PECB Insights

ISSUE 34 ISO STANDARDS AND BEYOND SEPTEMBER-OCTOBER 2021

ETHICAL HACKERS

THE ULTIMATE SOLUTION TO CYBERCRIME

PECB Insights Magazine

delivered to your mailbox

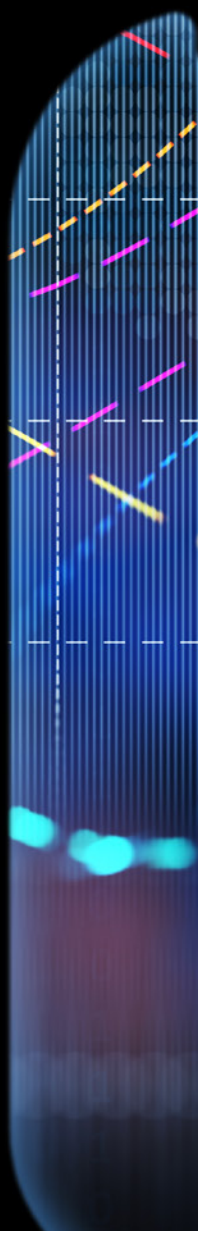
Subscribe & find out more at

www.insights.pecb.com

In This Issue

"You can never protect yourself 100%. What you do is protect yourself as much as possible and mitigate risk to an acceptable degree. You can never remove all risk."

KEVIN MITNICK
The World's Most Famous Hacker , CEO at Mitnick Security Consulting , Author and Professional Speaker



Ethical Hackers: Protecting Organizations and Fighting Cybercrime

BY NIKHIL AGARWAL


SECURITY

Hacking is a very powerful skill that continually advances and gains popularity. Cyberattacks are among an organization's most feared threats. One of the best forms of tackling this threat is hiring an ethical hacker to perform a penetration test and look for vulnerabilities using the methods of a hacker. The ethical hacker's report allows organizations to upgrade their systems and take preventive measures to avoid incidents. In many ways, an ethical hacker is similar to a secret shopper who goes into stores in the dark to look for flaws and provide suggestions for changes. Secret shoppers may also report shoplifting events to assess a store's security.

Likewise, ethical hackers — who use similar methods as cybercriminals — can help organizations find flaws, strengthen their networks, and improve their techniques.

A rushed digital transformation era and ethical hacking

Digital transformation accelerated drastically with the outbreak of the Covid-19 pandemic. Lockdowns have forced many organizations to switch to working remotely, with many of them going remote permanently. Yet, working remotely has one key challenge: home offices are not as secure as office sites. This created more opportunities for hackers to compromise organizational devices and networks. Organizations worldwide have increased their budget and resources to protect their systems and information from hackers. Most nations have powerful security laws and cybersecurity departments working inseparably with local law regulatory authorities to catch cybercriminals. To increase the awareness about security in the digital workspace, Cyber Security Awareness Month is organized in October by a community-led effort between governments and industries to uncover issues related to the importance of cyber security on the Internet.

The increase in cyber-attacks has led more organizations to recognize the need for new and more creative ways of addressing hacking problems. This gave birth to ethical hacking (also known as white hat hacking), an important and handsomely rewarding position. Ethical hackers try to gain access to an organization's most sensitive information and systems. They report to the organization of their weak points and provide suggestions for improvement. To do so, they must be very professional and adequately qualified.

Organizations should be able to analyze and prioritize their systems and information in terms of their importance and likeliness to be attacked and compromised in case of hacks. This is essential in order to maximize the benefits of their cooperation with an ethical hacker.

Unlikely heroes

Ethical hackers have become the unlikely heroes in the fight against cybercrime. They find and neutralize risks and weaknesses before they are undermined exploited by people with malicious intent. The difference between ethical and criminal hacking is that the first is conducted only with the consent of the target and for improvement purposes. Ethical hacking is very efficient because it uses the methodology of a hacker to discover vulnerabilities that may go unnoticed. Information is one of the most valuable elements of the digital world. Even the world's largest and sophisticated organizations have fallen victim to cyberattacks. As more and more organizations move their business in the virtual world, the risk security breach is almost unavoidable. A data breach can cause damage reputation, customers trust, and future business opportunities. The sublime landscape in this way critically directs the demand for a true and comprehensive assessment of an association's security practices.

Adopting a proactive security strategy can help organizations protect their data and capital. Ethical hackers offer an outsider and professional perspective on an organization's weaknesses. Even organizations that employ an internal red team can occasionally hire an external ethical hacker to gain a new perspective on their defense systems.

Other benefits of hiring an ethical hacker include building customer trust by communicating the process to customers and demonstrating compliance with regulatory guidelines, including PCI and GDPR. Of course, even the work of the most talented ethical hacker is in vain if the organization fails to effectively respond to the detected problems.

What's left?

According to a study by McKinsey & Company, digital transformation progressed by up to seven years ahead of schedule in 2020. Threat actors and cyber thieves, on the other hand, modified their strategies to take advantage of these shifts and the pandemic's disruption, resulting in an increase in attacks across all industries.

As the world keeps going digital, conventional crime is also being replaced with cybercrime. In 2021, criminal hacking groups are allegedly using machine learning on the dark web and dark web forums, making their phishing operations more sophisticated.

Cybercriminals also receive compensation in cryptocurrency, which is harder to track and has become a business motive for many criminal companies since their introduction to ransomware. This, in turn, makes ransomware a more important tool in their exploit toolkits.

In this digital era, every organization should employ ethical hacking in its system to safeguard their online presence, because data breaches significantly harm any organization's reputation, and can even be the cause to legal and regulatory fines.

Ethical hackers are pushed by law to highlight any security issues they identify during their tasks, as this is confidential information that might be exploited by criminals. Overall, the skills of an ethical hacker, combined with other great security measures like multi-factor authentication, access control, and data encryption, can significantly improve corporate defense systems.

Nikhil Agarwal
Cybersecurity Evangelist | Trainer | Public Speaker

Nikhil is an innovative information security leader and evangelist, currently working as Senior Manager - Cyber Cloud, Risk Advisory with Deloitte Singapore. He leads large-scale cloud security and digital transformation programs.

