PECB Insights

ISSUE 36 ISO STANDARDS AND BEYOND JANUARY-FEBRUARY 2022

CMMC, IT SECURITY, AND CYBERSECURITY

WHAT TO EXPECT

PECB Insights Magazine

delivered to your mailbox

Subscribe & find out more at

www.insights.pecb.com

In This Issue

"Data is the pollution problem of the information age, and protecting privacy is the environmental challenge."

BRUCE SCHNEIER
Internationally Renowned Security Technologist, Privacy Specialist, and Author

The Cybersecurity Skills Gap

Why education is our best weapon against cybercrime.

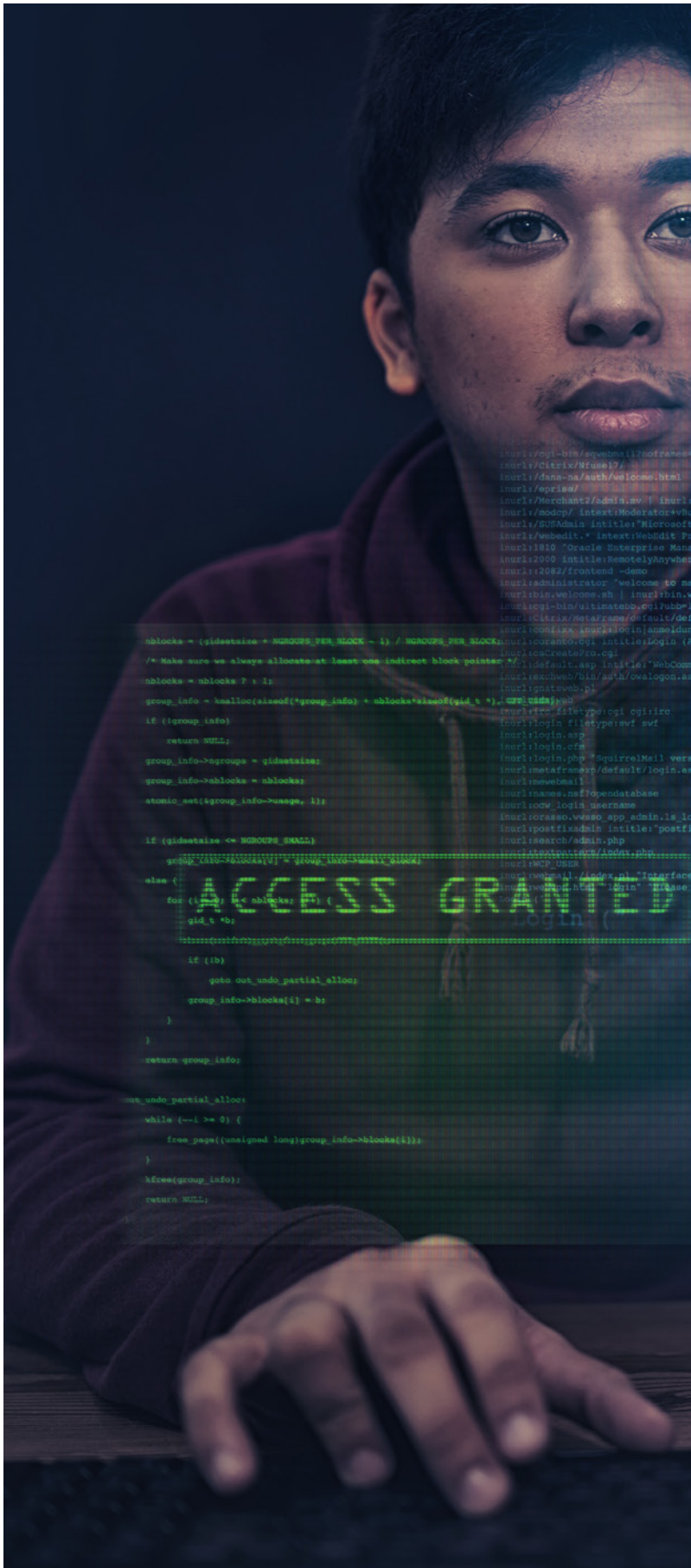
The Internet has been one of the biggest winners in the past year's pandemic, with traffic and transactions reaching unprecedented levels in 2020. Unsurprisingly, the number of malicious attacks and activity has risen with it. According to INTERPOL Secretary-General Jürgen Stock, "cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19".

Coming at a time when estimates state that up to 3.5 million cybersecurity jobs will go unfilled this year, this is bad news. Are we losing the battle? Upskilling those already in the cybersecurity industry and enticing newcomers to join is our best defence, but programmes and schemes are piecemeal, and not enough.

We sat down with world-renowned IT security specialist Dr Edward Humphreys to discuss concerns about the cyber-skills shortage and its potential implications for business and society. Dr Humphreys sits on a number of committees run jointly by ISO and the International Electrotechnical Commission (IEC), including ISO/IEC JTC 1, Information technology, subcommittee SC 27, Information security, cybersecurity and privacy protection, which has over 200 published standards and a further 77 in development. An expert in his field, he is often quoted as the "father" of the ISO/IEC 27001 family of standards for information security management systems.

Q&A with DR EDWARD HUMPHREYS

Convener of working group ISO/IEC JTC 1/SC 27 WG 1, Information security management systems



ISO: Cybersecurity is a constant battle, with demand for cyber talent continuing to rise and outpace supply. Where does the situation stand today?

Dr Edward Humphreys: It is useful to quote some ancient wisdom on battle strategy. This quote is often used today in various educational and training settings for professionals in many fields, including management, business negotiations, and of course, cybersecurity.

“If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.” – Sun Tzu, The Art of War

The more information we have about our strengths and weaknesses, and those of our enemy, the better prepared we are. We need to gain information about who the enemy is, why, when, how and what they might attack and what they want to gain from it. If we know ourselves and our enemy well, we have a high chance of winning the battle.

Having a cyber-aware workforce with skilled professionals and well-informed employees puts us in a good position. This means investing time and money in cybersecurity education, training, and awareness. Organizations with a winning strategy for cybersecurity are those with an effective risk management process and a skilled cybersecurity workforce. Taken together, these two elements enable an organization to assess its strengths and weaknesses to better withstand attack.

ISO: There is a drastic worldwide shortage of skilled experts in this area. Why is this?

Dr Edward Humphreys: Technology keeps changing, so it is hard for industry personnel to keep up, and often it requires specialized knowledge that takes time to develop.

According to the European Union Agency for Cybersecurity (ENISA), manufacturers and other organizations using Industry 4.0 and Internet of Things solutions often do not have time to train staff adequately before things change again, leaving themselves exposed to potential risks. What’s more, the training that is available is inadequate and/or expensive.

Over recent years, the escalation of cyber-attacks has seen organizations urgently rush to recruit skilled professionals, leaving the market depleted of available talent. The need and urgency to take action has been made worse by the COVID-19 situation and the wake-up call resulting from the dramatic rise in successful attacks.

The education and training of cybersecurity talent have not kept pace with the race to build a skilled workforce.

The reasons for this shortage are many and various. At the formal educational level (university, college), the take-up to do cybersecurity as a qualification has been steadily growing over the past decade or so, but the numbers graduating still fall way short of industry demand. It takes time to educate and train highly skilled professionals, and time to gain practical working experience. Meanwhile, investment in cybersecurity training has been severely hampered as budgets for items of expenditure not directly related to profits and revenue earning have been cut or reduced.

ISO: What does this mean for our future if nothing more is done?

Dr Edward Humphreys: The worldwide shortage of skilled cyber personnel has a direct and significant impact on organizations and their ability to protect themselves. And this collectively adds up to an appreciable threat to a nation's overall economic well-being, and by extension, that of society.

The problem covers at least three areas of concern:

- Skilled professionals to manage, administer and support organizational security and operations
- Skilled cyber-engineers to design security systems and develop secure software and tools
- General cybersecurity awareness at every organizational level so that everyone has a baseline knowledge of the threats and risks, and what this means in the context of each and every individual's job function

The growth in the use of the Internet and online services, the introduction of new technologies and the rapidly changing digital landscape compounds the need for better cybersecurity. The desperate shortage of cyber-skilled professionals will clearly hold back progress in achieving adequate and effective protection.

If the global shortage of a skilled cybersecurity workforce continues, organizations will find it more difficult to be on the winning side of the battle. The future outlook will be one of increasing exposure to cyber-attacks resulting in heavier financial losses, greater disruption to operations, interruption of services and supply chains, compromising of personal privacy and safety, and many other impacts.

ISO: What initiatives are underway to try and encourage cyber talent to fill the widening skills gap?

Dr Edward Humphreys: ENISA advocates cross-functional knowledge on IT and OT security and to further the training and education offering.

It has placed capacity building as a key objective in its new strategy and is doing lots of awareness-raising activities with consumers to promote safer online behavior.

It is also promoting and analyzing cybersecurity education in order to tackle the cybersecurity professional shortfall, which represents an issue for both economic development and national security.

There are a number of cybersecurity career awareness campaigns in countries such as the US and the UK, but the promotion of these campaigns is fragmented and there is nothing that is internationally harmonized.

Some countries have established programmes to consider the problem. These include national awareness campaigns encouraging universities, colleges, schools and training organizations to promote the take-up of cybersecurity as a field of study. In Canada and the UK, for example, cyber education is starting to be introduced in schools for children as young as eight years old. This is reassuring as we need to build future generations of cyber-skilled talent.

ISO: You are currently working on a new standard to address education in the cybersecurity industry. How is it intended to help?

Dr Edward Humphreys: One of our working groups has begun developing a technical report for cybersecurity education and training. When it is published, it will outline the why, what and how of cyber education and training to help improve the current situation. This new technical report will provide insight into why cybersecurity education and training are important and how they are essential to building a well-informed and competent workforce that can protect business and society. It also brings home why cybersecurity education needs to be made a strategic priority in workforce development within organizations and government, across all business sectors.

The guidance will list what is available with regard to national programmes and initiatives, formal education, professional training, standards and guidelines. Thus, it can be used to identify areas for improvement and further development. It will also go into specialist areas of cybersecurity education that are critical to ensure effective cyber protection.

ISO: Who is this document aimed at and when can we hope to use it?

The document is intended to be useful to anyone involved in cybersecurity: users, suppliers, certifiers, policy makers and regulators, educationalists, consumers, vendors and manufacturers. We expect to see it published at the end of 2021 or early 2022.

ISO: What can organizations do in the meantime to protect themselves?

One of the key actions that organizations must take is to fully understand the risks they face, and to apply a baseline of controls to try and mitigate these risks. ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls, provides a set of controls that are derived from industry best practice; this fulfils organizations' need to build winning capability by understanding themselves better, as I mentioned at the beginning. The more they understand about the attacks they could face and what their weaknesses are, the better they can reduce them. The wisdom of Sun Tzu in The Art of War is just as applicable today as when it was first written.

CMMC, ISO/IEC 27001, and ISO/IEC 27032 Differences and Similarities

BY CARL CARPENTER

In order to be able to discuss the similarities and differences between the three frameworks, we need to understand the background of each one. There certainly are some similarities between all three but also wide areas of vast differences.

Firstly, we need to understand that ISO/IEC 27032 is really about implementing security rather than a security framework that must be adhered to ISO/IEC 27001 or CMMC. Thus, ISO/IEC 27032 is about being a cybersecurity manager that manages one or more cybersecurity frameworks such as ISO/IEC 27001, CMMC, or possibly both simultaneously. It goes into more of the administrative controls, such as creating policies that adhere to the security framework.

Generally, it could be viewed, that a certified ISO/IEC 27032 Lead Implementer would bring a company up to speed with a framework of some sort, and then an ISO/IEC 27032 Lead Manager would keep that framework alive and not allow security to start sliding backward. So, for example, ISO/IEC 27032 would indicate that the Confidentiality, Integrity, and Availability (CIA) triad must be followed but not mandate exactly how to follow it. That would be the job of a framework such as ISO/IEC 27001 or CMMC.

It is widely known that ISO/IEC 27032 and ISO/IEC 27001 are from the ISO family, while conversely CMMC is from the NIST family. The longer you work with the two families the more you realize they are cousins to each other with one (ISO/IEC 27001) being more internationally based and the other (CMMC) being more focused around the United States.

Foundational Material

As it relates to foundational material, it absolutely must be pointed out that ISO/IEC 27001 is a tried, proven, and seasoned framework with almost two decades of successful implementation. CMMC is in its infancy, relatively speaking, but rapidly making an impact in numerous areas.

As everyone is aware, ISO/IEC 27001 covers numerous areas of security and is designed to be fairly universal regardless of what line of business the company is in. However, CMMC is not designed as such and it does specifically target companies that support the US Department of Defense (DoD). Once we understand this, the differences between the two frameworks start becoming more apparent.

For example, ISO/IEC 27001 is a one-shot framework in which you either are compliant or not. CMMC is a framework that has maturity built into it. In other words, you may be CMMC Maturity Level 1 (ML1) compliant but not CMMC Maturity Level 3 (ML3) compliant. That is not to say that you cannot mature ISO/IEC 27001 but it takes a good ISO/IEC 27032 Lead Manager to understand the vision and need to do so.

To continue on this area of difference, any maturity target in relation to ISO/IEC 27001 is really up to the ISO/IEC 27032 Lead Manager whereas the maturity for CMMC is clearly defined.

Another area of difference is that there are no legal requirements to implement ISO/IEC 27001, so when it is implemented, it is to indicate to others that a company is secure while following an established standard. However, CMMC does have legal requirements attached to it, so essentially it boils down to the following: if you want to do business with the DoD then you will be CMMC compliant, and if you are not compliant while doing business with the DoD then you could be facing numerous federal sanctions.

As it relates to the fundamentals of the frameworks, there are numerous overlaps. Both require separation of duties, complex passwords, network segmentation, minimization, etc., all the basics that are in any framework from ISO/IEC 27001, HIPAA, PCI, FFIEC, and so on. However, in my experience, CMMC takes the concept of a security framework to the next level.

An area of CMMC that is not present within ISO/IEC 27001 is that CMMC is really a combination of NIST 800-171/FAR 52.204-21 and has multiple levels of data classification. While ISO/IEC 27001 may require data classification in a holistic sense there are no actually defined classification labels (that is up to the ISO/IEC 27032 Lead Implementer/ Manager to figure out) nor are there different levels of security based on the classification level. On the other hand, CMMC requires at least ML1 to handle or process Federal Contract Information (FCI) and ML 3 to handle Controlled Unclassified Information (CUI). It is important to point out that CUI is, essentially, directly below the classification level of SECRET according to the US Government, with an example of SECRET data being what was released to WikiLeaks by Chelsea Manning.

Evolution

Of course, ISO/IEC 27001 has evolved over time and will continue to do so. As the threat evolves, technology grows or improves as well. CMMC is no different when it comes to this. However, where ISO/IEC 27001 seems to take the lead is a much more methodical pace involving industry leaders and mentors across the globe to provide useful input to maturity. CMMC, on the other hand, does not seem to have that same methodical pace of maturity.

To begin with, CMMC started with version 1.0 (CMMCv1) with 5 maturity levels, with Maturity Level 2 and 4 designed to be transitionary before landing at either ML3 or 5. However, in November of 2021, CMMC matured to version 2.0 (CMMCv2) which had significant changes and still appears to have a high probability of further changes.

One obvious change was that v1 went from 5 maturity levels to 3 in v2. In a way, this makes sense, however, this also removes the ability for a company to demonstrate forward momentum on maturity until that company has already achieved it. An example of this evolution is demonstrated in the graphic.

