easily take up a day, even without Universal Studios which is part of Sentosa Island.

Duration: 6-8 hours

Book tickets to SEA Aquarium now.

Sentosa Island

Marina Bay Sands Sky Park

Clarke Quay

Clarke Quay (pronounced as Clark Qi) is famous for its nightlife. With splashy lights and karaoke nights by the riverside with people gaily relishing themselves, it was easy to fathom why this is a favorite spot for tourists and natives alike.

Travel tip: If you'd like to party with a vibrant crowd, then visit Clarke Quay during the weekends!

Additionally, if you are up for high adrenaline-pumping experience, check out Gmax extreme reverse bungee in Clark Quay. It opens at 11 a.m. and is usually open until pretty late in the night! Here are the prices:

GX-5 Extreme Swing: S$45/person

Student Rate: S$35/person

Trampoline Bungy: S$10/person for 5 mins

Duration: 3 hours

Would you dare?

DAY 4

Let's spend most of Day 4 at one of the most awaited activities in Singapore – Universal Studios. It can be followed by a visit to Merlion Park and then some late night shopping if you wish!

Universal Studios


Merlion Park

A Day at Universal Studios

Universal Studios is one of my favorite spots in Singapore. It's located within the Sentosa Island. Yet, reserve a day exclusively for Universal Studios in your Singapore itinerary. Ranging from Transformer's ride, Revenge of the Mummy, Dinosaur's ride, and shows like Steven Spielberg movie production and Water world show, Universal Studios is so much fun for kids and adults alike.

If you are looking for an adrenaline pumping adventure, don't miss out on the Battlestar Galactica which is high on adrenaline.

Here's a video of Battlestar Galactica, if you dare!

Duration: 8 hours

Book tickets now to Universal Studios to avoid long queues.

Travel Tip: On weekends or holidays, opt for Express Pass for easy and unlimited access to Universal Studios. It can be bought as a supplement to the normal passes at the merchandise stores inside the park or at the booths just outside the entrance gates. The starting price of the Express Pass is around S$50 as a supplement to a single day ticket or S$130 added to the seasonal ticket.

Merlion Park

Anyone who hasn't been to Singapore would still identify the city with the Merlion statue. Merlion statue is a mythical creature with a head of a lion and body of a fish, and the unofficial mascot of Singapore. After all, it's seen everywhere from sports teams to tourism as a national icon. Apart from being a popular spot among tourists, it also offers a photo opportunity to capture the majestic Marina Bay Sands. Best to visit during dusk. Moreover, it's free!

Duration: 1 hour

Little India

Mustafa Center is a well-known shopping district located in Little India, which offers everything under one roof – be it groceries, electronics, apparel, footwear, or jewelry. Most of all, it is popular for offering cheap electronic goods. As Mustafa Center is a 24-hour shopping complex, it can be easily squeezed in during the night. You can accommodate it in any of the nights in the itinerary. Walking along this street, you realize that you are right back in India – with bustling streets, Bollywood music, and tons of Indian restaurants.

Duration: A minimum of 2 hours

DAY 5

Let's dedicate a day in Singapore to roam around the city and do some retail therapy!

City Tour around Singapore

Drive along the Orchard Street, Anson Road, Robinson Road, Raffles Place. Orchard Street is a well-known shopping destination famous for luxury brands. In addition, try out the ice cream sandwich in Orchard Street.

China Town

If you are looking for budget-friendly souvenirs, look no further than China town. This is a perfect shopping place for tourists. If you have time, sample authentic Chinese cuisine in of the eateries in and around China town. You can also pay a visit to the Buddha Tooth relic temple – a Buddhist temple and museum complex in China town.

Additionally, there are many other things to do in Singapore, if you have time to spare!

Accommodations in Singapore

Here are a few recommendations of stay by The Roving Heart

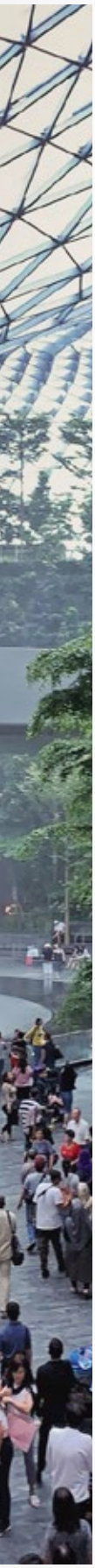
The Claremont Hotel – Located close to Mustafa Center, and close to the city center, it's convenient to base yourself out of here to visit Singapore's main attractions. Ideal for a budget stay! Book your stay at The Claremont Hotel here.

Ascott Raffles Place – On the other hand, if you'd like to splurge, then make yourself at home at Ascott Raffles Place. It is one of the top-rated hotels in Singapore and is right at Orchard Street. It features colonial-style buildings and screams luxury! Book your stay at Ascott Raffles Place now.

Fullerton Bay Hotel – If you'd like to have a view of Marina Bay Sands to wake up with, then it can't get any better than Fullerton Bay Hotel. It's right at Merlion Park, so you can spend a good time there, day or night! Book your stay at Fullerton Bay Hotel now.