He is ranked 18th in Cyber Security, 10th in Emerging Technologies & 3rd in Cloud Security in the Consultancy Industry, amongst the top 25 consulting leaders by Onalytica, analyzing the top 48 Consultancies globally.

Nikhil has evaluated, architected, and led teams to implement security-focused tools and services for cloud, containers, and CICD pipelines, covering application and platform security, orchestrating security controls and integrating them with security operations, and identity and access management (IAM) solutions. He is an expert in both traditional cybersecurity practices, such as penetration testing, devsecops, cloud security, container and Kubernetes security, architecture review, cyber forensics etc., and Next-Gen cyber security practices, like red teaming, shadow IT, cyber threat intelligence (CTI), darknet monitoring etc.

As a noted technology expert, Nikhil has worked across cultures and serving clients globally while working in Europe (Germany), Africa, MEA, and APAC countries in various industries.

Website – www.reachtonikhil.com

2021 IT Training Watch List Company by Training Industry

We are proud to announce that PECB has been selected as the 2021 IT Training Watch List Company!

This title is awarded by **Training Industry**, the most reliable source of information in the professional education. It is given to companies with emerging or unique strengths or capabilities.

We thank our customers and partners for their support and loyalty over the years. Achievements like this inspire us to keep providing high-quality training courses.

FIND OUT MORE ▶

Creating Opportunities from a Crisis

Guidance on building back better when disaster strikes.

When COVID-19 struck the world, it was a huge surprise for many, exposing fragilities in systems and organizations everywhere. Those that were prepared for the unexpected, however, generally fared better. Taking lessons learned from the pandemic and international expertise, ISO/TS 22393, Security and resilience – Community resilience – Guidelines for planning recovery and renewal, has just been published.

The technical specification provides guidelines on how to develop recovery plans and renewal strategies from a major emergency, disaster or crisis, such as the COVID-19 pandemic. It includes how to identify the short-term transactional activities needed to reflect and learn, review elements of the system impacted by the crisis and reinstate operations.

Duncan Shaw, Project Leader of the group of experts that developed the document, said that when any crisis occurs, most organizations just want to get back to normal as quickly as possible. But in doing so, they could miss valuable opportunities.

“Major disruptions can be a catalyst to address some significant underlying issues and make important strategic changes,” he said.

“Recovery is just the beginning. Renewal is where relationships are built, shortcomings and vulnerabilities are addressed, and inequalities are remedied. It’s about reshaping operations to build resilience over the long term.”

Duncan added that work on the guidelines began in the early months of the pandemic, and its development involved dozens of interviews and discussions with experts and various stakeholders from all over the world. The result is international best practice drawing on real-world experiences that aims to support local and national organizations as they deal with COVID-19, and beyond.

“It will encourage an important change in mindset from just “recovery” to “recovery and renewal”, which will serve to enhance resilience in the communities where it is used.”


PARK

Legal Hacking and Data Protection

MOJISOLA ABI SOWEMIMO

Data protection involves procedures and processes developed and implemented to protect personal data in a computer system or network. It involves protecting data from loss through several ways, including backup and recovery.

Data security is the practice of protecting data, and there are several methods adopted to protect data against corruption, loss, and compromise. Different tools can be used to enforce data security, some of which are data protection laws and frameworks.

Data protection laws help to ensure that data is used correctly and legally by authorized users. Having a robust data protection/privacy program helps build trust with organizations and customers, which translates to customer loyalty and increased profit.

Consumers are getting more aware of where their data is stored and how secure it is with merchants.

Legal hacking, also known as ethical hacking, involves breaking into computers and devices mainly to test or access the set defenses. The goals and scope of the legal hacking will be set before the hacking.

It enables organizations to identify vulnerabilities and improve or develop technology to reduce, mitigate, or resolve risk.

This article will further explain the relationship between data protection and legal hacking. As you read further, you will also get answers to questions like:

- What do data protection guidelines do to ensure an effective data protection program?
- How can data protection prevent illegal hacking?
- Are there security controls for data that organizations should comply with?
- Can legal hacking be used to protect data – and how?

The evolution of data

The evolution of the internet and international trading has enabled faster and easier transfer of personal data across organizations, countries, and continents. The increase in the dissemination of data has led to a need to protect personal data from falling into the hands of malicious attackers. This has led to the creation of data protection laws and binding frameworks.

Data is a valuable asset irrespective of who has access to it, i.e. authorized and unauthorized users. Data breaches come at a very expensive cost to organizations, leading to reputational damage, legal action, downtime, and reduction in customer loyalty and patronage. There is no limit to the effect of a data breach on affected individuals, some of which are humiliation, financial loss, physical or psychological damage, or threat to life. Data privacy is a fundamental human right for data subjects (owners of data), while it is a legal and moral obligation of organizations to their customers.

What is personal data?

Personal data is any information that can be used to identify an individual. This includes some types of personal data that are deemed sensitive. Some examples of this include a data subject's health history, sexual orientation, and race. This type of data can be used to exploit, profile and discriminate against individuals. It is the most sought type of data for enterprises and people with malicious intents.

Who is at risk?

Everyone and all organizations are at risk. Having a smartwatch, Facebook profile, Instagram, and LinkedIn profile indicates that your personal information is being shared online and offline. Identifying specific platforms on which your data is shared can be difficult to trace. This makes it essential for organizations to ensure that there is a robust data protection/privacy program in place to protect customers' data.

What is a data breach?

A data breach is deemed to have occurred when there is a security violation leading to confidential, sensitive, or protected data being exposed to an unauthorized person. It indicates that there is a loss of control of a computer system or network as a result of a cyberattack which usually leads to fines.

According to IBM, the global average cost of a data breach for 2021 is $4.24 million, making it the highest average total cost in the 17-year history of this report.

Data protection threats

Cyberattack is one of the threats to data, and there are different types of it. A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. A cyberattack is also theft, exposure, alteration, and destruction of data through unauthorized access.

Data protection laws

There are data protection laws and binding frameworks developed that help to ensure that data is protected. These laws help secure data while ensuring its availability for business purposes without compromising the data subject's privacy.