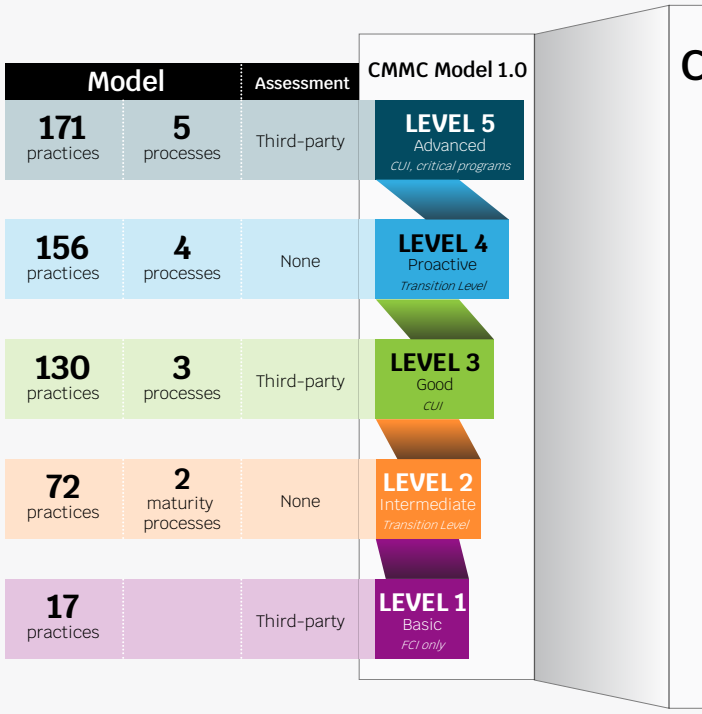
Another area of change for CMMC was that an auditor was required to be onsite for v1 ML1 in comparison to a company self-attesting to ML1 in v2. A similarity with ISO/IEC 27001 is that there is no requirement for an auditor to be onsite for any part of the actual audit as everything could be done via zoom. However, for CMMC v2 ML2, an auditor must be on location to personally witness the company perform evidence tasks.

Another area of difference is that an ISO audit could be viewed as easier to deal with than a CMMC audit from the standpoint of the company getting audited.

An ISO audit generally requires one item of evidence to meet an audit area with possible expansion for sampling. Conversely, CMMC auditors are obligated to get at least two items of evidence for each audit area with one of those items being a one-on-one interview with a key person, who performs that task, to demonstrate or verbally explain in sufficient detail that the particular practice is well established within the company.

The CMMC auditor must ensure that the person performing the relevant task is doing so at an expert level. Granted, that is in addition to actual evidence that still must be collected. So, for example, an ISO/IEC 27001 auditor may ask for proof of data backup being performed, as well as follow-on proof of data restoration, with log files possibly being sufficient. A CMMC auditor will ask for the same and then require the administrator to demonstrate both processes just to see if the administrator acts confused through the process.

One similar area is the indirect management of CMMC. By simply being CMMC compliant and wanting to maintain that compliance, or by maturing into a higher level of compliance, meeting all the CMMC requirements would naturally align with the functions that an ISO/IEC 27032 Lead Manager would perform.

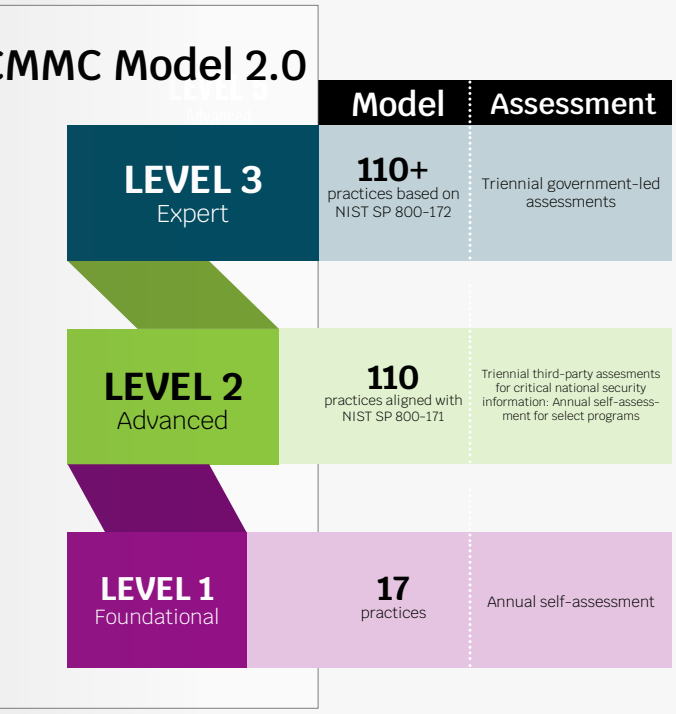


Pitfalls

There are some pitfalls that you need to be aware of as well, most relating to CMMC. Generally, once a company gets an ISO/IEC 27001 certificate, they are set for three years before needing a new audit. CMMC is the same, however, a company that holds any CMMC maturity level can be audited by the DoD or a Prime Contractor at any time to ensure continual compliance. This is to ensure companies do not do the work to become compliant but then slide backward after being awarded. Companies are specifically warned that spontaneous follow-on audits could happen at any time.

Where this comes becomes effective is when CMMC is attached to a federal law called the False Claims Act which has significant penalties attached to it. ISO/IEC 27001 does not have any sanctions attached to it, as becoming compliant is still essentially a voluntary action by a company. As an example of severity, in 2020 alone, the US Department of Justice recovered over $2.2 billion due to false claims by providing generous rewards for whistleblowers.

The CMMC audit process is also more complex when compared to ISO/IEC 27001, with multiple review stages required before being awarded a CMMC Maturity Level, during which, if at any review stage a reviewer does not think there is enough evidence, then the audit is denied until the issue is rectified.



Of course, this does not apply to v2 ML1 given it just requires an attestation and no actual auditor present.

Closing

In a general sense, ISO/IEC 27001 is a foundational framework for any company to implement with a consistent evolution based on solid input by seasoned professionals worldwide. However, CMMC is rapidly gaining traction in the Defense Space within the USA and will likely continue to evolve past v2 at some point based on the needs of the DoD.

Moving into a CMMC framework can be challenging however starting with an ISO/IEC 27001 framework before moving to CMMC can make that process much easier.

Lastly, having a solid ISO/IEC 27032 Lead Manager to blend CMMC into an existing ISO/IEC 27001 framework can easily reduce cost and headache if any company believes CMMC is in that company's future.

PECB is approved as a Licensed Partner Publisher (LPP) from the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) for the Cybersecurity Maturity Model Certification standard (CMMC). For further details, please click here.

Carl Carpenter
Consultant at Arrakis Consulting

Carl is a former CISO of a $6billion entity where he was responsible for protecting data of all types and regulatory environments such as FFIEC, HIPAA, and PCI as well as working with the FBI, IRS, and US Department of Labor around investigations relating to money laundering. He has performed assessments against Fortune 10 and 50 companies in the areas of GDPR, CCPA, ISO/IEC 27001, and as a CMMC-AB Registered Practitioner (RP). Carl currently performs CMMC assessments, as well as, CMMC pre-audit support to help ensure a successful CMMC audit. Carl is also a PECB trainer in ISO/IEC 27001, ISO/IEC 27032, and CMMC Foundations and hold numerous other certifications.

Cybersecurity Legislations: How to be a Cyber Savvy Leader

BY ANTHONY ENGLISH

As a veteran security practitioner, I can attest that the cybersecurity and information security landscape has evolved dramatically in the last 30+ years. At the beginning of my career in IT, the ability to recover data from a hard disk drive was just starting to become possible, and the first computer viruses were problematic at times but they were often more annoyances than anything else.

The cybersecurity landscape has changed over time, but like all technology-based bodies of knowledge, it is now in a state of constant evolution with bad actors evolving techniques and tools, conversely, cyber defenses are adapting to address new threats. Part of this cyber evolution includes cybersecurity legislations meant to help protect against the various types of cyber threats out there.

According to the United Nations Conference on Trade and Development (UNCTAD), 80% of countries worldwide have what the UNCTAD refers to as "cybercrime legislation" with an additional 5% of countries with draft legislation. Now, this count by the UNCTAD is quite comprehensive by including e-commerce type legislations, consumer protection, privacy and data protection, and cybercrime but obviously all these legislations are relevant to a cybersecurity practitioner. Business leadership needs to at least be aware of how these various cybersecurity legislations might impact the organization. Based on the UNCTAD count, there are more than a few hundred cybersecurity legislations across the globe, and furthermore, many of us in cybersecurity must be aware of and maintain compliance with some regulated standards and frameworks (e.g., ISO/IEC 27001, NIST, SOC, PCI-DSS, etc.).

How can you keep up with all this information?

There are a few tips to help any security or privacy practitioner wade through the sea of compliance requirements out there. Firstly, a quick definition of legislated versus regulated compliance, as I see it:

legislations are similar to laws, by being requirements that are defined and approved by governments for application to their citizens or within their borders, whilst regulations are requirements that are typically defined by an industry or practice body.

An example of a cybersecurity legislation would be something like GDPR or the Singapore Cybersecurity Act (CSA). Examples of regulatory types of compliance might be the increasingly common requirement in lottery and gaming for certification against ISO/IEC 27001 or the requirement by the PCI Council for entities that process payment card transactions to be compliant with PCI-DSS.

Despite there being some semantics involved here between cybersecurity legislations and cybersecurity regulations, I believe that most cybersecurity professionals do not have time to make the distinction when they are considering what is applicable to their organization.

When I worked as a CISO or a vCISO, during the early days in my role, my goal was to always get a list of applicable cybersecurity legislation put together (including regulatory compliance requirements) for the organization. Once I understood what was applicable, I could then start to build a security roadmap to:

a. Implement compliance

b. Measure compliance

c. Report compliance

d. Improve upon compliance

By mapping the various compliance requirements, I could also look for commonalities between the various legislations, and thereby, apply compliance once to address many legislation or regulation requirements. This can be a daunting task if you start from scratch yourself but there are some free tools out there to help you get this done, for example: NIST publishes their SP 800-53 framework in a spreadsheet (called their Control Catalog Spreadsheet) and organizations such as the Cloud Security Alliance publish their control framework in spreadsheet format as well but mapped against other frameworks and standards, such as ISO/IEC 27001. Using these already built spreadsheets, you can start your mapping exercise. Now, there are also commercial tools out there to help you navigate some of this landscape but many of those do not include privacy legislations so be sure you choose a tool that includes the content that you need (because, otherwise, you can probably build your own spreadsheet just as efficiently and for a lot less money).

Free online resources such as the ones I mentioned previously, unctad.org, can help you to start to scope the legislations that apply to your organization but be aware that some legislations have evolved to be applicable to the data of their citizens regardless of where the data ends up. For instance, the New York Shield Act and the California Consumer Protection Act (CCPA) are both USA State-level government privacy legislations but if your organization, for example, is based in the UK, and it has US client data for citizens of New York State or California, then those State-level legislations could apply to you. It is important to scope your compliance requirements and to ensure that you have completed your compliance mappings.

Luckily, there are many commonalities among various legislations across the globe and we can see this very clearly when we apply the two security triads, which many of us have learned in our study of the core ISO/IEC cybersecurity standard: ISO/IEC 27001, The Confidentiality, Integrity, and Availability (CIA) triad and the People, Process, and

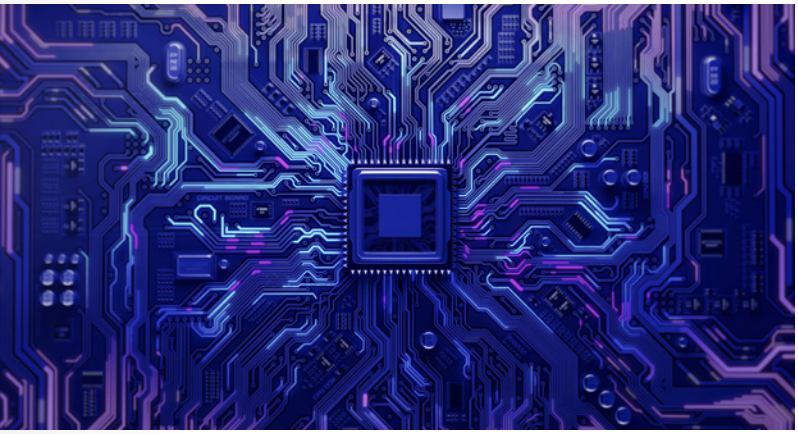
Technology (PPT) triad can both be used as lenses to focus your view of the multitude of cybersecurity legislations in the world. With regards to cybersecurity, you are always looking to protect data or assets by applying both of these triads, the same applies to data privacy protection. In addition, data privacy legislation has some commonalities, for starters: consent, use, disclosure, and correction are some of the common principles of data privacy. As a cybersecurity leader or influencer, if you keep these core security principles in mind and as foundational material for your security programs, then you can, in my opinion, better navigate the cybersecurity legislations in scope for your organization.

What if you are not a cybersecurity leader or influencer and you want to provide relevant security guidance to non-cybersecurity audiences?

When I am communicating with senior management or even to the Board level, I frame the cybersecurity discussion in the context of the business by:

- Converting technical or cybersecurity specific information into the language of what the actual threat to the organization looks like (e.g., ransomware can cause loss of access to assets so what would that cost the business in each case? Rather than describing ransomware and how it can be combatted)
- Avoiding the Fear, Uncertainty, Doubt (FUD) approach (e.g., ransomware is everywhere and it is getting worse and we will lose everything if it hits us!). FUD is similar to the fable of Chicken Little who went about saying the sky is falling constantly until no one listened anymore.

If there is one thing that this global pandemic has taught us, it is that no matter how bad we know the situation is now or can become, we all get fatigued by being given nothing but negative news. As responsible adults or responsible cybersecurity practitioners, we cannot ignore reality and pretend everything is fine because that will solve nothing and potentially make things worse. We do what we can to help the situation and this type of solution-driven discussion is a great way to push your cybersecurity agenda forward. With regards to cybersecurity legislations specifically, looking for ways to make the applicable legislations work for your organization can make compliance more functional, as opposed to being just a check box exercise (e.g., by getting your operations teams to document their processes and procedures as part of compliance you can now rely on documented information available to anyone who needs it at any time).



What if you are a busy non-cybersecurity person who needs to know enough to understand the cybersecurity needs?

There are online news sources available to the busy non-security team member: PECB Insights magazine, PECB webinars, and PECB Conferences are a few good examples, and there are others out there. In addition, I have personally seen Board members be recommended to complete some basic cybersecurity training so they can at least understand the context of data and privacy protection in their organization. Ultimately, you will need to find the best way for you, to swim through the ocean of cybersecurity legislations out there and, as with all things these days, you should expect a lifelong learning experience on this topic!

Anthony English
CEO/CISO Bot Security Solutions Inc.

Anthony English is a seasoned IT and Security professional with multiple certifications in both disciplines. He 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 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. He holds multiple certifications including ISO 27001 Master, PCIP, CISSP, CBCP, CIPP/C, CISO, CRISC, CGEIT, ISO 27032 Lead Cybersecurity Manager, CISM, CISA, and more.

Abilene Academy's Success Story

When I was asked to contribute to the Success Story portion in this edition of PECB's Insights Magazine, I wondered what I would be talking about. First of all, what is success and have we really experienced a success story?