Marina Bay Sands – Of course! How can I not mention Marina Bay Sands while listing out places to stay in Singapore? It's an iconic building that represents Singapore internationally. The stay is quite pricey but it comes with a 57th-floor infinity pool that offers unparalleled views of the city skyline. Book your stay at Marina Bay Sands now.

Singapore Changi Airport



Singapore Changi Airport

So, why did I include a special mention to Changi Airport in the Singapore itinerary, you ask? Well, Changi Airport is no ordinary airport. It is a microcosm of Singapore and is worthy of being a destination itself. It is rated as one of the World's Best Airports many times, and for good reason. Apart from the usual dining and shopping experiences, Changi airport has an entertainment deck, cinemas, Singapore's tallest slide, Sunflower, Orchid, and Cactus Gardens, and so on. So, depending on your arrival or departure dates, make some time to spend at the airport as well!

Find more things to do at Changi Airport here.

If you have a layover of over 5.5 hours in Singapore, you are eligible for a free Singapore tour as well. So, if you are passing by Singapore, and have enough time, then make sure to avail this cool perk! Transit passengers traveling with Singapore Airlines can request for a free S$40 voucher at iShopChangi. This promotion has been running for years and it helps in buying, at the least souvenirs. Find more information about it here.

Additionally, find out some more attractions for doing Singapore on a budget here.

Helpful Information about Singapore

Visa on arrival is not available for Indians. However, they offer an online tourist visa. The application process for the visa is hassle-free and usually takes a maximum of 5 days to process. Another option is to have either relatives or friends in Singapore with a PR or citizenship fill in the letter of introduction for a visa application. Find out more about applying for a Singapore visa here.

Transport in Singapore ranges between taxis, metro, and buses. Taxis are easily available and the price is fixed. If you are a group of four or above, then it works out cheaper with a taxi. Else, stick to the metro. It is convenient and well connected. Additionally, there are hop-on hop-off buses for a day or two for tourists which covers a lot of places. If you are not sure of the itinerary, you can try it out!

Transact using Singapore dollars(S$) in Singapore. S$100-200 per person per day on an average including stay and a moderate number of activities on a budget.

Singapore is hot and humid mostly throughout the year. July – September is usually the ideal time to visit. The Great Singapore Sale and food festival happen during that time too. February – April is also a good time as the weather is pleasant at this year of the year and yet, not as expensive as the tourist months.

PECB GDPR Implementation Toolkit

Your Guide to GDPR Compliance

The PECB GDPR Implementation Toolkit provides some of the most efficient methods that define roles and responsibilities as well as instructions on meeting the requirements of this data privacy regime.

BUY IT ONLINE

PECB Store

ON-DEMAND WEBINAR!

Interested to know what are the key differences and similarities between CPRA, GDPR, Virginia CDPA, and NY Shield Act?

Register for the next PECB webinar and learn everything you need to know about these data privacy regulations and how they differ from each other.

CPRA, GDPR, Virginia CDPA, and NY Shield Act: Essential Things You Need to Know

March 24 / 3:00 p.m. CET

Presenter:

Odia Kagan

Partner, Chair of GDPR Compliance and International Privacy at Fox Rothschild LLP

→ GET YOUR SPOT NOW!

PECB WEBINARS

LEARN AT EASE

Connecting you to the best education through recognized PECB training courses!

Check our most recently updated training courses!

Status	Training Course	Language	
Updated	ISO/IEC 20000 Lead Implementer	English	→ VIEW
Updated	EBIOS Risk Manager	French	→ VIEW
Updated	GDPR – Certified Data Protection Officer (CDPO)	French	→ VIEW
Updated	ISO/IEC 27001 Lead Implementer	Spanish	→ VIEW
Updated	ISO 31000 Risk Manager	Spanish	→ VIEW
Updated	ISO 22301 Lead Auditor	Spanish	→ VIEW

EASING THE ROAD TO SUCCESS!

Training Course Catalog 2021

We continuously strive to translate our efforts and commitment to provide excellence in keeping our training courses updated with the latest trends, standards, best practices, and approaches.

Explore and choose the training courses that you need to boost your skills, improve performance, and gain certification.

SPECIAL TI

TITANIUM

PLATINUM

GOLD PA


Note that PECB Partners are listed as per the credits a

HANKS TO

PARTNERS

PARTNERS

ARTNERS

acquired from January 1, 2020 to December 31, 2020.

In Memory of Andranik Markosyan and Penny Riordan

PECB has always had excellent partners who have continuously contributed to the success of our company. Today we remember two valuable trainers and auditors of our network that we lost recently — Andranik Markosyan and Penny Riordan.

They have shown what working with passion, commitment, and professionalism looks like. This is a great loss to us all, and they will be dearly missed but not forgotten as their legacy will be alive in PECB.

Andranik Markosyan

1969 - 2020

IT Security Expert, PECB Certified Trainer and Auditor

Penny Riordan

1960 - 2021

Independent Trainer and Consultant, PECB Certified Trainer and Auditor

BUILD
YOUR CAREER
WITH US!

As technologies shift, so does the threat landscape.
We remain steadfast in our commitment to
keep you safe and support your career journey
through our cybersecurity training courses.

GET INFORMATION. GET ANSWERS. START HERE.

PECB