The EU GDPR is Europe's data privacy and security law with requirements for organizations around the world. The GDPR imposes laws on organizations that target or collect data related to people in the E.U. Different countries have different data protection laws, which is essential with privacy and security regulations, constantly evolving to match up with evolving data risks.

Since data is highly sought after, there must be adequate security from the inception of the collection of data. The GDPR has a framework that can be used to ensure that data is protected from compromise, and if compromised, has little impact.

One of such frameworks is the data protection principle, which is:

1. Lawfulness, fairness, and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability

This guide ensures that when data is collected, it is limited and specific to the purpose of collection. Applying this will also ensure that there is a solid foundation for data protection measures.

How can data protection prevent illegal hacking?

We talked earlier about the data protection principles that help provide a solid foundation for data collection. After collecting data, the next question that comes to mind is how we can protect data that has been collected.

GDPR recommends that there should be a risk assessment for data collected. This is essential for identifying the right security to protect personal data.

It also recommends that technical and organizational measures be taken as well.

In order to ensure that the appropriate security is in place for data, the following should be considered:

1. Nature of data
2. Context of data
3. Purpose of data
4. Scope of data

These questions should be answered for all types of data collected by organizations. A risk assessment may be required to be able to answer these questions. Identification of the appropriate security measure for protecting data will be a decision made by the information security, data protection team, and other relevant stakeholders.

Security controls for data that organizations should comply with

Having an effective data security program does not end with designing and implementing one but also with having controls in place to ensure its effectiveness. Notable security control attributes are:

- Confidentiality: Data is available on a need to know basis
- Integrity: Data is complete and accurate
- Availability: Data should be accessible when needed
- Resilience: Data can withstand and recover from errors or threats

These attributes, when implemented, guide towards ensuring that an organization's data security is robust and controls are in place to ensure data security in place protect data from unauthorized access, compromise, and illegal hacking.

Legal hacking

At first thought, the term 'hacker' or 'hacking' connotes a wrongful act punishable by law. This, however, is not always the case.

A hacker is a person that uses technical knowledge to achieve a goal. With reference to data security, a hacker is someone that uses computer programming skills to disrupt computer security in a controlled environment.

There are different types of hacking, such as illegal hackers whose sole aim is to act maliciously, steal, exploit and sell data. They access data unauthorized.

The other type of hacker is the legal hacker (also called an ethical hacker) who works to keep data safe from other hackers, by finding vulnerabilities in the system. A legal hacker works with the system owner's consent and reports on findings to the system owner. A legal hacker accesses data authorized.

Benefits of Legal Hacking:

- Improvements to law and legal policies
- Improvements to technology

How legal hacking can help protect data

Legal hacking identifies existing threats to data and areas within an organization's system or network that illegal hackers can exploit. Legal hackers submit their findings to system owners and also identify how threats can be resolved or mitigated.

Legal hackers hold conferences, workshops and create opportunities to train and educate legal and other non – IT professionals to provide them with a different perspective to address policy issues around data protection laws and legal services delivery. The findings of legal hackers also help to develop legal policies. That can help implement laws that will protect data subjects and also make illegal hackers accountable.

Legal hacking is a form of risk assessment, recommended to be a continuous exercise.

By virtue of this description, legal hacking is a form or tool of data security as the findings of a legal hacker can be used to develop and also improve established security for data protection, eliminate vulnerabilities, and improve security measures and control, which will lead to tightened technological security and effective data protection.

This analogy clarifies that legal hacking is a method of identifying risk, and identifying risk for adequate remediation is one of the goals of data security and data security is a practice of data protection.

Mojisola Abi Sowemimo
Data Privacy Professional

Mojisola is a Data Privacy Professional trained by Kazient Privacy Experts, a global leading firm in the Privacy Industry. She is a Certified Privacy Professional and passionate about helping businesses to uphold the trust given to them when individuals hand over their personal data. Mojisola utilizes her 15+ years of experience to optimize business processes and manage change effectively to help them comply with international privacy legislation. She helps organizations to protect their reputation and most valuable assets whilst inspiring confidence, cultivating trust, and maximizing income.

PECB Certified Lead Ethical Hacker Training Course

Ethical hacking is the best and most efficient way to find system weaknesses and implementing preventative measures.

PECB offers you the opportunity to become a Certified Lead Ethical Hacker with the new CLEH training course.

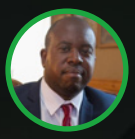
See what experts and trainers say about PECB's CLEH training course:

With cyber threats becoming more and more present and sophisticated, penetration testing is a must to prevent attacks. PECB, through the CLEH course, offers an opportunity to all those who want to be part of the battalions of testers in order to prevent attacks on companies. The CLEH offers content that combines both operational and management, which allows having competent intrusion testers to guarantee the security of companies. I learned a lot from the PECB CLEH course.

Savadogo Yassia, Head of Cybersecurity Department, ARCEP, Burkina Faso

I was fortunate to enroll in the new PECB ethical hacking training course. It helped me to revise some penetration testing techniques as well as to learn many others. The CLEH course will help cyber enthusiasts dive into the world of ethical hacking. It is also an opportunity for businesses to know the threats they face and their weaknesses, thus better secure their assets. Congratulations to PECB for this significant addition to their training catalog.

Bachir Benyamm, Managing Director at OASISEC, Algeria



I am glad that I was chosen to attend the Lead Ethical Hacking training course. The course was delivered virtually, which was something I was expecting for an Ethical Hacking Course. The trainer was just great,and PECB was supportive throughout the process.
Well done PECB!

Frances Sithole, Senior Cybersecurity Trainer, Zimbabwe

Fantastic course! If you want to get your CLEH certification, this is the course to take. The instructors are knowledgeable and patient and walk you through the exercises repeatedly to ensure adequate knowledge transfer and plenty of practice. Highly recommend this course!!

Carl Carpenter, Consultant at Arrakis Consulting, Arizona

First of all, I want to thank PECB for giving us this opportunity. The CLEH is a great module that will allow those who want to become penetration testers or SecOps to have a solid basis for learning and improving in ethical hacking.