This gave me an opportunity to meet with the Abilene Academy team to do a retrospective on where we started and where we are today. We could have opted for enumerating facts and figures on how well we do and how "smart" we are. But we concluded that success is not ours alone; we share it with our customers, our partners, trainers, and we also share it with PECB.

So let us analyze the factors that led to this success.

We talk the talk because we walk the walk

Firstly, what is Abilene Academy? The training services division of Abilene Advisors. Our initial intention when creating Abilene Advisors in 2015, was to gather our skills, expertise, and competencies to help our customers implement management systems and comply with normative and regulatory frameworks. We consider education and training to be some of the main drivers of a successful management system implementation.

All our trainers are experienced advisors, and all our advisors must spend time delivering training courses.

This is a fundamental cornerstone: the main principle when delivering a course is to make sure that we tell "real-life" stories. We are convinced that the participants who chose Abilene Academy do not want to spend four days listening to a person reading the course slides, nor do they need someone to explain what is on the slides. PECB's excellent training material is self-sufficient for that. The added value of our course delivery is nothing less than our own experience. Hence our motto at Abilene Academy is: Experience matters!

We aim to be trustworthy and generous

A wise businesswoman once told me: "If you keep your hand closed, no one will ever take what is in it but nothing will be deposited in it either; if you open your hand, some will take what you have in it, but others will deposit something".

As a team, we do not hesitate to give. We spend time with our participants long after the courses, we help them with different services, such as short-course refreshers, administrative shortcuts, or attentiveness to their financial limitations.

We also open our hands to our partners and to PECB and never hesitate to spend time for the common greater good.

So far, this approach has paid off.

We make sure that everyone in the team adapts to the customer service mindset. It is not simply solving problems for the customers. It is about creating a delightful and

unique experience that develops long-term relationships and loyalty. It is not enough to deliver a course. We have to focus on the entire experience: the purchase, the preparation, the delivery, and the aftersales service. For instance, if participants have traveled to be with us, we try to make sure they enjoy their stay.

The Head of training services with her vast experience in the luxury industry, used to say: "We pamper our customers. Every customer is unique and must be delighted by our services. Every customer must feel like they are the only one". That is why we have returning customers.

We attempt to constantly observe, understand, and anticipate the needs of our customers; before, during, and most of all, after the delivery of the course. Also, we seize every opportunity to reassess and identify what leads to certain results within our organization.

As an example, we have a unique agreement with the ISO Central Secretariat that allows us to provide each participant with their own legitimate and licensed copy of the necessary ISO standard.

> **"Abilene Academy offers a set of quality training, adapted to the needs of the IT market. The Abilene Academy team by its professionalism allows to follow, to provide, to advise people in the choice of training, to offer several types of training in relation to each person's needs. The strength of Abilene Academy is its adaptation to our professional expectations as they bring real flexibility in the articulation of the formations which are proposed. In addition, the professionalism of the entire team makes the difference, from registration to training. Thanks to Abilene Academy" – Jean-Guy Ahanda**

We are not afraid to try and fail, because we are confident in our abilities

Ideas and innovations are always there but putting them in action is another story. Many obstacles come along the way, such as time and money. However, we once decided

that if 50% of our initiatives would be successful, that would be considered a very good performance. So we try and fail, try again, and again until we succeed.

The Scottish mathematician Thomas Carlyle said it best:

> **"Nothing builds self-esteem and self-confidence like accomplishment".**

No need to climb Everest. It suffices to look at our everyday actions and judge them with objective compassion. This way, all the little challenges count, and self-confidence is constantly nurtured.

So we will continue trying and failing, and more importantly trusting ourselves to eventually succeed. Even if that sometimes requires swimming upstream and ignoring detractors.

We are always on Day 1

Surely, the COVID-19 pandemic forced most of us to deploy countless resources of imagination and inventiveness to maintain our businesses afloat, "adapt or disappear", necessity is the mother of invention.

We surely did reinvent the way we work in response to the pandemic: a new course delivery platform (our #LearnAnywhere concept), a new marketing approach, and a new customer relationship channel.

And most of this change and evolution would not have been possible without PECB. After all, this is normal, it is what makes a resilient economy. But for Abilene Academy, we do not consider this enough. We will not wait to be constrained to move: reinvention is happening every day! We have adopted Amazon's CEO, Jeff Bezos, Day 1 mentality: every day of our company is Day 1 of our startup, focusing on what our customers would need, how they would need it.

> **"Day 2 is stasis. Followed by irrelevance. Followed by excruciating, painful decline. Followed by death. And that is why it is always Day 1." – Jeff Bezos**

We do not fight change, we embrace it

Many influences tend to push us into Day 2, such as natural entropy, lack of discipline, new technology trends, competition, even success itself, because it makes you self-satisfied and lazy. The solution is to not fight against these influences but to accept them and build on them.

The economy, the crisis, the pandemic, everything gets in our way to prevent us from doing business and crushes us if we fight against it, because after all, we are insignificant. So we happily embrace the changes and make the most out of the new or changing circumstances.

We focus on the results, not on the processes

What works well today, is no guarantee of future results. So we try to stay light and agile by:

- Focusing on the outcome of our actions and initiatives, not on the processes
- Deciding quickly and frequently revisiting past decisions

- Changing directions swiftly if we cannot reach expected results
- Asking ourselves constantly where we can go from here to efficiently obtain short-term positive and gratifying outcomes with limited resources

Hard work and discipline

These may be the most important factors of all. All victories inevitably come at a cost.

> **"What is success? I think it is a mixture of having a flair for the thing that you are doing; knowing that it is not enough, that you have got to have hard work and a certain sense of purpose" – Margaret Thatcher**

We recently received the PECB Central Europe Partner of the year Award. That is validating and we are full of gratitude! But behind this award, there is a lot of sweat. Countless hours of hard, and often repetitive work as well as the implacable discipline of the Abilene Academy team.

We break some rules

This comes with creativity and innovation. Rules are there to be changed because the world changes. And because creativity is inventing, experimenting, growing, taking risks, breaking rules, making mistakes, and having fun, therefore, we extend our thanks to PECB for their flexibility and understanding.

Breaking rules is also looking outside the box, getting out of your comfort zone, and being ready to fail.

I would add eagerness to fail, because failure enables us to learn and become stronger and that brings us back to Day

1, the day when we still dream big and think that everything is possible. When we still believe that when there is a will, there is a way.

> **"If your dreams don't scare you, they're not big enough." – Mike Horn**

We are proud to contribute to a better world

Finally, the last factor is luck. We were lucky to have been selected by a number of large international organizations and NGOs (though living near Geneva undoubtedly helps!) to assist them in implementing ISO's best practices and in delivering training courses.

We have the honor of offering our services to organizations such as: The Global Fund (whose mission is to fund projects to fight against malaria, tuberculosis, and HIV), to Gavi, the Vaccine Alliance (who contributes decisively to the fight against the SARS-CoV-2 pandemic in developing countries), the International Atomic Energy Agency (IAEA), and the International Committee of the Red Cross (ICRC).

Contributing to a better world brings us this feeling of fulfillment that makes us jump out of our beds every morning, ready to take a bite of hard work.

> **"Abilene Acadamy can benefit risk and information security managers in both public and private sectors to improve their organizations' ability to meet their goals. The trainers are top-notch and the venues, highly conducive to learning. Highly recommended!" – Andreas Tamberg (The Global Fund)**

In conclusion

To summarize, the ingredients to our success are being trustful, generous, and self-confident. Dream big and never forget your dreams, work hard to make them a reality. Do not fight change but embrace it, break some rules, acknowledge your luck, and show gratitude. That is, at least, what worked for us. We are not so presumptuous as to think that this would work for everyone.

Henri Haenni
CEO & Head of Sales at Abilene Advisors SA

Henri is the CEO and Head of Sales of Abilene Advisors SA, a cybersecurity, resilience, and data protection advisory and training firm located in Switzerland, on the shore of the Geneva Lake. He and his team advise large international organizations globally on how to implement information security and business continuity best practices and international standards. He is also an international instructor, PECB certified trainer, and lecturer at Paris 1 Sorbonne University.

Tips on Maintaining a Healthy Work-Life Balance

Discussions around work-life balance and burnouts are one of the most common. Due to the flow that the world is operating at, whatever your job may be, most industries are becoming notoriously demanding, with roles carrying vast pressure and responsibility.

To quote Nigel Marsh in his TED Talk on this topic: "*Certain job and career choices are fundamentally incompatible with being meaningfully engaged on a day-to-day basis with a young family*", however, to what extent are information security professionals fated to work long hours without having sufficient time for other aspects of their lives such as; family, friends, hobbies, etc.?

Here is a list of some simple practices to help you in balancing your work and life.

1. Prioritizing and maximizing your time

Throughout the day there are many things competing to grab your attention, and it can be difficult to attend to all of them. Creating a to-do list can help in prioritizing your tasks by categorizing them in different matters of urgency and importance.

Often times calculating how much time each task takes helps in the creation of your list. Even though there may be days when completing 100% of your tasks is unlikely, make sure that you do not get overwhelmed and ensure that you have a system in place to address the most crucial tasks?

2. Playing to your strengths

Decide what you want to do and stay with it. If you want to be a leader, get involved with management and strategy. If you want to be technically hands-on, then sharpen your craft.

An important point is utilizing your team. As a leader, you need to learn to delegate and hand off some activities. As an analyst, then draw upon your team and ask for support. Deploy the resources you have in their strongest areas to maximize results.

3. Having set work hours

Make sure you predetermine your work hours and stick to them. This way you will not get lost in your workload and lose track of time.

Long work hours affect both, your physical and mental health. Spending a significant part of your day working means there is not enough time to rest and recharge for the upcoming day.

4. Making time for yourself

Time management is important in all life aspects, but of utmost importance when it comes to making time for yourself during the workweek. Allocating time for your own physical and mental well-being is key. Be that a few minutes run before the start of your day, a 30-minute cup of a coffee break for your relaxation, or a few pages of a book during your lunchtime. It is crucial to give yourself enough time to switch off from your job so you can make time for something you enjoy and are passionate about. Consider how your activities contribute to your mental and physical health, career, or personal satisfaction. Take a look at your schedule and see where you can fit some time for yourself.

5. Identifying productivity peaks

Focus on your strengths. Know the time of day you are most efficient, an example would be; if you are a morning person assign tough, high-concentration tasks to the mornings. Focus on your strengths.

Some people are at their most productive and creative in the early morning, others prefer a slower start and are most efficient themselves in the afternoon.

Structure your workload around your most productive periods to reduce procrastination and the frustration brought on by a lack of productivity. As long as the work gets done, it should not matter when in the day it happens. Remember, work-life balance does not come down to a single factor. It is not simply about the number of hours worked or the weeks of vacation taken.

We all require unique support to thrive in the workplace and maintain a happy, healthy, and fulfilling personal life. Attaining the perfect work-life balance can be difficult, but taking on the above advice and asking yourself these analytical questions, can certainly get you thinking about how best to utilize your time and guard against burnout.

Mark your calendars for February 21-22, 2022, for our upcoming Anti-Bribery Conference. This will be a two-day virtual event that similarly to our previous virtual conference, will feature two sets of three simultaneous sessions per day. The first set of sessions will begin at 3:00 PM CET, and the second set will be at 5:00 PM. Each virtual panel will last for one hour and will be headlined by anti-bribery experts and professionals from around the globe.

The PECB Anti-Bribery Conference 2022 will feature an extensive program that will contain sessions in English, French, and Spanish. Panels will cover topics from different areas of anti-bribery and the fight against corruption, with a specific focus on ISO 37001, whistleblowing, money laundering, and much more. To view the entire conference program, please click **here**.

The PECB Anti-Bribery Conference is a one-of-a-kind opportunity to hear from ISO 37001 professionals and enthusiasts from all around the world in an online environment. Connections made at PECB conferences are long-lasting and provide you with new potential business ventures.

Do not miss out! **Reserve** your seat for free now, and do not forget to invite a friend or colleague.

REGISTER HERE!

PECB ANTI-BRIBERY CONFERENCE 2022

Security Considerations for 5G Technology Enablers

BY LUC SAMSON

In order to completely fulfill the business needs driving the development of 5G by the 3GPP standard organization, 5G uses and introduces technology enablers that transform 5G networks into cloud-based, programmable, software-driven, service-based, and holistically-managed infrastructures, utilizing enablers such as cloud technologies, Artificial Intelligence, open APIs, and Multi-access Edge Computing.

Although 3GPP standard specifications have increased the security of 5G relative to 4G, the use of those enablers, some of which are not in the scope of 3GPP, have introduced new security threats and vulnerabilities that cannot be addressed solely by the 3GPP security framework.With such a diversity of technology enablers composing the 5G solution eco-system, the overall 5G security framework looks fragmented.

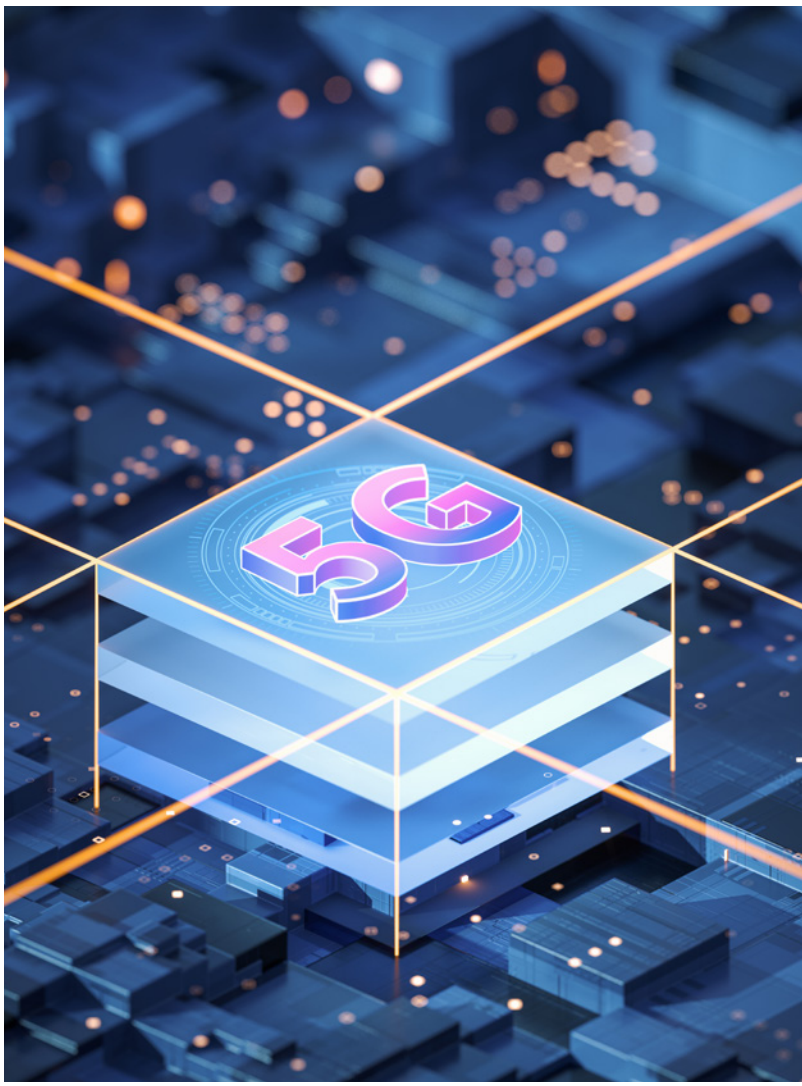
This article presents the technology enablers introduced or used by 5G, with their respective security vulnerabilities. It also presents the contribution of key organizations, government, and industry groups that work on securing 5G enablers via security standards, vulnerability analysis, and best practice recommendations.