Nicaise Kouame, Infrastructure and Security senior manager at BNETD| Founder and CEO at NKTEK HOLDING, Côte d'Ivoire

The CLEH course is a great ethical hacking course, blending academic content with practice scenarios.

Pablo Barrera, Cybersecurity Services Director, Guatemala

LEADERSHIP

Creating a Security-Awareness Culture: What is the Leader's Role?

BY MADHU MAGANTI

People, processes, and technology are often seen as the three pillars of Information Security. Although a proper balance between the three is seen as essential, the aspects of internal culture and employee training as they relate to the "people" pillar are often overlooked. As an Information Security program is only as strong as its weakest link, a lack of focus on the people within an organization can lead to reduced effectiveness of any spend on processes and technology.

In order to bolster the "people" pillar, organizations should seek to establish an internal culture where employees understand the importance of cybersecurity and uphold defined policies, procedures, and controls. Modifying the existing corporate culture to incorporate this aspect of security awareness will require buy-in and support from all the leaders within the organization, who should be responsible for the following:

1. **Supporting the initiative** – The most important thing that leaders within an organization can do to promote a security-awareness culture is to maintain a positive attitude towards Information Security. Showcasing their support for the security measures desired by the organization will help convey the importance of these goals to the employees around them. Negative signaling from any leaders within the organization may encourage resistance among the employees.

   Additionally, leaders should be on the lookout for any employees who are not adopting the required attitude towards Information Security and should attempt to address the situation in a positive, proactive manner.
2. **Leading by example** – Regardless of what they tell employees, leaders who openly deviate from policies, procedures, or controls are showing the employees around them that this is acceptable behavior. This can range from using a simple "shortcut" in a procedure to using a personal computer that has not been approved by IT. Employees who see leaders not complying with these measures may start to question why they have to do them or may follow suit without asking for approval.
3. **Understanding Information Security** – While leaders within an organization may not be Information Security experts, they should be provided with additional training. Having this knowledge will allow the leaders to better explain Information Security to the employees around them as needed, as well as reduce the likelihood of the individuals being involved in any incidents or events which may reduce their credibility within the organization.
4. **Being involved** – Leaders within the organization should be made aware of or involved in creating items such as the Incident Response Plan, Business Continuity Plan, Disaster Recovery Plan, and other key procedures. While they may not need access to all the details, being aware of such information may allow leaders to better contribute to the organization.

Why is culture important?

As an often-overlooked portion of "people, processes, and technology", internal culture and security awareness are often the only things that come between your organization and a successful Social Engineering attack. A security-awareness culture will encourage employees to question suspicious activity, be more resilient to Social Engineering attacks, and be more adherent to defined policies, procedures, and controls.

A manufacturing firm suffered from a business email compromise in mid-2021. Business Email Compromise (BEC) is an exploit in which an attacker obtains access to a business email account and imitates the owner's identity in order to defraud the company and its employees, customers, or partners. In this case, the scammer posed as the CFO after following and waiting for a Friday evening to send an email to an Accounts Payable employee asking him to send out a payment to a "new" vendor for $450,000. The email had a sense of urgency attached to it as well as clear instructions that required the employee to pay the vendor that very evening.

The employees in this company never questioned anything that came their way and were doers. The scammer took advantage of the fact that there was also this culture within the firm of not questioning anything that came in from a position of power, vis-à-vis the CFO. This is a classic case where the scammer took complete advantage of a poor security culture. A strong security culture could have helped avoid situations like these and other scams by creating a heightened sense of security within the organization to verify before trusting such emails or other communication.

Having a strong control environment also ensures that all payments go through a certain level of approval based on dollar amounts besides ensuring segregation of duties controls. Create a culture of collaboration and reward employees for bringing up security concerns timely. This not only allows everyone to feel accountable but also creates an opportunity for the employees to act as guardians for the organization. If the tone at the top was security-oriented and employees could reach out to their leadership without any fear of repercussion, the CFO could have been called to verify the contents of the email.

Who is a leader?

For the purposes of creating a security-awareness culture within an organization, a lot of individuals can be considered leaders. Ranging from the Executive Management team to managers overseeing the corporate office, changes in culture must start from the top down but be enforced at every level of authority. Any deviations from the goal security-awareness culture may have rippled through the organization, with higher-ranking leaders causing larger setbacks with noncompliance and leaving the organization more exposed to Social Engineering attacks.

As part of a consulting firm, we encounter many situations that could merely be avoided if the whole organization took security seriously, including the upper management. We ran into a peculiar case at a large healthcare organization where a VP sent out an email that mentioned that all employees would need to do the security awareness training and that anyone who does not attend it will be fired. Unbeknownst to the VP, there was also a phishing campaign that was being run for everyone in the organization. The results were that a large percentage of the employees did not click on the email that we had sent out because they had gone through the security awareness training, which educated them on what to look for as part of phishing emails. The interesting point that stood out for us was that the VP who had sent out the email had not only not taken the training but also clicked on the phishing simulation email.

We see several situations where the C-Suite does not want to comply with the IT Security policies that the rest of the organization complies with. This not only creates the culture of "Why should I do it when the leadership does not believe in this?" but also ensures that the upper management, who are typically carrying a lot of sensitive information with them, are at higher risk of being compromised. It is imperative that the leaders lead by example and not help set a bad tone at the top.

Planning matters

At the end of the day, any organization looking to add security awareness to their own internal culture should do so only after extensive planning. While the responsibility for Information Security may fall on a certain group of people, this group should attain buy-in and seek input from leaders throughout the organization and work closely with them for the implementation of any planned changes. Doing so may reduce the burden on the responsible group, improve employee attitude towards changes, and ensure a more seamless experience overall.

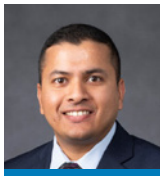
Depending on the size or scope of the project, it's not uncommon for organizations to partner up with specialized consulting firms or establish internal committees with representation from multiple business groups.

- Leveraging professionals who have a long history of building and improving Information Security environments from the top down can prove to be an invaluable resource. A consulting firm may reduce the likelihood of costly errors occurring, help manage the project and keep it on track, contribute years of relevant experience, facilitate internal communications, provide input on other relevant

topics such as business process improvement or risk management, or anything else agreed upon in the project scope. This will provide an organization with a scalable amount of human capital at agreed-upon costs, as opposed to either hiring a set number of employees or being time-constrained based on the current amount of available employees – assuming they don't get assigned additional projects/ responsibilities in the same time frame.

- Internal committees are a great way to facilitate regular communication in larger organizations and will allow the responsible group to attain buy-in and receive input from multiple leaders at once. This will ensure that leaders are on the same page during the planning phase and that the organization can be better coordinated during the implementation phase – resulting in the smoother deployment of planned changes.

Countless factors that go into successfully changing your organization's culture, but the importance of attaining buy-in or even help from internal leaders, should not be underestimated.



Madhu Maganti
CPA, CISA, Partner at ABIP, P.C

Madhu Maganti, CPA, CISA, is a partner at ABIP, P.C. and has over 18 years of experience in Cybersecurity and other IT advisory services, including IT strategy and planning, business process improvement, and IT compliance assessments, and more. Madhu leads the firm's Cybersecurity & Technology Services group. Madhu's experience is with mid to large-size firms across a variety of industries, including technology, healthcare, energy, and finance.

Prior to joining the ABIP team, Madhu gained industry knowledge and global experience leading several IT and finance teams within a leading technology company, as well as serving in leadership roles at management consulting and CPA firms. Madhu graduated from Bangalore University with a Bachelor of Commerce and from Baruch College (Zicklin School of Business, New York) with a Masters in Accountancy. He is a member of the Information Systems and Audit Control Association (ISACA) and the Institute of Internal Auditors (IIA).

Managing Cyber Risks within the Mid-Market during and Post Pandemic

BY SEYED HEJAZI

Introduction

Since the start of the COVID-19 pandemic, organizations around the globe hustled to provide the infrastructure to support the sudden and immediate need of working remotely. There were three main categories of organizations when it came to providing remote workforce the means to continuing business: large enterprises that were already well-positioned due to the connected nature of their business; organizations that had access to the required infrastructure but needed large-scale changes to make remote working possible; and those that had not planned for remote working and needed ad-hoc planning and preparation of infrastructure.

Many mid-market organizations fall under the third category; requiring IT teams to work around the clock to architect solutions, acquire tools, and mobilize teams to support the continuity of the business. Unfortunately, cybersecurity and protection of the newly architected networks, and remote-working solutions were overlooked due to time and budget limitations. As reported by Tanium Survey, 7 out of 10 organizations report facing new security challenges as a result of the pandemic, but only a third of them consider cybersecurity a top priority for 2021. Therefore, many of the planned security-related projects were concluded. This opened an opportunity for the malicious actors to capitalize on this gap and intensify their attacks.

What is going on in the wild?

Cyber-attacks have proliferated during the pandemic. Less secure remote working environments and insufficient awareness amongst the general users have contributed to this issue since the beginning of the pandemic. Statistics below highlight the magnitude of the risks organizations face:

- **99%** of analyzed cybersecurity claims, for a total of $537M, originated from Small-to-Medium Enterprises (with less than $2 billion in revenue), according to NetDiligence Cyber Claims Study 2021 Report;
- According to a Sophos State of Ransomware Report 2021, **37%** of respondents were hit by ransomware in the last year;
- According to the same report, the average ransom amount paid by mid-size organizations was **$170,404**;
- Accordingly, organizations have faced an upward trend in cyber-attacks specific to the nature of the pandemic.

Advancement in ransomware

Ransomware attacks have changed in the past couple of years, specifically during the pandemic, and that change in the attackers' mindset and strategy is here to stay. Specifically, attackers are:

- Showing less interest in casting a wide net and blindly spreading their malware in the wild. They rather conduct reconnaissance against their target, sometimes maintain a presence in the environment to exfiltrate valuable information such as information about the executives and details of financial and bank statements, and lastly unleash sophisticated and targeted ransomware;
- Developing their own security probing tools as opposed to leveraging existing "hacking tools";
- Increasingly exfiltrating large volumes of data, hoping to threaten the target organization to publish or sell their data;
- Actively deleting or encrypting backups to prevent the victim from using that to recover from the attack and not pay the ransom.

Furthermore, Ransomware as a Service (RaaS) is becoming a booming business for high-end criminals who provide the purchasers with malware, training, and customer service!

The risk of ransomware attacks is so high, and the impacts are so deep that the US administration is seeking an alliance with 30 other countries to combat the increasing risk of ransomware attacks and illegal use of cryptocurrency.

Phishing attacks

These attacks do not have any new technical aspects in their nature, but the phishing emails have now focused on exploiting the nature of the pandemic, and by leveraging human's sense of urgency, they have been more successful. Examples include phishing emails that pretend to originate from:

- Public health officials such as World Health Organization (WHO), US Centers for Disease Control and Prevention (CDC), or other local government health officials around the world;
- Company representatives such as Human Resources (HR) department, employee insurance coordinators, or executives with messages around emergency announcements or request for donations; or
- Law enforcement with messages around curfews, lockdowns, protests, etc.

Process attacks

Attacks targeting new or adjusted processes that have been put in place due to the pandemic are another method that adversaries are targeting organizations around the globe.

Attackers realize that many corporate communications and processes are under rapid alteration to accommodate remote work and may lack communications. For example, an attacker may ask an administrator within the target company to approve an illegitimate invoice by claiming that the original approver is not available due to an illness (e.g., COVID-19).

Alternatively, attackers may focus on processes that have been forced into manual mode because platforms, people, or processes are now unavailable. For example, banks may be overloaded with phone calls and slow to respond to requests, so attackers pressure employees to bypass controls to directly move payments.