1.0 5G Business Drivers

Four generations of cellular technologies were all about connecting people, whereas 5G is about connecting people and everything else.

In line with this vision, the 5G business objectives are:

- **Enhancing Service Offerings** – relative to 4G with improved network performance, a wider range of types of devices supported, and more vertical segments being better served
- **Creating New Business Models** – beyond connectivity provider by fostering an open and agile ecosystem of partners and allowing customers to self-manage their services



- **Improving Operational Efficiency** – by shortening the time-to-market and time-to-customer of new services, by simplifying network operations, and reducing the cost of services

Taken together, those objectives will accelerate the digital transformation of pivotal economic sectors.

2.0 5G Enablers

This figure shows the dependency between the 5G business drivers and the 5G technology enablers.

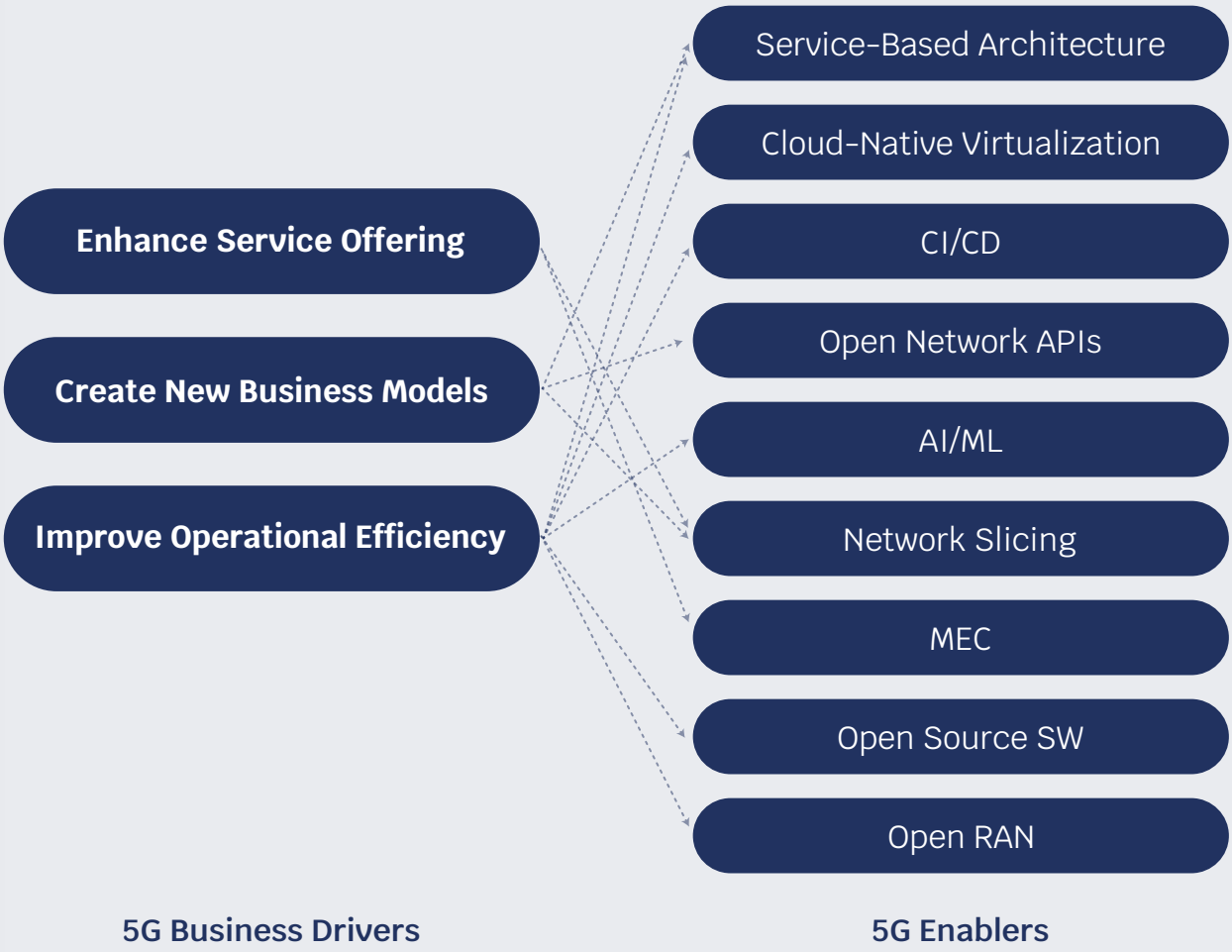

Enhance Service Offering
Create New Business Models
Improve Operational Efficiency
Service-Based Architecture
Cloud-Native Virtualization
CI/CD
Open Network APIs
AI/ML
Network Slicing
MEC
Open Source SW
Open RAN
5G Business Drivers
5G Enablers

Figure 1

2.1 Service-based Architecture

The biggest contribution towards a Cloud-Native 5G comes from the 3GPP-proposed Service Based Architecture (SBA) in all control-plane, user-plane, and management-plane Network Functions. This architecture makes the development of the 5G network far more modular compared to legacy systems and enables functional and service agility. With SBA, 5G network functions communicate using HTTP 2.0 messages, with REST API calls to each other on their well-defined interfaces.

To protect the SBA, 3GPP TS 33.501 introduces a new security domain for 5G SBA domain security composed of a set of security features that include:

- Network function registration, discovery, and authorization security aspects
- Authentication (TLS 1.2 or 1.3), authorization (OAuth 2.0), and encryption (TLS 1.2 or 1.3) of API calls between the 5G NFs

3GPP has been also working on specifying hardening of network nodes so that their security can be tested and certified. Security requirements and test cases for network equipment implementing 3GPP 5G network functions are specified in 3GPP Security Assurance Specifications.

2.2 Cloud-based Network Virtualization

One of the most important innovations in the 5G architecture is the complete virtualization of the core network. Whether virtualized as Virtual Network Functions (VNFs) or Container/Cloud-native Network Functions (CNFs), the 5G network can now be deployed on any public, private, or hybrid cloud infrastructure.

As a result of virtualization, network resources can be configured, possibly without human intervention, and allocated to service the needs of specific customers or service categories, without needing physical adjustments or dedicated infrastructures. This enables service and network automation.

Although container-based cloud-native architecture provides some inherent security protection due to isolation and containerization, the virtualization of network functions will introduce new and complex security vulnerabilities that can be categorized as:

- Container vulnerabilities
- Container networking vulnerabilities
- Hardware & host vulnerabilities

Some solutions for the abovementioned include:

- Hardening of the NFV and CNF Infrastructure
- Implementing strong security mechanisms for authentication, authorization, encryption, and validation in the virtualization management layer
- Securing the Orchestration and Automation layer responsible for managing the VNF/CNF

The following organizations have made significant contributions to cloud security:

- ETSI Network Function Virtualisation Security (NFV SEC) working group: NFV security specifications
- NIST: guidance and recommendations
- 3GPP: security assurance for virtualized products; security impacts of virtualization
- ENISA: security aspects of virtualization
- ONAP: VNF API Security Requirements
- NSA-CISA: Security Guidance for 5G Cloud Infrastructures
- CSA: Best practices for mitigating risks in virtualized environments

2.3 CI/CD

Although used extensively in the IT domain, CI/CD is relatively new to the telecom domain. CI/CD will become a necessary part of the network life cycle management to achieve automation and agility, ensuring carrier-grade stability, and improving operational efficiency. A CI/CD pipeline could span multiple organizations, originating in the SW vendor domain and terminating in the operator domain, thus increasing the security risks.

Security aspects must be integrated into the design of the end-to-end CI/CD pipeline from start to finish and should be incorporated in security best practices. NIST SP 800-204C provides guidance for implementing CI/CD pipelines with high-security assurance.

2.4 Open Network APIs

3GPP standardization defines the following network exposure capabilities to enrich the collaboration between network operators and the eco-system of third-party service and application providers:

- The **Network Data Analytics Function (NWDAF)** collects network data, performs analytics, and provides results to the operator's analytic engines.


5G

- The **Network Exposure Function (NEF)** in 5G provides the ability to convert network capabilities and network APIs into special service APIs that can make network capabilities discoverable and available at the application level.

The uses of these new Open Network APIs introduce new threat vectors, but 3GPP has taken steps in enhancing the security for the external API communication by introducing security features and security mechanisms for the common API framework (CAPIF) as specified in 3GPP TS 33.122. 3GPP TS 33.501 covers security aspects of Network Exposure Function (NEF).

2.5 Artificial Intelligence & Machine Learning (AI/ML)

AI/ML is a key enabler for 5G in the automation of network planning, network operations, and service assurance across all network layers i.e. 5G RAN, the backhaul transport, and the 5G Core. However, this enabler is also available to the attacker, and AI-driven attacks are anticipated.

5G being increasingly dependent on AI/ML for critical functions and services will not only create greater incentives for attackers to target those algorithms, but it also brings the potential for each successful attack to have more severe consequences. In addition to providing generic software and hardware security for the AI/ML applications, the integrity and confidentiality of the AI models and data need to be protected to prevent attackers from stealing the data or changing the inference results.

The ETSI Industry Specification Group on Securing Artificial Intelligence (ISG SAI) develops technical specifications and reports focusing on three key areas; using AI to enhance security, mitigating against attacks that leverage AI, and securing AI itself from attack.

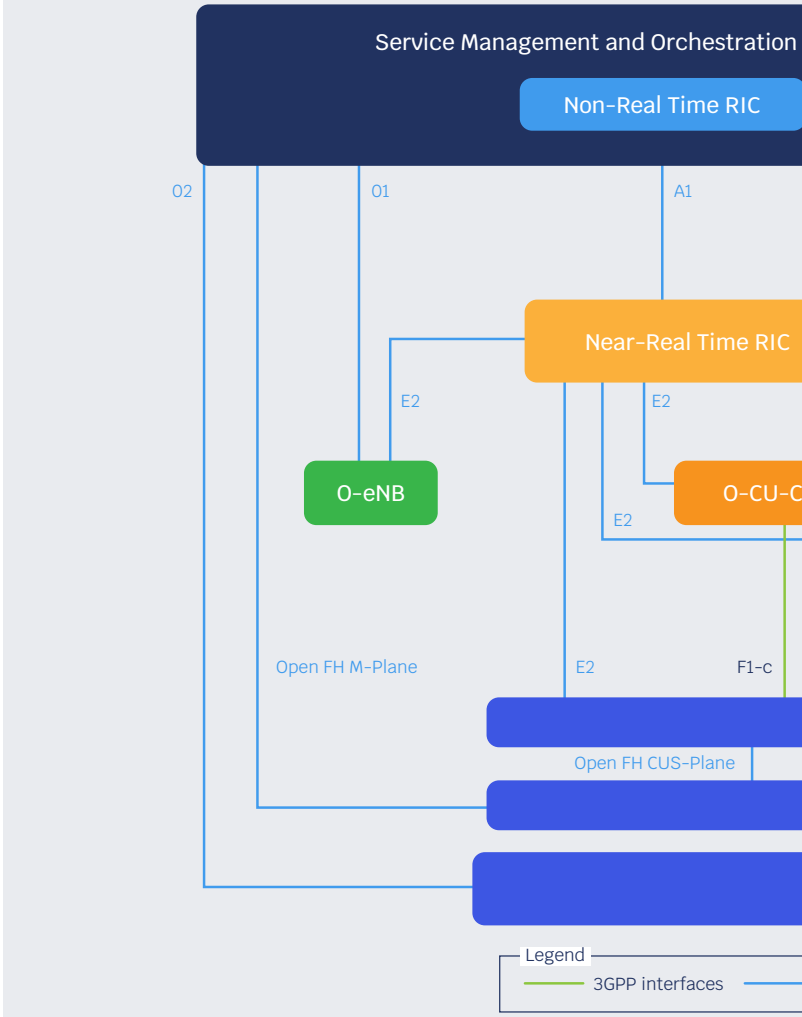


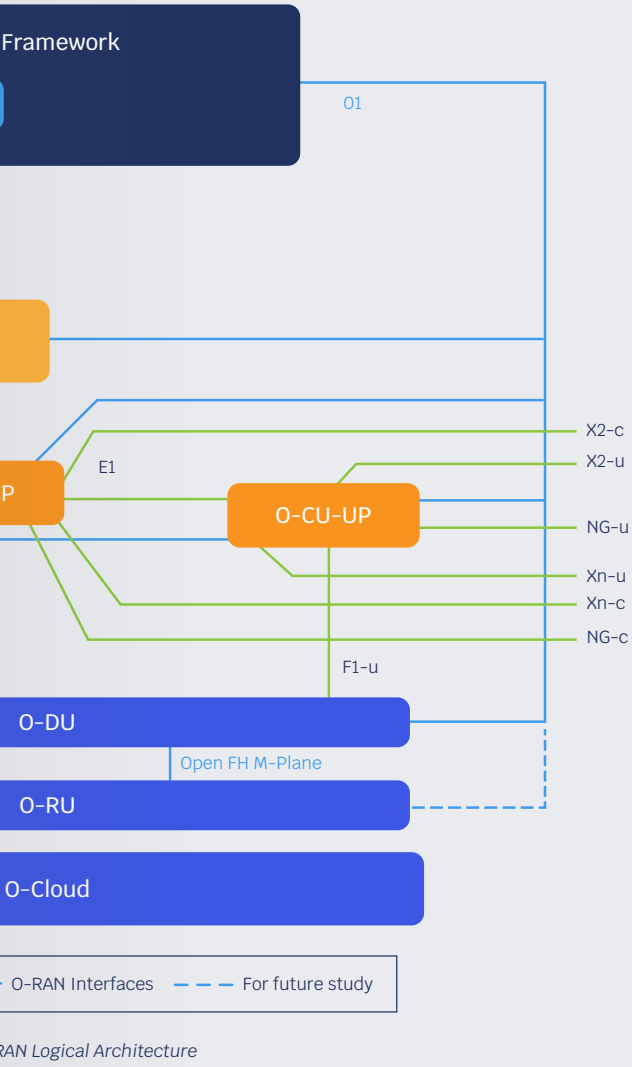
Figure 2: O-R

ETSI GR SAI 004 describes the problem of securing AI-based systems and solutions. ETSI GR SAI 005 summarizes and analyses existing and potential mitigation against threats for AI-based systems.

NIST is currently working on an AI Risk Management Framework that aims to foster the development of innovative approaches to address characteristics of trustworthiness.

2.6 Network slicing

Network slicing is a key architectural feature in 5G that enables multiple virtual networks to be created on a single physical network infrastructure. A network slice is effectively a logical network serving a defined business purpose or customer consisting of all required network resources configured together. With network slicing, the 5G system is capable of simultaneously supporting multiple combinations of reliability, latency, throughput, positioning, and availability requirements.



RAN Logical Architecture

However, improper network slice management may allow malicious actors to access data from different slices or deny access to prioritized users. Network slices are intended to be configured with different levels of security depending on the user SLA requirements. Therefore, the security model for each slice should be adapted to the specific use case and should consider the following categories of measures:

- **Slice Access Security:** to complement network-level authentication mechanisms with network-slice-specific authentication and authorization mechanisms
- **Slice Isolation:** of traffic, of bandwidth, of processing, and storage
- **Slice Management Security:** management of network-slice-specific log information to support post-incident and root cause analysis

3GG TR 33.811 and 33.813 present studies on the threats, potential security requirements, and solutions for the 5G network slicing management, and they include identification of key security issues and recommended mitigation measures.

2.7 Open RAN

The ambition for Open RAN is to create a multi-supplier RAN solution that allows for the separation between hardware and software with open interfaces and virtualization, hosting software that controls and updates networks in the cloud. The promised benefits include supply chain diversity, solution flexibility, and new capabilities leading to increased competition and further innovation.

As shown in the figure, the O-RAN Alliance architecture introduces additional interfaces, functional splits, and disaggregation.

The expanded attack surface from additional RAN network functions and open interfaces creates additional security vulnerabilities.

The O-RAN Alliance Security Focus Group (SFG) develops solutions to counter threats, and it sets security requirements and protocol specifications for each O-RAN release to guide the development, deployment, and operation of an O-RAN:

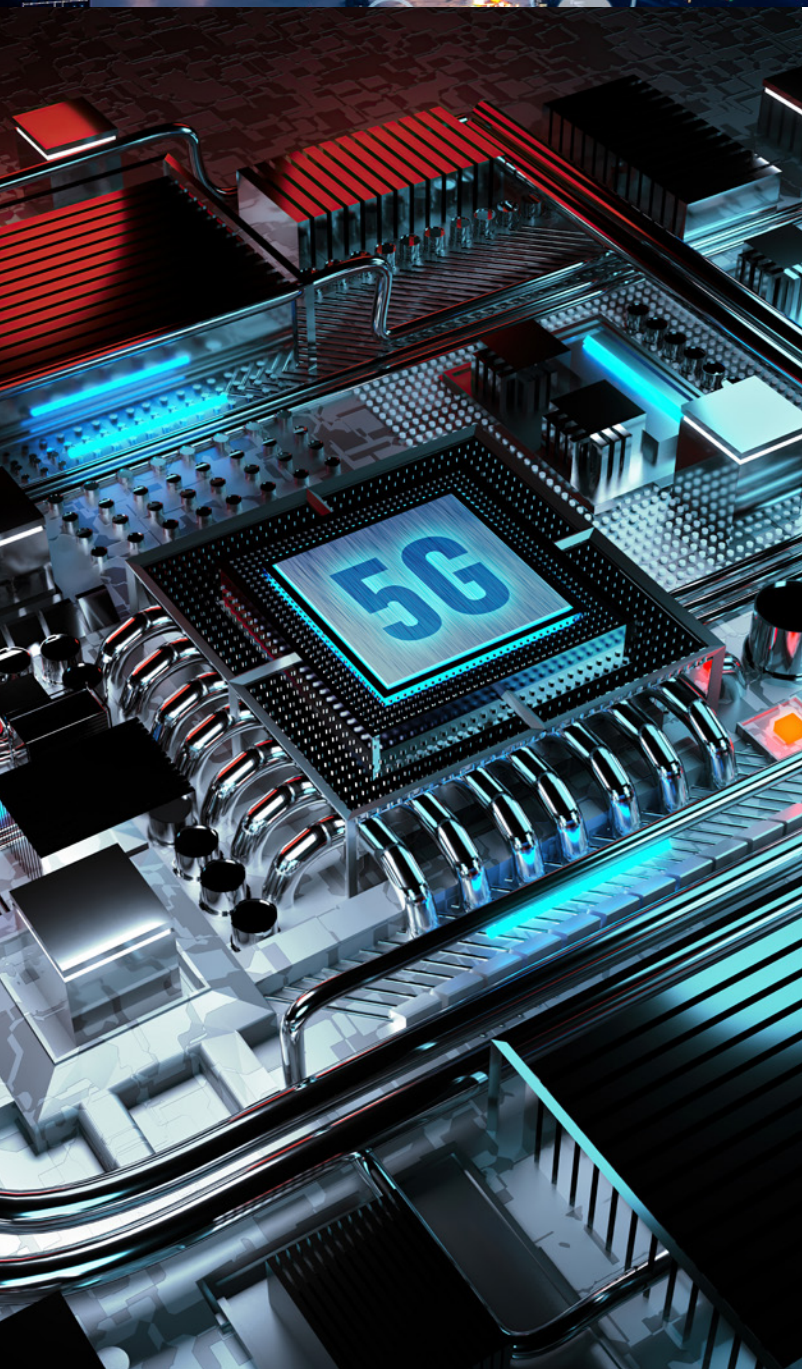
- O-RAN Security Protocols Specifications v2.0
- O-RAN Security Threat Modeling and Remediation Analysis 2.0
- O-RAN Security Requirements Specifications v1.0

2.8 Multi-access Edge Computing (MEC)

In the context of 5G, Edge Computing is a concept that enables services to be hosted close to the service consumers, with 5G network elements and application servers potentially installed on customer premises.

MEC provides a significant reduction in end-to-end latency and on load on the transport network, which is key to addressing several new and enhanced use cases – including Industrial IoT, Industry 4.0, autonomous driving, etc.

By having network elements and MEC application servers hosted on customer premises outside the security perimeter of the operator's network, the key security threats to MEC are related to physical security, software tampering, MEC nodes overload, abuse of MEC open APIs, and vulnerabilities related to virtualization and containerization infrastructure hosting the MEC. Because the various elements of the MEC system can be deployed, managed, and operated by different stakeholders, MEC environments are intrinsically heterogeneous, which increases the security risks.



Furthermore, the overall MEC system security design heavily depends on the security practices and specifications of closely related 5G enablers e.g. cloud infrastructure, Open Network APIs.

- ETSI White Paper No. 46 MEC security presents the status of security-related standards, such as:
  - ETSI ISG NFV for infrastructure virtualization and management
  - Trusted Computing Group (TCG) for physical platform security
  - IETF specifications for securing access to MEC services
- ENISA 5G Threat Landscape identifies the potential threats related to MEC
- 3GPP TR 33.848 on security consequences of virtualization applies to many MEC use cases where the need for additional security controls is higher than in core network data center

2.9 Open-source SW

The use of software from open source is common in a range of initiatives driving open architectures and virtualized telecoms infrastructure such as Telecoms Infrastructure Project (TIP), Open-Radio Access Network (O-RAN) Alliance, Linux Networking Foundation, and Open Networking Forum. Most of those initiatives sponsor open-source projects upon which 5G commercial solutions rely.

Open-source code has a number of advantages, most notably:

- The transparency of code reduces software complexity, fragmentation, and bug count
- It increases interoperability across commercial products by creating de facto standards
- Contributes to a wide community of developers that can accelerate telco cloud implementation.
- It facilitates security testing by independent third parties

Risks

- The integrity of the software, especially from open-source locations and the overall software supply chain, is an area of vulnerability
- Malicious developers can introduce intentional backdoors
- Attackers can review the code and identify vulnerabilities

The use of open-source software requires a higher level of due diligence, which organizations can implement by using tools and applying industry best practices for supply chain management, secure software development, and secure software maintenance, including:

- Software composition analysis (SCA) tools are used to generate the software bill of materials (SBOM), a documented list of third-party software suppliers, including free and open-source software; SBOM is an industry best practice for a secure Software Development Lifecycle (SDLC) process to properly and safely handle software vulnerability notifications and updates
- Static & dynamic application security testing (DAST & SAST) to analyze and test applications for static code-based and dynamic run-time security vulnerabilities
- The Linux Foundation Core Infrastructure Initiative (CII) has a Best Practices Badge for open-source projects to self-attest
- OWASP has made available many automated vulnerability detection tools available to open-source projects
- NIST offers valuable guidance for open-source software security:
  - NIST's recent white paper "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)" recommends that open-source software consumers ensure that software modules are vetted for vulnerabilities and actively maintained for remediation.
  - NIST SP 800-161 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" provides guidance for OSS to be continuously evaluated, monitored, whitelisted, inventoried, supported, and remediated.

3.0 Conclusion

This article has presented an overview of references to key security standards, vulnerability analysis, and best practice recommendations with regards to the 5G technology enablers.

Luc Samson
President at Briskwave Consulting Canada

Mr. Luc Samson is president of Briskwave, a consulting firm that helps wireless carriers and solution providers rapidly take advantage of new opportunities, design cost-effective networks, efficient operational processes, and accelerate acceptance and deployment of new services & solutions. Mr. Samson's expertise lies in managing strategic initiatives in technology evolution, vendor selection, and solution deployment with a focus on 5G transformation and network sharing. He is currently planning 5G deployment with carriers in North America and has extensive experience in successful network sharing programs.

Mr. Samson holds a Master's degree in applied sciences, and he is the author of numerous technical papers, and he owns two patents. More detailed information can be requested at luc.samson@briskwave.com.

PECB is honored to receive a nomination for the Best Cybersecurity Education Provider for 2022!

This nomination is presented by **Cybersecurity Excellence Awards**, who honor individuals, organizations, or products that showcase excellence, leadership, and innovation in information security.

We would like to greatly thank our customers and partners for their continual trust, support, and loyalty. It is through our cooperation that we have evolved and will continue to get better.

VOTE HERE ▶

The Future of Mobility: Opportunities and Cybersecurity Threats of Autonomous Cars

BY PINAKI LASKAR

In January 2014, SAE International, formerly known as the Society of Automotive Engineers, classified the future of the automobile. A system was developed defining six levels of automated driving from SAE Level Zero (no automation) to SAE Level 5 (full vehicle autonomy). It has since become one of the most widely used standards for systems classification.

Autonomous driving is at a developing stage, however, it is estimated to help safe driving. Despite that, as people, the avoidance of accidents may not be entirely possible as of now but the developments in the field seem hopeful. In my opinion, the case of autonomous driving is that it creates plenty of business opportunities and frees up time, suddenly you do not need a driver, allowing you to use that time to do something else, such as; sort out your kids' homework during that commute, sort out groceries, or get some extra work done. With the implementation of autonomous driving, advertising platforms will be able to explore more business ventures as well!

Granted, there are some areas of concern that raise a few questions, for example, who is liable for the handover period between self-driving systems? What suggests that staged handover systems may be needed to ensure a safe transfer of control, especially at higher speeds?

Lawmakers have been urged to consider the time it takes a driver to take back control from automated systems after new research revealed a significant gap in reaction time. The latest report found delays of up to three seconds between a vehicle deactivating its autonomous mode and a driver taking back control. While there is clearly much to understand about the safety and security of autonomous and cooperative automated driving (AD), connected cars remain in development – and will become a viable proposition in the not-too-distant future.

Let us clarify that the presence of devices in an automobile that connects the devices within the car/vehicles,

networks, and services outside the car including other vehicles, home, office, or other apps, makes the car connected to Wi-Fi. Cars can now warn drivers of accidents, traffic, collisions, and other safety alerts such as snowy or slippery roads.

Multiple threats and vulnerabilities exist and more will doubtlessly emerge as technology progresses. It is worth noting that, nowadays, vehicles increasingly feature automated driver assistance technologies – such as; forward-collision warning, automatic emergency braking, and vehicle safety communications.

Vehicle cybersecurity, for some time, has been a glossed-over area of research in the development of driverless vehicles. While this is an ongoing multi-industry discussion, there are still some pertinent issues.

Technology is about trust

Advancements in driver assistance technologies rely on a multitude of electronics, sensors, and computer systems. Connected and automated vehicles, also referred to as 'cyber-physical systems', with components in the real and virtual worlds.

As all other things online, these systems are vulnerable to those that regularly disrupt computer networks, like data thieves or malicious actors (be that personal or financial information), spoofers (who present incorrect information to automobiles), and denial-of-service attacks (that shut down computers or vehicles). In addition, hackers could shut-down or take control over a vehicle, lawbreakers could ransom a vehicle or its passengers, and car thieves who direct a self-driving car to relocate itself.

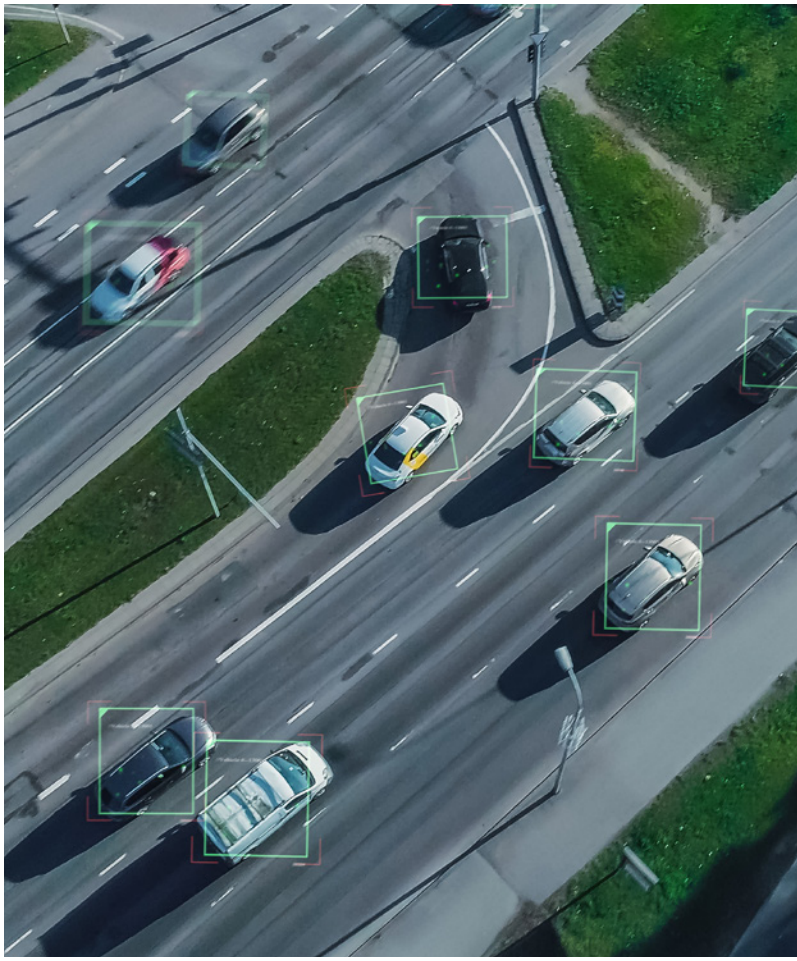
Many vehicles use the Controller Area Network (CAN) to communicate with a car's Electronic control unit (ECU), which operates many subsystems, such as; antilock brakes, airbags, transmission, audio system, doors, and many other parts—including the engine. The newer car models, also use Diagnostic Version 2 port that is used to diagnose problems, this could be abused by CAN traffic, and interrupted from the On Board Diagnostics (OBD) port which can be plugged into a car as a backdoor for external commands, controlling services, for example: the Wi-Fi connection and unlock the door.

For automobiles, applying cybersecurity is vital. Systems and components that handle safety must be protected from harmful attacks, unauthorized access, damage, or anything else that might have an interference with safety functions. Furthermore, vulnerabilities in automated parking are more prominent due to mechanical attacks disabling the range sensors in park-assist, or remote parking in order to require additional maintenance. To name a few examples:

- In 2016, hackers proved the Nissan Leaf could be hacked from anywhere in the world via mobile app and web browser
- In 2015, cybersecurity researchers demonstrated a remote attack on a Jeep Cherokee, sending it off the road
- In 2015, hackers exploited a vulnerability in BMW's Connected Drive technology to unlock the cars
- In 2016, hackers remotely unlocked Volkswagens

There are additional security threats to the wide-ranging networks that will connect with autonomous vehicles, for instance: the financial networks that process tolls and parking payments, the roadway sensors, cameras and traffic signals, the electricity grid, and even our personal home networks. How does the AD industry deal with such multifarious potential safety and security issues?