How to address the risks

In order to address the cyber risks associated with the pandemic, the same security principles and good practices should be followed. More emphasis should be placed on remote working capabilities, remote connectivity, endpoint and user device security, identity and access management, security logging and monitoring, and security of cloud services. Based on what we have seen during most of the recent attacks, below are outlined the key steps to take to prepare your organization and address the risks:

1. Address the basics of security hygiene; patch your systems for the recent vulnerabilities, and prepare segregated backups;
2. Define a strong password policy and implement it across all your platforms and systems;
3. Implement an appropriate level of network segmentation to enable timely containment of incidents and breaches;
4. Develop a mobile security policy that includes a "Bring Your Own Device" (BYOD) scenario to limit the exposure of organizational data through employees' mobile devices;
5. Provide continuous security awareness training to employees and executives according to the most recent trends (e.g., those mentioned earlier in this article);
6. Implement a multi-factor authentication tool (MFA)
7. Leverage advanced tools such as Endpoint Detection and Response (EDR) tools to enhance your detection and response capabilities;
8. Maintain a robust security monitoring and detection program to identify threats well in advance;
9. Conduct technical security testing as a means to identify vulnerabilities that can be exploited by attackers;
10. Develop, improve, and rehearse a cybersecurity incident response plan; know who to contact and what steps to take during a cybersecurity incident;
11. Develop and test your disaster recovery plan (DRP), and ensure the recovery objectives can be met;
12. Ensure you have a communication plan, specifically with your stakeholders, customers, legal counsel, and third-party service providers;
13. Develop a third-party risk management program and ensure that appropriate clauses are documented in your third-party contracts, demanding your service provides and vendors to keep you informed about possible incidents involving your data;

14. Develop and maintain a privacy policy;
15. If you have outsourced it or security services to a managed service provider, test their capabilities;
16. Understand what you can afford and what is the threshold in case you decide to pay a ransom, and decide on the contingency funds;
17. Decide on your cyber insurance policy, review it and ensure it covers what is important for you;
18. Leverage cyber threat intelligence (CTI) to determine if credentials from your organization have been breached in any previous cybersecurity incident;
19. Have access to skilled cyber response service providers who can assist contain the incidents and recovery on time;
20. Know your compliance requirements in case you need to report breaches to regulators and other bodies.

In addition to the tactical steps above, organizations should develop a comprehensive cybersecurity program aligned with good security practices and common standards. Such a program will establish a framework for implementing controls around protecting the organization and its crown jewels and help prioritize the initiatives with a larger impact.

Large initiatives such as implementing a zero-trust security model, cloud-centric computing environment, and decentralized identity take longer but will prove to be hugely beneficial for large enterprises that can afford to invest in the future.

Post pandemic and privacy

With vaccines provided to many individuals around the globe, organizations in different jurisdictions are mandating proof of vaccination, vaccine passports, or negative test results for employees and customers.

This poses new privacy and security challenges as organizations need to safeguard these sensitive documents – that in many cases may contain Protected Health Information (PHI).

Organizations that never dealt with PHI or other personal sensitive information are suddenly in possession of such information.

If your organization is collecting these vaccine passports, test results, etc., you need to ensure you have a plan for storing and safeguarding such information according to the applicable laws and regulations.

in

Seyed Hejazi
Director, Security and Privacy Risk Consulting at RSM Canada

Seyed Hejazi is director of security and privacy risk at RSM Canada. Having more than 15 years of experience in Cybersecurity and I.T., Seyed possesses deep knowledge of cybersecurity and privacy risks, governance models, frameworks, technologies, and leading practices. Seyed's knowledge of security operations, cyber threat intelligence, incident handling, digital forensics, and the cybersecurity related regulations has enabled him to help organizations transform their cybersecurity practices by leveraging the appropriate combination of people, processes, and technologies to protect confidentiality, preserve integrity and promote availability. Seyed holds a Master's degree and designations including CISSP, PMP, GCIH, GREM, CFE. He teaches cybersecurity courses at the University of Toronto.

Meet the panelists headlining the PECB Insights Conference 2021

The PECB Insights Conference is almost here, and the registration period will remain open only until 12:00 PM Friday, November 12th. The two-day conference will feature two sets of three simultaneous sessions in three languages, English, French, and Spanish.

Just like previous PECB Conferences, this year's conference will also feature some of the best information technology, security, and privacy experts from around the globe.

At the end of each session, you will get the opportunity to address your most pressing questions and learn from these amazing professionals.

You can read more about what will be discussed during each conference session in our topics **explained article**.

The panelists come from different areas of expertise, including but not limited to AI, Blockchain, IoT, CMMC, Data Privacy, GDPR, and much more. You can read their biography by clicking on the image of each **panelist**.

We hope to e-see you during our conference on 15 and 16 November!

REGISTER NOW FOR FREE! ▶

MODERATORS

JORGE GARIBAY OROZCO

Director general at Let´s Cloud IT
Mexico

JORGE EDO JUAN

Partner Director and Training Responsible at Mobiliza Academy
Training Director in ISACA
Spain

JULIO CÉSAR BALDERRAMA

Co-Founder and CEO of PROYECTO AURORA
Argentina

DANIELA CIREASA

Privacy Manager - Netspace, Senior Partner - Neoprivacy
Vicepresident - ASCPD
Romania

ABDELMALEK NAJIH

IT Security Compliance and Threat Intel Officer at IQ-EQ
Luxembourg

JOHN VERRY

CISO & Managing Partner at Pivot Point Security
United States

SOLOMON UGAH

Senior Security Analyst, Bennett Jones SLP
Managing Partner, OmNiche Consulting Inc
Canada

BRUNO VERACHTEN

Hacker in Residence at Worldline
France

DANIEL ELÍAS ROBLES

Principal Consultant at Savant Consultores
Dominican Republic

WALID ABDAOUI

IoT and Cloud Consultant at Devoteam Revolve
France

STELLA MAKONA SIMIYU

Chief Operating Officer at Sentinel Africa Consulting Ltd
Kenya

JOSINA RODRIGUES

Academic Advisory Board Member at INATBA
Portugal

PECB INSIGHTS 2021 CONFERENCE

PANE

LUC SAMSON
President at Briskwave Consulting
Canada

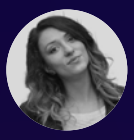
EDUVIGIS ORTIS MORONTA
Strategic Alliances Leader at SAS Founder & President of Women4Cyber
Spain

LAURA MARTÍNEZ RETAMAR
Consultant at GlobalSUITE Solutions
Spain

BECHIR SEBAI
Founder and CEO at ACG Cybersecurity
France

VINCENZO TIANI
Partner - Brussels Office at PANETTA Law Firm
Belgium

Adjunct Professor at IULM University
Italy



ANDRA FECIORU
Head of Product Management at Frontiers
Switzerland

ADARSH PANDA
Artificial Intelligence & Data Science Lead, Credera UK
United Kingdom

ERIC BADERRAMA
CISO at RappiPay
Mexico

ANNA LONDON
Founder & CEO at Chrysallis, Inc.
United States

TUDOR GALOS
Data Protection Senior Consultant at Tudor Galos Consulting
Romania

JULIA URBINA-PINEDA
CEO at CyberIIoT
Mexico

JUDICAËL BLANC
President at Alphaxdata
France

JOSELINE HERNÁNDEZ
Sales Engineer at Sophos
Argentina

MARY JULIA RODRÍGUEZ
Operational Risk management at Banco General
The Republic of Panama

PABLO BARRERA
Information and Cyber Security Services at Estrategia y Seguridad
Professor at Universidad Francisco Marroquin
Guatemala

MICHÈLE COPITET
Founder and director of EGONA-Consulting
France

LISTS

NABIL ALY

Founder and CEO at Sabytel Technologies Inc.
Canada

Founder and CEO of Niskaa Group SPRL.
Belgium

VALERIANE SAKA

Information System Security Manager, Bank Of Africa Madagascar
Madagascar

MANUEL COLLAZOS BALAGUER

Owner and General Manager at PRIME PROFESIONAL SAC
Peru

JUAN DÁVILA

Managing Director at PRAGMATIC Cybersecurity, Information Security, Government and IT Audit
Peru

ROBERT HELLWIG

Managing Director & CISO at CARMAO GmbH
Germany

YASSIR KARROUTE

Founder and CEO at REDLab
France

REGINE BONNEAU

Founder and CEO at RB Advisory, LLC.
United States

KHURRAM SHROFF

Chairman of the Board & CEO at iMining Technologies
Canada

JOSINA RODRIGUES

Academic Advisory Board Member at INATBA
Portugal

SHERRIF ISSAH

Information Security, GRC Consultant,
Director of Communications at Institute of ICT Professionals
Ghana

ARTHUR DONKERS

Managing Director at Cyberlink Security Ltd
Ireland

NUNO CORTESÃO

Co-Founder & CEO at Zharta
Portugal

PETER GEELEN

Director and Managing Consultant at CyberMinute and Owner of Quest for Security.
Belgium

LEIGHTON JOHNSON

CTO and Founder at ISFMT
United States

KARIM GANAME

Founder & Cybersecurity Researcher and Expert at StreamScan Cybersecurity
Canada

Penetration Testing Tools

BY ERWIN GEIRNAERT

The technological revolution of the last 20 years has seen cybercrime evolve as much as, if not more than, its counterpart, cybersecurity. Some recent forms of cybercrime include:

- New attack vectors
- Monetization of breaches by distributing state-of-the-art ransomware
- Data exfiltration and extorsion

Combining zero-day exploits with human-operated attacks is eye-opening for organizations to reduce their attack surface and level up the patching game.

A penetration test is a black-box exercise by ethical hackers to find and exploit weaknesses in the network, infrastructure, applications, APIs, etc. If done regularly, it is very efficient in discovering vulnerabilities and weak points.

There is an essential difference with the advent of bug bounty platforms like Bugcrowd, Synack, and HackerOne. A penetration test is limited in time, bound by contractual agreements between the client and the penetration tester(s), as well as by the pen testers' abilities.

In a bug bounty program, the client asks bug bounty hunters (security researchers) to identify vulnerabilities in the defined scope, often throughout a year.

Because of the explosion of social media, several bug bounty celebrities have released their internal tools to the public. This article focuses on the tools and methodology that penetration testers and bug bounty hunters use to find vulnerabilities.

Penetration testing tools are illegal when used without explicit written permission by the client, the so-called "out-of-jail card."

Burp Suite Professional

Burp Suite Professional is a web proxy intercepting all web traffic from the browser, a mobile app, or an internet application. For many years, it has been the most used web proxy to test web applications and APIs. Burp Professional's founding company, Portswigger, comprises well-known security researchers like Dafydd Stuttard and James Kettle. On their website, there is an interesting quote by Dafydd: "I created Burp Suite as a side project when I was working as a penetration tester a long time ago. I was lazy and wanted to automate my job. I ended up having more fun working on the software than doing actual testing, so I decided to focus on that."

Dafydd is also the author of one of the best books available on web security: "The Web Application Hackers Handbook" (short, "WAHH"), published a decade ago. The book can be considered a penetration testing tool of its own. Dafydd made the excellent decision not to publish a third version of the book, but instead create an online version called the Web Security Academy.

This version is packed with technical information on web vulnerabilities and fantastic online labs, and it is completely free! A few months ago, Portswigger also released a very interesting certification: Burp Suite Certified Practitioner.

A few years ago, Burp implemented an embedded browser, making it very easy to start with hacking websites without the need to configure the proxy settings in the browser.

Burp Suite has three editions:

- Community: Free, but limited in functionality and performance
- Professional: Annual price per user
- Enterprise: An enterprise web scanning solution to compete with web scanning tools like Detectify

Burp Professional has several essential modules:

1. Burp Proxy: This module maintains an entire web traffic history, including requested and received HTTP requests with the full HTTP header and HTTP body. Burp Proxy allows to intercept an HTTP request, change it, or send it to other modules, like Burp Repeater, Burp Intruder, and Burp Decoder.
2. Burp Repeater: This module allows the penetration tester to repeat an intercepted HTTP request, changing headers and parameters to investigate the HTTP response and learn more about the web application. The penetration tester can remove cookies to check for authentication issues, replace cookies with other values to verify the authorization controls, change the request method, and do whatever is needed to manipulate the application.
3. Burp Intruder: This is the most limited module in the Community Edition because it's the most powerful and most used by penetration testers. It allows to automate thousands of requests with different payloads and can be used to brute-force directories, filenames, usernames, passwords, as well as to exploit vulnerabilities like direct references or broken object-level authorization.
4. Burp Scanner: This module is now fully integrated into the dashboard and is no longer separate. Launching a scan is now done by right-clicking on a domain/URI and selecting Scan. In the scan configuration, it is possible to configure the crawling, the audit mode, the authentication records, and the performance.
5. Burp Decoder: This tool is used to decode or encode any string to see the contents like Base64 encoding or MD5 hashing.