In order to secure products across the supply chain, the automotive sector must develop new ways to collaborate.



Products can be secure only if they are designed with security in mind. High-quality components—from software to hardware—must implement the design. Original Equipment Manufacturers (OEMs) need to create and enforce stringent guidelines to minimize software-security gaps and also enable easier modifying or patching systems.

A secure design, however, does not guarantee security. To be effective, solutions must be implemented constantly. This requires an increase in collaboration between product-security teams and corporate IT-security teams. This is why over-the-air (OTA) updates, currently available for some cars, are essential for connected systems.

OTA updates assist OEMs in quick counter attacks and help eliminate specific vulnerabilities before attackers exploit them. Nonetheless, implementing support for OTA updates is pretty complex and costly, both for vehicles and the back-end infrastructure. Responsibility for implementation lies with manufacturers.

So, the need for creating strict and effective regulatory guidelines, as well as beneficial multi-sector alliances to deal with regulators and to share intelligence on threats or vulnerabilities, is even more evident.

Some automotive companies are already creating alliances, while other OEMs and suppliers should consider joining them.

Customer safety should be of utmost importance for automakers, so that connected cars will get constant oversight and protection. OEMs, Tier 1s, regulatory bodies, insurance companies, technology companies, telecommunications organizations affected by the new attack landscape are working to strengthen cybersecurity.

In recent years, government agencies have begun producing reports and guidelines such as the Cyber Security and Resilience of Smart Cars by ENISA (the EU Cybersecurity Agency), the Federal Guidance for improving Motor Vehicle Cybersecurity, NHTSA, Vehicle Cybersecurity, and Automated Driving Systems (ADS): A Vision for Safety 2.0 in the US.

In the UK, lawmakers have published their Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles.

National governments are also acting on the appearing public safety implications of vehicle cybersecurity. For example, in 2017 US regulators passed bills like the 2015 Spy Car Act and the Security and Privacy in Your Car Study Act, which focused on vehicle cybersecurity.

US authorities have also passed the SELF DRIVE Act and the AV START Act, which make cybersecurity a necessary component of any automated driving system.

However, even if the industry puts its best efforts forward, we will succeed only if car drivers understand the importance of cybersecurity, make efforts to maintain it, and take measures to avoid threats. There is a lot of work to still be done but there are interesting challenges and opportunities awaiting.

One of the main conclusions to be pointed out, is that while legislators need to take into consideration the handover period while determining new regulation, it is still important to highlight the capability of drivers and avoid restraining the appeal of the technology by unfairly penalizing them.

in

Pinaki Laskar
Founder of Fisheyebox Autonomous Intelligence

A Visionary who is Transforming Tech into an Art & Business and an AI Researcher, Inventor, Futurist Speaker, XAI Author & Thought Leader, Spatial Computing Savant, and NextGen Mentor. He is a disruptive Innovator & Cognitive Technologist, and has been the founding brain for many disruptive AI solutions ranging from Autonomous Car and Intelligent Transport System, Brain for ITS & Future Mobility, Developing AI Chips, and Providing affordable Autonomous Driving DNA for self-driving Autonomous cars.

Pinaki is one of the top 10 Influencers of Self-driving Cars and Data scientists in the world and the Top 20 Global Thought Leaders & Influencers on Autonomous Vehicles.

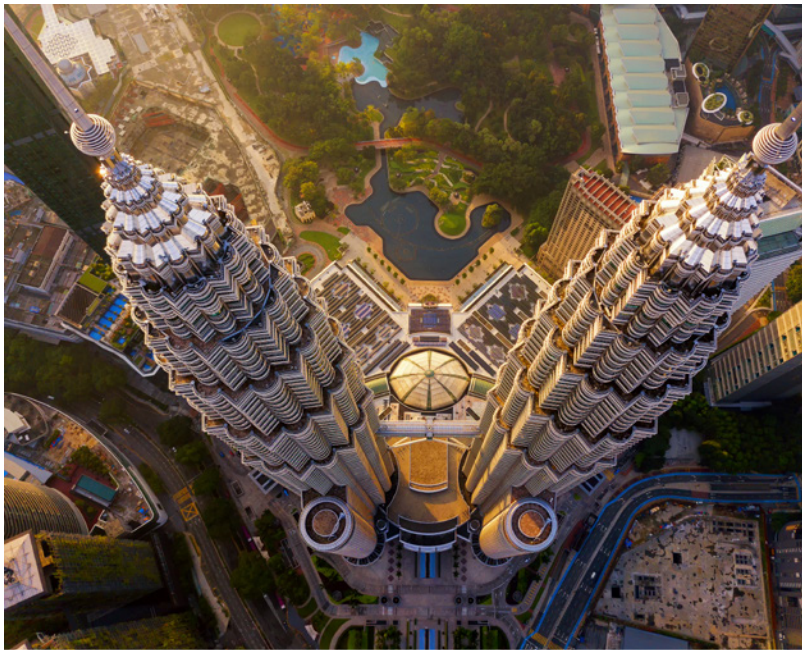
WALKING THROUGH THE CAPITAL

KUALA LUMP

OF MALAYSIA

UR

A colorful cultural hub, the capital of Malaysia, Kuala Lumpur, also known as “KL” or “The Garden City of Lights”, has a lot to offer for your stay. From boasting gleaming skyscrapers, colonial architecture, numerous landmarks, charming locals to a swarm of natural attractions, wandering the streets of KL means immersing in and out of an urban present into an ancient past. If you need more reason to love Kuala Lumpur, there is an abundance of gastronomic delights – with thousands of hawker stalls, cafes, and restaurants serving every imaginable type of delicacies.



Places you must make time to see

For a person with a busy schedule, hitting two birds with one stone must sound appealing. As the most visited attraction of the city, the infamous Petronas Towers had to make the list. Due to their size, they are quite hard to miss.

It is easy to get fascinated simply on entry in view of the architecture itself, however, the view from the world’s highest twin towers is nothing short of exceptional, especially through its glass floors. I would highly recommend making sure you are there around the evening since KLCC Park right outside has a light show every night, and you will understand why they call this city ‘the garden of lights’. In saying that, if nature is something that interests you more, visiting Kuala Lumpur’s butterfly park, bird park, or the elephant sanctuary might be right up your alley.

In the interest of understanding more of the culture and history, the Batu Caves are a must and a once-in-a-lifetime experience. The whole attraction is brimming in sculptures and hand-painted architectural details which stand out against the nature surrounding the perimeters. Do not let the idea of climbing 272 stairs scare you, because the climb is barely noticeable, and saying it is worth it is an understatement.

And if you are looking for a bit of fun and a relaxing day, Sunway Lagoon Theme Park is not something you want to miss. From fascinating dream-like sceneries to a whole zoo, the park leaves little to the imagination offering waterpark rides, a show, various restaurants, rollercoasters, and many more attractions to enjoy.

Restaurants and Bars

Given Malaysia’s multiculturalism, it is heaven for those who enjoy trying different cuisines due to its diversity. If a luxurious experience is what you are after, Marini’s on 57 will provide all that for you, making you feel like royalty.

With floor-to-ceiling windows and a glass roof, it offers you fine dining with an up-close gorgeous view of the towers. On the other hand, Petaling Street is a popular destination for street food where all go to grab spices, ingredients, and specialties such as salted roast duck or Hokkien mee, a Southeast Asian dish made of noodles, fried eggs, and a mix of meats.

On the topic of bars, The Iron Fairies provides a fairytale experience due to its interior, amazing service, and cocktail variety. However, it is highly recommended to make time and try local drinks such as Teh Tarik, also known as “pulled tea”. Besides it being delicious, having it for the experience is also worthwhile considering the theatrics of it being made.

Shopping in Kuala Lumpur

With such a wide array of shopping malls in Kuala Lumpur, it is no surprise that this is a country that takes retail seriously. More than eight major shopping malls can be found within the heart of the city, all offering world-class brands. Having a shopping day in KL is very efficient due to its pedestrian underground tunnels that connect most of the city, allowing you to never have to step outside in the Southeast Asian heat.

PECB Partnership

Our partnership with PECB was inked on the 14th of April 2020. Since then, we have collaborated well to organize a number of ISO 37001 ABMS Lead Implementer and Lead Auditor Certification Programs. We have successfully facilitated these programs with great support from the team at PECB. They provided us with end-to-end support and instant access to required documents and information as and when it was required. Even though our two teams operated in different time zones across the pacific, we managed to handle communication well. No major hiccups were apparent during the course of running our sessions, and participants have generally been very satisfied with the entire learning and certification process. We hope to continue a strong and mutually beneficial partnership going forward.

With the enforcement of Section 17A, Malaysian Anti-Corruption Commission Act 2009 (Corporate Liability Provision), and adoption of the initiatives under the National Anti-Corruption Plan 2019-2023, we see a tremendous opportunity to continuously promote, develop and certify professionals under the ISO 37001 ABMS Certification Programs offered by PECB in collaboration with Graymatter Forensic Advisory Sdn. Bhd.

Raymon Ram
MSc (Econ. Crime Mgt.), CFE, CAMS, ISO 37001 ABMS LA

Raymon is a Certified Fraud Examiner (CFE), Certified Anti-Money Laundering Specialist (CAMS) and ISO 37001 ABMS Lead Auditor with a Master’s Degree in Economic Crime Management, and Certificate In Corporate Governance by the Basel Institute of Governance, Switzerland.

Currently pursuing his Doctorate In Business Administration (DBA), he is the Founder and Managing Principal at Graymatter Forensic Advisory Sdn. Bhd., a solution-based training and consultancy specializing in Financial Forensics, Fraud Risk Management and AML/CFT Compliance. He also holds the position of Secretary General at Transparency International Malaysia (TI-M), and serves on the DTIC Governance Working Group, Malaysian Institute of Accountants (MIA).

IT Security Act 2.0: What Obligations It Imposes?

BY ULRICH HEUN

In April 2021, the IT Security Act 2.0 was passed by the German Federal Ministry of the Interior. Among other things, the regulation provides for changes in connection with the protection of critical infrastructures (KRITIS). For example, KRITIS companies are confronted with the expansion of their reporting obligations. CARMAO GmbH shows how companies can comply with the new requirements. Together with PECB, the expert for corporate resilience also offers qualifications and further training for specialists and managers on the implementation of specific measures in the area of information security complying with the new law.

The German Federal Government sees a need for many KRITIS operators to catch up on information security. KRITIS companies are organizations or facilities of critical importance to the state, the failure, or impairment which would result in lasting supply bottlenecks, significant disruptions to public safety, or other serious consequences for the common good.

A comprehensive report by the Federal Office for Information Security (BSI) had shown: IT systems in critical infrastructures are not sufficiently protected against cyberattacks. The 2020 communiqué on the state of IT security in Germany shows an increase in the number of reportable IT security incidents at KRITIS operators of over 60 percent within one year, which is why an adjustment of the existing IT Security Act was deemed necessary and carried out in 2021. The new law also strengthens the role of the BSI. It becomes the central authority with far-reaching powers.

KRITIS companies now highly challenged

The IT Security Act 2.0 significantly expands German KRITIS regulation by imposing more obligations on KRITIS operators while granting the state more power. For the operators of critical infrastructures, the new law means, among other things, a great deal of uncertainty regarding current and future requirements, as the tightening of the law may entail investments in technology, personnel, or the involvement of service providers.

Companies will be subject to an increased reporting obligation to the BSI if certain KRITIS facilities defined in the law are affected. Operators of such critical infrastructures are required, for example, to implement extensive documentation and reporting. Another major innovation of the law is the inclusion of the "waste management" sector in the list of industries that operate critical infrastructures.

In addition, the category "infrastructure of special public interest" was introduced, for which the KRITIS rules are also to be applied. This concerns sectors such as; culture, media, and defence industry.

The new regulations will lead to more KRITIS operators and more affected companies, as well as, suppliers in the German economy.

For them, it is important to increase their efforts for cyber security in order to be able to comply with the new legal requirements. In the course of the IT Security Act 2.0, organizations of "considerable economic importance" are also to present to the BSI their plans to improve their IT security.

The office then has the authority to order extra measures. In addition, companies are obliged to report cyberattacks to the BSI without delay.

BSI is also responsible for cyber security certification

The BSI is being successively strengthened within the framework of the IT Security Act 2.0 and it is being equipped with more expanded tasks as well as power.

On the basis of the new law, the BSI has now been appointed the National Cybersecurity Certification Authority (NCCA). As NCCA, the BSI is bestowed with two important functions: certification and supervision. Both functions are strictly separated and carried out independently of each other.

As part of its statutory supervision activities, the NCCA is responsible, among other things, for monitoring and enforcing statutory regulations and obligations, as well as for tracking relevant developments in the field of cybersecurity certification.

The new security law requires systems for attack detection that continuously and automatically record and evaluate suitable parameters and characteristics from ongoing operations.

These systems should be able to continuously identify and avoid threats and to provide suitable remedial measures for any disruptions that have occurred. The necessary systems for attack detection should protect the infrastructure as comprehensively as possible. In addition to the company's IT infrastructure, telecontrol technology, network control technology and process control technology are also included.

Digital consumer protection provides for basic security standards

The transfer of consumer protection tasks to the BSI is also new. The task is to strengthen security in the sense of digital consumer protection. Increasing digitalization permeates almost all areas of life, with many advantages, but also quite a few disadvantages. The increasing networking of information and consumer electronics, household appliances, and other objects of daily use creates new risks and potential attack targets for cyber criminals. As the national cyber security authority, the BSI is therefore also enforcing the establishment of basic security standards and sees the information and sensitisation of consumers as an essential task.

In future, the IT security of products is to be made visible with "IT security labels". For manufacturers, this means, that they must also comply with stricter requirements and provide regular updates and troubleshooting measures for their products. This should put a stop to the active exploitation of vulnerabilities by criminals. In its first report on digital consumer protection, the BSI warns against software and systems that often contain highly complex vulnerabilities – to the detriment of society. The report cautions against serious omissions in the security design of products. Dangerous security vulnerabilities have been found, for example, in networked doorbells and "smart" toys. This carelessness extends to providers and consumers. The still popular Microsoft operating system Windows 7 also poses a considerable security risk. The operating system has no longer been provided with free security updates since the beginning of 2020, thus, it is becoming progressively more vulnerable.

CARMAO experts help meet the new requirements

Not all points of the new safety law are uncontroversial. Many experts and specialists do not see the new extensive documentation and reporting obligations as a significant gain in security. According to CARMAO GmbH, for instance, the additional obligations keep companies from their core business. Therefore, affected companies should think about an information security management system (ISMS) or contact IT security specialists in order to be able to meet the increased requirements.

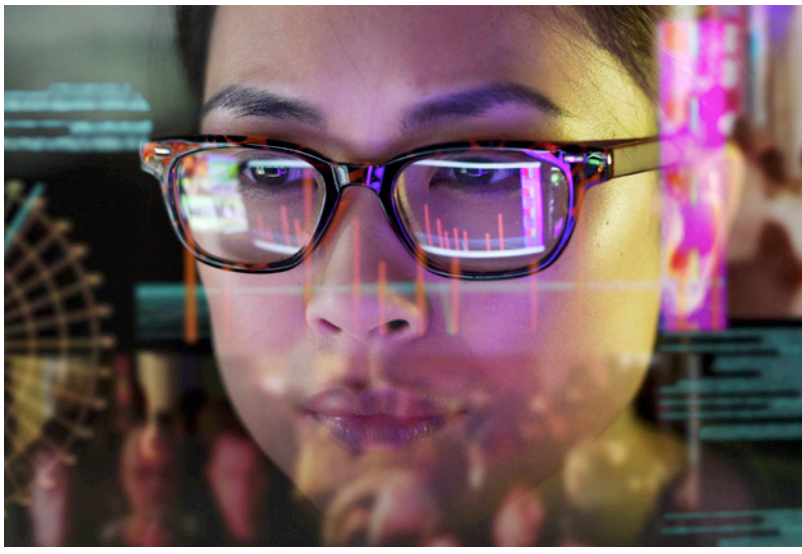
In the IT security infrastructure of a company, potential weaknesses often remain undetected without a consistent basic structure. In case of a problem, there is a lack of clear processes and responsibilities. An information security management system (ISMS) creates the necessary clear basic order and lays the foundation for a comprehensive IT security strategy. CARMAO GmbH has published a guideline on the strategic orientation and introduction of an ISMS. Companies can request this free of charge.

CARMAO experts also provide support in the implementation of specific information security measures, e.g., by providing external information security officers, reviewing IT emergency management, internal audits, preparing for KRITIS audits, resilience assessments, and much more.

Training the workforce as a means of information security

Furthermore, CARMAO GmbH offers training, consulting, and services around the topics of information security, business continuity management, and organizational resilience.

As an authorised Gold Partner of the PECB, CARMAO is continuously expanding its cooperation with PECB for its training and advisory services in order to meet the requirement of a globally educational standard. In this context, CARMAO sees continuous training as an important lever for organizations to implement meaningful corporate resilience with its individual components. The workforce should therefore be sensitised, qualified, and continuously trained for their tasks in areas such as; information security, compliance, business continuity, risk management, and service management.



Sustainability is another premise that is considered in the CARMAO and PECB seminars. This results from the growing need for expert knowledge. With digitalization and globalization, the half-life of learned knowledge and processes is visibly shortening in many sectors, but at the same time other requirements are increasing and changing – e.g. for information security. Corresponding strategies transcend national borders and are often controlled centrally, especially in internationally oriented companies.

The partnership of CARMAO and PECB combines the extensive experience of both companies and offers a new approach to understanding and efficiently eliminating corporate risks. Sustainable management of these risks as well as the continuous building of organizational resilience are elementary, especially to meet the growing requirements through the IT Security Act 2.0.

Ulrich Heun
Founder and Managing Partner
at CARMAO GmbH

in

Ulrich Heun is the founder and managing partner of CARMAO GmbH, founded in 2003, and a proven specialist in the field of organizational resilience. In addition to consulting on topics in the area of information security management systems (ISMS), their extension to data protection (ISO/IEC 27701), risk management, business continuity management (BCM) as well as data protection management and BSI IT-Grundschutz, he focuses on the conceptual development of CARMAO's CHARISMA Resilience Management Framework. In addition, he is active as honorary chairman of the CISO Alliance e.V. Ulrich Heun is a PECB Certified ISO/IEC 27001 Lead Implementer, PECB Certified ISO/IEC 27005 Lead Risk Manager, PECB Certified ISO 22316 Foundation, PECB Certified Cloud Security Manager, and a PECB Certified Trainer

Certified Lead Ethical Hacker Training Course

An ethical hacker has become a must in organizations. Through Ethical Hacking Certification you will obtain the necessary expertise, knowledge, techniques, and methods that will make you an asset to any organization.

PECB offers you the chance of becoming a Certified Lead Ethical Hacker with CLEH training course.

LEARN MORE

Anticipating the Newest Version of ISO/IEC 27002

ISO/IEC 27002 is an information security guideline that intends to help an organization implement, maintain, and improve its information security management. It is the code of practice for information security controls and assists in providing more details for the controls laid out in Annex A of ISO/IEC 27001.

While the updates being made will not directly impact the ISO/IEC 27001:2013 framework, they will give additional context and clarity for those seeking certification in 2022, particularly as it relates to modern data security practices such as cloud security.

The expected changes in this new version will be the introduction of 12 controls, while the existing ones will be regrouped, and the controls of the 2013 version will be reduced to 93 from 114 controls.

PECB is updating the ISO/IEC 27002 training course in accordance with the changes of the standard.

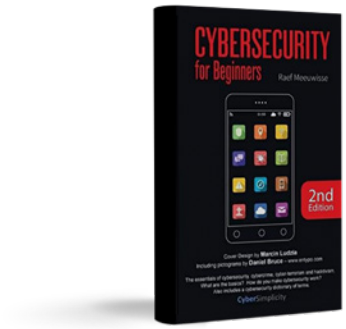
For more information contact us at **marketing@pecb.com**.

Understanding the Digital World

As the technology that surrounds us keeps evolving rapidly, the level of its complexity is increasing as well, leading to potential misuse. Prioritizing data protection is becoming very prominent. Not everyone can study the field and understand all details, however, reading a book to learn portions of it will do us all good, from leaders of organizations to parents.

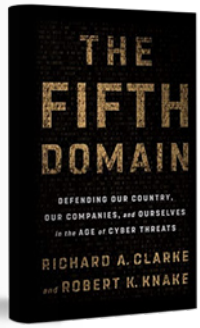
If you are looking to expand your knowledge on topics such as information security or cybersecurity, here is a list of recommendations that not only share information but also help us understand the importance of security in the digital world, filled with data, analysis, and real-life stories.

1. Cybersecurity for Beginners by Raef Meeuwisse



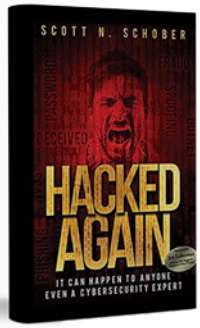
As most business people nowadays share a common interest in learning more about the essentials of cybersecurity, this book will provide you with all the basic information that you need. Simultaneously, being an excellent resource for any information security expert interested in updating their knowledge. To quote the author: “The world has changed more in the past ten years than in any ten year period in human history. Technology is no longer a peripheral servant, it shapes our daily lives. Companies that can use technology wisely and well are thriving, while companies that make bad or no technology choices collapse and disappear. The cloud, smart devices, and the ability to connect almost any object to the internet are an essential landscape to use but are also fraught with new risks and dangers of a magnitude never seen before”. In the rapidly changing cyber world, this book balances complexity on the topic while also including real-life examples to keep the readers intrigued.

2. The Fifth Domain: Defending our Country, Our Companies, and Ourselves in the Age of Cyber Threats by Richard A. Clarke and Robert K. Knake



The Fifth Domain provides an insight into how governments, organizations, and citizens can face hackers keen on manipulating the digital world. Through numerous previous stories of cyber-attack fatalities, it has become evident that cyber threats oppose a real-world consequence, and now with the potential to lead to wars, it makes the importance of action even more prominent. The author dives into some of the most well-covered stories, like the Stuxnet attack, which assisted in slowing Iran's nuclear program, to lesser-known ones like EternalBlue, the cyberattack that closed hospitals in Britain and froze shipping crates in Germany midair in 2017. This book provides intel on making cyberspace safer by defending our security and privacy.

3. Hacked Again by Scott N. Schober



Hacked Again shares the dangers of the digital world through the detailed story of a cybersecurity expert and CEO of a top wireless security tech firm, Scott Schober, the author himself. As a working, family man, and business owner; running a successful security company and reporting the latest cyber breaches in hopes of offering safety tips to millions of viewers. However, when a mysterious hacker starts stealing thousands from his bank account, going through his trash, and taking over his social media personality, Scott stands to lose everything he has. He explains the chaos his life faced after being compromised by multiple cyber-attacks. Through this book, besides sharing his own experience, he shares tips and lessons he learned being on the end of an attack of the sort.

4. The Cyber Effect by Mary Aiken

Technology can be used for good or bad purposes. As an expert in forensic cyberpsychology the author's research interests include cyber security, organized cybercrime, cyberstalking, technology-facilitated human trafficking, and the rights of the child online. Aiken provides surprising statistics and incredible-but-true case studies of hidden trends that are shaping our culture and raising troubling questions about where the digital revolution is taking us. This book raises a lot of conversations on how the Internet is shaping development and behavior, societal norms and values, children, safety, privacy, and our perception of the world.

Top Five High-Paying Job Positions You Can Pursue with an ISO/IEC 27001 Certification

Nowadays, we are seeing that information is being exposed to a variety of risks, as a result of an increasingly interconnected environment. Digital threats such as ransomware and phishing attacks are becoming more common and sophisticated, and this is making the implementation and updating of information security controls and processes a challenge for organizations.

The PECB ISO/IEC 27001 training course has been developed to help you understand the practical approaches involved in the information security management system implementation as well as enable you to identify and effectively treat information security risks. Therefore, obtaining certification against this standard will show that you are driven to acquire and demonstrate the skills and knowledge to support an organization in successfully implementing information security policies and procedures as per the organization's needs.

The information security industry has immense growth in demand, therefore creating an increase in job openings for the upcoming years. Here is a list of the highest-paying jobs in information security.

1. **Chief Information Security Officer**

According to PayScale, Glassdoor, and ZipRecruiter, the average salary of a chief information security officer (CISO) is $166,456 per year.

2. **IT Security Architect**

According to PayScale, Glassdoor, and ZipRecruiter, the average salary of an IT security architect is $138,138 per year.

3. **IT Security Consultant**

According to PayScale, Glassdoor, and ZipRecruiter, the average salary of an IT security consultant is $99,317 per year.

4. Security Director

According to PayScale, Glassdoor, and ZipRecruiter, the average salary of a security director is $94,734 per year.

5. Information Security Specialist

According to PayScale, Glassdoor, and ZipRecruiter, the average salary of an information security specialist is $93,557 per year.

The ISO/IEC 27001 family such as ISO/IEC 27005, ISO/IEC 27032, Cloud Security, etc., assists you in understanding the practical approaches that are involved in the implementation of an information security management system (ISMS) that preserves confidentiality, integrity, and availability of information.

Due to this, the ISO/IEC 27001 family of standards can provide a wide range of career opportunities to those who are interested in protecting their organizations from various malicious attacks, especially in the current world of sophisticated attacks and hackers.

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

CLICK HERE TO SEE HOW PECB CAN HELP

CMMC 2.0: What is It and Why the Change Was Enacted Now

BY LEIGHTON JOHNSON

On November 4, 2021, the Department of Defense (DoD) introduced the new, revised version of the Cybersecurity Maturity Model Certification (CMMC) for their 300,000+ supply chain contractor organizations. This new version development effort, which started in March 2021, was the culmination of DoD's program review of the CMMC endeavor enacted by the new US Administration after the November 2020 election. There was a series of comment submittals, advisory papers, suggestions, and general advice delivered to DoD on CMMC over the previous year by a wide range of organizations, corporations, panels, and groups; all suggesting different changes needed for CMMC. These suggestions ranged from stopping this effort altogether as a "waste of money", to minor alterations of the program. DoD has a long history of enacting program reviews over the past 30 years, surrounding large military weapons and administrative programs. Therefore, to me, the change action was not a new or unusual activity.

CMMC 2.0 introduced several major adjustments to the original CMMC Model. These changes included:

a. Changing the Level from 5 down to 3, with Level 1 unchanged, the new Level 2 being equivalent to the old Level 3 and the new Level 3 being equivalent to the old Level 5

b. Removing the ban on POAM's (Plans of Action and Milestones) for Level 1 and some of Level 2 requirements

c. Changing Level 1 to a self-attestation effort on the part of the contractor organizations from the original requirement of needing to be a third-party assessed by designated assessment organizations.

d. Adjusting the less critical controls in Level 2 to also being self-attested by the contractor organizations

DoD reverted back to the US Government's standard for managing Controlled Unclassified Information (CUI), the NIST Special Publication 800-171, as the sole authoritative source for defining what security controls are needed to manage the contractor's efforts and systems.

DoD removed the extra areas they had added to CMMC 1.0, concerning availability and asset management with the new CMMC 2.0. Listed below are these changes and what they mean to the DoD Industrial Base (DIB) contractors.

1. The first change reduces the areas of focus to more manageable 3 levels. Level 1 is based on organizations self-reviews and self-assessments. DoD has already produced the Level 1 self-assessment guide for organizations to use in reviewing the 17 controls needed for Level 1 attainment.

   Level 2 is the full 110 controls implemented from SP 800-171 into the contractor environment for processing, storage, and transmission of CUI within their environment. This covers 14 areas of concern, such as; Access Control, Incident Response, Information Integrity and Media Protection among others, and is split into 2 approaches for review. The initial approach is for non-critical areas and allows the organization to self-attest to compliance. The second approach is for more critical systems and data which requires the C3PAO (Certified Third-Party Assessment Organization) assessors to conduct the organization's independent assessment. Determining the approach that will be used is based upon the CUI's involved and the critical nature of the contract to be supported and will be made, at least initially, by the DOD Contracting Officer, not the Organization Seeking Certification (OSC).

   Level 3 is for contractor organizations and systems with the most important and critical data to be handled by the organization. This level will focus on the advanced need for security and will be reviewed and assessed by a governmental agency only.

2. The second change is related to Plans of Action and Milestones, otherwise known as POAMs. POAMs are items that are not currently at their needed level of application but necessary to protect the CUI data and security components that enable or deliver the protection. The original CMMC Model did not allow POAMs to be active at the time of assessment; they were to be completed and installed. However, the change to CMMC 2.0 has now provided the organization to have POAMs on items deemed to be non-critical. This is currently to be determined by the assessor and the DoD, not the organization under review. This allows for organizations to budget and plan for future installations of security capabilities and equipment, rather than having to "spend the money" upfront to prepare for their CMMC Level assessment.

3. The third change is that Level 1 reviews are now based on corporate self-reviews and self-assessments. DoD has already produced the Level 1 self-assessment guide for organizations to use in reviewing the 17 controls needed for Level 1 attainment. These controls, such as requiring user IDs and passwords for each account, are basics for security in all organizations and are easy to reach compliance with organizations. The caveat with this change is the official self-attestation of compliance, Level 1 will be required to be submitted and signed by a corporate officer of the organization. Therefore, enforcement, which is available under the US False Claims Act legal criteria, will be implemented. In fact, the US Dept. of Justice has already created a special Task Force, including members from DoD and DHS as well as other federal agencies, to focus on False Claims Act violations of federal contractors.

4. The fourth change is the bifurcation of Level 2 assessment efforts. The non-critical Level 2 controls and practices will be allowed to be self-assessed by the organizations, under MMC 2.0. The selection of which ones are non-critical is up to DoD, not the organization itself. The rest of the practices and controls will require a C3PAO-based assessment to be performed by a Certified Assessor and Assessment Team with an independent report produced which defines which requirements are met and which areas are not, in accordance with CMMC Level 2 Assessment Guide and NIST SP 800-171A guidance. It is currently estimated that the number of organizations that will require C3PAO assessments has been reduced by this one change from 300,000+ down to 70,000-100,000. But this will require all organizations desiring to attain Level 3 certification to accomplish this Level 2 C3PAO assessment first before the DoD assessment team conducts their Level 3 assessment; which is the projected way this is to be completed as of now.

What do the above-mentioned CMMC changes mean to the average DoD contractor?

First, more time is now available for organizations to get ready for their assessment so they can win DoD-based contracts in the future. We will see as information is released by DoD on the actual timelines needed to complete these efforts. Second, the full DIB contractor base, worldwide, is still affected by this change, so that area has not changed. It has been estimated that 10-15% of the DIB is based outside the US.

Third, smaller contractor companies and organizations will have an easier path to Level 1 achievement, thereby resulting in less expense and manpower needed to accomplish this level of corporate certification.

Fourth, CMMC is still moving forward with DoD's desire to manage its supply chain risks, which is what CMMC is about to start with.

in

Leighton Johnson
CTO of ISFMT (Information Security Forensics Management Team)

Leighton Johnson, the CTO of ISFMT (Information Security Forensics Management Team), a provider of cybersecurity & forensics consulting and certification training, is a CMMC Provisional Assessor and Provisional Instructor (#0026) within the CMMC Ecosystem. He has over 40 years of experience in Computer Security, Cyber Security, Software Development, and Communications Equipment Operations & Maintenance; Primary focus areas include computer security, information operations & assurance, incident response & forensics investigations, cybersecurity testing of systems, systems engineering and integration activities, database administration, and cyber defense activities. He founded and leads two cybersecurity assessment/audit companies and is a principal in two other cybersecurity companies.

The GDPR – Certified Data Protection Officer (CDPO) Training Course Is Now Available in French!

Expand your horizons with this excellent opportunity to get your certification in GDPR – Certified Data Protection Officer (CPDO), all from the comfort of your home through eLearning.

To learn more on our training courses, please contact us at: marketing@pecb.com.

PECB eLearning

Differentiating Between CMMC 1.0 and CMMC 2.0

BY GEORGE USI

"If you see hackers, you see Usi," someone once suggested I use this line to introduce myself. Perhaps they presumed that people who do not know me would easily remember how to pronounce my name and possibly remember who I am.

Throughout my life; teachers, teammates, college professors, coworkers, and leaders frequently mentioned that my name was confusing to pronounce. For years I rarely put thought into why, until I started my career building internet backbones in a world of tech acronyms.

A colleague of mine once said: "You are lucky. The spelling of your name is easy to remember because it has three letters, much like many of the acronyms in the tech world", he further posited: "things in threes are way easier to remember."

So, now that my name is embedded in your memory, I am encouraged, delighted, and relieved that the CMMC 2.0 changes included a simplification from five levels to three. I also strongly believe that the psychology associated with "The Magic of Threes" benefits the new tiering model as I strongly believe non-technical leaders can easily understand anything in threes. In the spirit of the glass being half-full, I confidently propose that we should celebrate the new CMMC 2.0 in spite of the aches, pains, and grumblings in arrears of the change.

Benevolently, in the spirit of simplified reading of my article, I tried to organize my writing in threes as well.

The Good, The Bad, and The Unpleasant of CMMC 1.0, 1.0 Challenges, and 2.0 Justification

CMMC 2.0, now a 3-Level model, was redesigned and released late last year to what we might suggest as the "raised eyebrows" of about 2,000 registered practitioners, more than 100,000 Defense Industrial Base Companies and their base of sub-contractors, and a frustrated supply chain of vendors who invested into CMMC due to cascading requirements originating out primes or DIB Companies cascading down CMMC 1.0 to them.

Notably, the veterans who work for Omnistruct often described the hard deadlines for ML3 in the midst of a pandemic for the entire ecosystem as "untenable."

First, we want to cover the "why, what, and how" of CMMC 1.0 – The Good

- Why – Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) must be Safeguarded
- What – Setting an enforceable standard for cybersecurity regulatory, policy, and contracting for Department of Defense (DoD) Industrial Base Companies using an acquisition strategy
- How – Using the tiered CMMC model implemented through Federal contracts that can be audited by certified assessors trained and accredited by a governing body (CMMC-AB)

Second, CMMC 1.0 Major Problems – The Bad

- Why – CMMC 1.0 was a slog, complicated, and is exacerbated by the pandemic
- What – Scaling back the program was needed to go fast
- How – Foretelling contractual data classifications caused confusion of CMMC maturity level preparation

Third, let us cover the CMMC 1.0 change justification to CMMC 2.0 – The Unpleasant

- Why – CMMC 1.0 assessment system had issues, DIB and CMMC-AB progress overall was off schedule, and small businesses were hurting from the intensive resource load of CMMC compliance
- What – The five-tier levels and assessment system need streamlining, POA&Ms need allowances, and small businesses compliance needs to be affordable and reasonable
- How – Levels 2 and 4 were removed for simplification, POA&Ms were allowed, and self-assessment qualifications were expanded for small businesses with enhanced assessment ecosystem oversight

Why CMMC 2.0 Is the Right Direction

Simplification of Tiers

CMMC 1.0 was designed with the right intent and mindset but as most v1.0 of just about any launch, everyone discovered that it lacked practicality. After a number of engagements, the confusion on timelines, scopes, and the assessment ecosystem was creating more questions instead of answering them.

The original five-tier system had many of our practitioners looking at Level 2 as transient and needless. The virtual watercooler chats in our engineering channels frequently included comments about why Level 2 exists when Level 1 and Level 3 seemed to cover what reasonably mattered.

Additionally, Level 4 seemed like it was suffering from an identity crisis, in that many of our Practitioners and Customers were questioning if the mystery box that was Level 4 had been added simply to make sure there were a total of five levels (the second most appealing odd number behind 3), instead of the esthetically unappealing four.

With CMMC 2.0 now scaled back to three levels and the numbering system deemphasized by the newly rebranded descriptors of "Foundational (old Level 1), Advanced (old Level 3 now aligned to NIST 800-171), and Expert (old Level 5 now based on NIST 800-172)," the magic of threes now presides. Notably, even the audits are triennial!

Sadly, the satisfaction of threes ended when the assessment ecosystem split the "Advanced (the new Level 3)" assessment in two with an annual self-assessment for most entities and a triennial audit for DIB Companies stewarding critical national security information. We have some opinions on this, that we will voice in our conclusion as I imagine this decision will be a curveball of confusion for many.

Streamlined So We All Go Faster

We already know that hackers are winning the ground war of cybersecurity, especially when bad cyber hygiene practices prevail and cyber posture is poor. Considering the pace of the CMMC 1.0 progress amongst the DIB was slow, coupled with the CMMC-AB assessment ecosystem crawling along, a "Keep It Simple Simon" (KISS) streamlining approach was needed for the CMMC 2.0 update.

We all like to make wise investments and the allowance of a POA&M to make a plan that improves cyber posture reasonably over time is welcome. Practitioners and experienced DIB Companies can also benefit from an already familiar process and framework on a committed schedule with predictable budgets. The concession is that we will have to give up ground grudgingly to hackers who attack DIB Company gaps outlined as less critical. Through POA&M allowances and NIST 800-171 guardrails at the Foundational and Advanced levels, the DIB Companies can have a long-term acquisition strategy that spreads out and prioritizes the financial burden of compliance over time.

Our team of RPs and CPs were fully expecting an increased oversight of the assessment ecosystem in version 2.0. All of them were relieved by how the change commits to increased oversight of professional and ethical standards. Some of our key leaders of CMMC practitioners also recognized that self-attestation expansion will produce an immediate reduction in the sheer number of companies that need to be audited which allows everyone to go faster in patching the critical gaps.

Small Business Have Better Footing to Compete

Anyone who has been in Federal or SLED markets will recognize that leveraged procurement prerequisites like CMMC are incredibly time consuming and difficult for small business to integrate. The difficulty is at its highest when the "price ticket to entry" originates out of tiering systems where larger competitors often achieve the highest level of attainment in procurement compliance as a competitive edge, and especially when cash poor small business competitors can be easily eliminated.

These tactics tend to rule out small businesses that were unable to afford equivalent compliance status to meet a contract requirement at even the lowest level of CMMC.

Since the CMMC 2.0 allowed and expanded self-attestation for the first two levels, small businesses can breathe a small sigh of relief that realigns and expands the contracts they will be able to bid on, without requiring an auditor.

How Else Can CMMC Improve and Simplify?

The use of NIST CSF & NIST PF for Service Providers of DIB Companies. One of my Stanford professors once lectured that scaling up requires rigid and malleable methods. Rigid methods require rules and processes that are prescriptive when things are repeatable, methodical, and predictable so you can build operational flywheels and produce quickly. Alternatively, malleable methods suggest the use of guardrails for business situations that are unpredictable or less frequent. NIST 800-171 is rigid and more prescriptive whereas NIST CSF is malleable and entrenched with guidelines (like guardrails).

They may also offer a path to micro-business served dominantly by service providers allowing for CMMC attestation at scale, if delivered and regulated through an attestor service or the service providers of DIB Companies themselves.

Moreover, with over three million small businesses hiring outsourced IT and security help (MSP or MSSP), regulation in the MSP markets with NIST CSF and NIST PF as a standard could be an alternative to NIST 800-171 for micro-businesses and subcontractors of DIB Companies. We must concede that for this to work effectively, either a regulatory body or third-party administrator of cyber risk from the private sector would have to evolve so they could be utilized to audit and attest the DIB Company's Service Provider.

Impartially, the NIST CSF and NIST PF are volunteer and guideline focused and although the use of such a framework in a security program can be easily cross walked to the NIST 800-171, privacy laws that offer safe harbor to businesses who use NIST PF, would be highly suggested, regardless of your CMMC level.

Third-Party Administrator for Cyber Risk

The CMMC-AB has proven that we have room to grow in auditing, attesting, and accreditation oversight. The assessment split of "new level 2" into two paths of conditional self-assessment vs triennial audit might benefit from a new idea. As a TPA that administers 401(k)s, perhaps the CMMC-AB could mimic that concept by leaning on the existing base of RPOs and C3PAOs to be dedicated cyber risk administrators (a new "cyber TPA" market)? These cyber TPAs could be a requirement for all self-assessment conditions and have the potential to cascade to NIST CSF and NIST PF framework administration at scale. I would also suggest that these third-party administrators would be barred from selling security tools and services as part of their CMMC pledge. Granted, we think many professionals have recognized that hiring the same company who sold and integrated your tooling to conduct your audit and attestation could be easily called out as "the fox guarding the henhouse."

Additional consideration of this option will be needed collaboratively as we imagine that if a hacker succeeds and an investigation is required, it may look a lot like a student grading their own final exam.

Concluding Point of View

CMMC's vision and mission must continue. Please recognize with a sense of urgency that threat actors are attacking at a much faster pace and level of sophistication every day. Your investment in CMMC has a critical level of priority that requires dedication, experience, and perseverance to stay the course in your strategy and in the protection of our Defense Industrial Base.

Advanced Persistent Threat (APTs) actors understand that a blitz against the weak is most effective. Therefore, DIB Companies need to invest in a cyber "air war" strategy of frameworks, governance, and reasonable controls that reduce cyber risk effectively. They must also include a core framework like ISO/IEC 27001 (rigid) or NIST CSF (malleable) that can crosswalk/map to NIST 800-171 prescriptive controls. The US market certainly favors the "reasonable"

concept of over-prescriptive controls as do the attorneys that represent and defend them.

In our opinion, the CMMC 2.0 changes seem like a step back. However, the CMMC will continue to morph, adapt, and improve. We are hopeful future changes will include an alternative to the self-attestation approach of DFARS 7012 which had a poor track record. Admittedly, we believe California, Colorado, and Virginia comprehensive data privacy laws reflect the inevitability of a federal privacy law that will cascade down the self-attesters. We will be watching for overlaps and gaps between CMMC and privacy laws with our network of data privacy attorneys and cyber insurance providers.

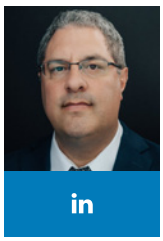
Also, recognizing that data converted by CMMC is not the same as other privacy data. We must also realize that consumer data we collect, process, or have proximal access to, is also sacred and considered privacy data. I am personally hopeful we all understand that privacy-relevant security incidents are now litigious with sanctions that will make a lost contract look like pocket change.

Poignantly, with new privacy laws popping up globally and with at least three US states (Connecticut, Ohio, and Utah) leaning into NIST CSF and NIST PF as a safe harbor option for businesses that use them, we suggest you avoid getting stuck in the mindset that CMMC will address all other requirements in privacy data protection.

Notably, every business will eventually have regulatory, contractual, and statutory requirements they must meet with pending consumer data-privacy legislation focused on holding business leaders personally accountable when they fail to keep sensitive data sacred. We are all subject to the looming checklists, regulations, and statutory requirements in this chaotic internet-delivered world we live and do business in.

Finally, CMMC was and still is, always about the need for investment to secure sensitive data from cyber threats. Your approach will require both the right mindset and footprint in approach and strategy. Also, adapting to NIST 800-171 for CMMC should be done with other regulatory and statutory requirements in mind. The train of cyber risk is coming and if you are working on the CMMC tracks, you just might be standing on the high-speed rail tracks of California's CCPA/CPRA!

Omnistruct focuses on transferring cyber risk from service providers, and their customers, who are grappling to adopt security programs, privacy programs, and other demonstrable cyber posture illustrations so they can earn and retain business in an increasingly cyber-aware supply chain. If you are grappling with CMMC 2.0, FedRAMP, NIST SP 800-171, NIST SP 800-53, you are not alone and might need some guidance. Call us at 916.484.1111 or email sales@omnistruct.com



George Usi
CEO of Omnistruct

George is CEO of Omnistruct Inc a SaaS-based cyber risk company.

George also co-chairs the California IPv6 Task Force, a not-for-profit IPv6 scientific advocacy group, and is also a Board Member of Secure The Village. Finally, George ideated and contributed to the first IPv6 interoperable network for first responders, Metronet6, with mentorship from HP Fellow Jim Bound†, Dr Vint Cerf, and HP Fellow Yanick Pouffary for which he was awarded the 2007 Internet Pioneer Award.

George is a graduate of CSU Sacramento and the Stanford Latino Entrepreneurship Initiative GSB Certificate Program by LBAN.

International Day of Education

24 January

Education and knowledge are the fundamental b

Now, with education being easier to access throug
a great opportunity for anyone to get started with
academics offered at PECB University creates an
aspirations. We are delighted that the enrollment
University wishes you a happy International day o

REGISTER HERE!

bases of paving the path to success.

gh the comfort of your own home, it has been
their educational journey. The multitude of
accommodating environment for all your
numbers keep increasing, in light of that, PECB
f education.

ENRICH YOUR ABILITIES, FOR BETTER OPPORTUNITIES

Make the most of PECB's new training course! Contact us at marketing@pecb.com or visit our website for more.

Training Course	Language	Status	
Certified Lead Ethical Hacker (CLEH)	French	NEW	→

YOUR GATEWAY TO SUCCESS

Find all the materials and tools you need to pave your path to development and success at your fingertips, through the PECB Store.

Here are some recommendations to get you started:

- ISO/IEC 27032:2012 Standard
- ISO/IEC 27001:2013 Standard
- ISO/IEC 27005:2018 Standard
- ISO/IEC 27002:2013 Standard
- ISO/IEC 27701 Toolkit

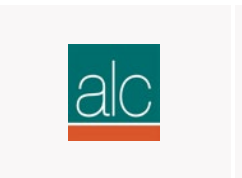
SHOP NOW! ▶

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.

MAKE YOUR CYBERSPACE SAFE!

Learn and get certified through our **CMMC** and **Cybersecurity** training courses!