One of the best features of Burp Professional is the BApp Store. It allows you to install additional modules from Burp security researchers, bug bounty hunters, or other Burp freaks. Using these extensions, penetration testers can use:

- *Authorize* to automate testing of authorization controls (Authorize will replay each HTTP request with a different cookie or token of a less-privileged user to learn how the application responds.)
- *Turbo* Intruder to send a lot of requests simultaneously
- *JSON Web Tokens* (JWT) to examine the strength of the JWTs used for authentication and see if they are vulnerable to known attacks
- *Add Custom Header* to add a specific header in each request
- *Flow and Logger++* to have complete insight into all the HTTP requests and HTTP responses that are communicated with the application

ProjectDiscovery, Inc.

ProjectDiscovery is a more recent platform maintained by some volunteers who have seed-funding led by SignalFire, with major investors Accel and Rain Capital.

They have some fantastic support from security veterans like Caleb Sima (VP Security Databricks), Gerhard Eschelbeck (former Google CISO), Michael Coates (former Twitter CISO), Jason Chan (Netflix CISO), and Sacha Faust (Senior Manager Security Intelligence at Amazon).

ProjectDiscovery wants to be fully open-source and cloud-based. That is the strength of their platform, since it allows the platform to provide several useful features, such as:

1. *Chaos:* ProjectDiscovery actively collects and stores internet-wide asset data. They already have information on 6 billion internet assets, which can be accessed using their API and their client developed in *Go* and are available on their GitHub page. In the Go *client*, it is possible to request all data for a specific domain, like uber.com, which returns the data from the Chaos API instantly, allowing the penetration tester to identify what asset to target. The following are some assets that can be targeted:
   chaos -d uber.com -silent

- restaurants.uber.com
- testcdn.uber.com
- approvalservice.uber.com
- zoom-logs.uber.com
- eastwood.uber.com
- meh.uber.com
- webview.uber.com
- kiosk-api.uber.com
- utmbeta-staging.uber.com
- getmatched-staging.uber.com
- logs.uber.com
- dca1.cfe.uber.com
- cn-staging.uber.com
- frontends-primary.uber.com
- eng.uber.com
- guest.uber.com
- kiosk-home-staging.uber.com

```
root@b0x:~# subfinder -d hackerone.com -v

        _     __ _          _
____  _| |__ / _(_)_ _  __| |___ _ _
(_-< || | '_ \  _| | ' \/ _  / -_) '_|
/__/\_,_|_.__/_| |_||_\__,_\___|_| v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for hackerone.com
[sitedossier] www.hackerone.com
[virustotal] api.hackerone.com
[virustotal] support.hackerone.com
[virustotal] docs.hackerone.com
[virustotal] mta-sts.hackerone.com
[virustotal] mta-sts.forwarding.hackerone.com
[virustotal] a.ns.hackerone.com
[virustotal] b.ns.hackerone.com
[virustotal] links.hackerone.com
[virustotal] info.hackerone.com
[archiveis] hackerone.com
[securitytrails] email.gh-mail.hackerone.com
[securitytrails] mta-sts.managed.hackerone.com
[securitytrails] web-seo-content-for-business.theflyingkick.websitedesignresource.api.hackerone.com
[passivetotal] cf-ssl5349-protected-cover-photos-user-content.hackerone.com
[passivetotal] o1.email.hackerone.com
[passivetotal] go.hackerone.com
[passivetotal] cf-ssl5349-protected-profile-photos-user-content.hackerone.com
[passivetotal] o3.email.hackerone.com
[passivetotal] profile-photos-user-content.hackerone.com
[passivetotal] cf-ssl41462-protected-profile-photos-user-content.hackerone.com
[passivetotal] cover-photos-user-content.hackerone.com
[passivetotal] staging.hackerone.com
[passivetotal] cf-ssl41462-protected-cover-photos-user-content.hackerone.com
```

2. *Subfinder:* This is a subdomain discovery tool that discovers valid subdomains for a specific target by using passive online sources. Subfinder can be configured with the correct API key to query the following APIs: Binaryedge, C99, Certspotter, Chinaz, Censys, Chaos, DnsDB, Fofa, Github, Intelx, Passivetotal, Recon.dev, Robtex, SecurityTrails, Shodan, Spyse, Threatbook, Virustotal, Zoomeye
3. *Nuclei:* This open-source vulnerability scanner was created in *Go* and is powered by the community. Contributors can add custom vulnerabilities using a description language in YAML, allowing very straightforward and quick updates to the scan templates. These vulnerabilities range from default credentials to unauthorized access and proof-of-concept for exploits. Many penetration testers have already automated their workflow by using the workflows in Nuclei to deliver consistent penetration tests. The following quote from the GitHub repository elaborates on the matter:

"For Penetration Testers - Nuclei immensely improve how you approach security assessment by augmenting the manual, repetitive processes. Consultancies are already converting their manual assessment steps with Nuclei, and it allows them to run a set of their custom assessment approach across thousands of hosts in an automated manner.

"Pen-testers get the full power of our public templates and customization capabilities to speed up their assessment process, specifically with the regression cycle where you can easily verify the fix.

- Easily create your compliance standards suite (e.g., OWASP Top 10) checklist.
- With capabilities like fuzz and workflows, complex manual steps and repetitive assessment can be easily automated with Nuclei.
- Easy to re-test vulnerability-fix by just re-running the template."

Conclusion

In the last years, penetration testers have improved their automation skills and cooperation. They share their experience online and use different platforms, like Hack The Box, Web Security Academy, and bug bounty programs to improve their skills.

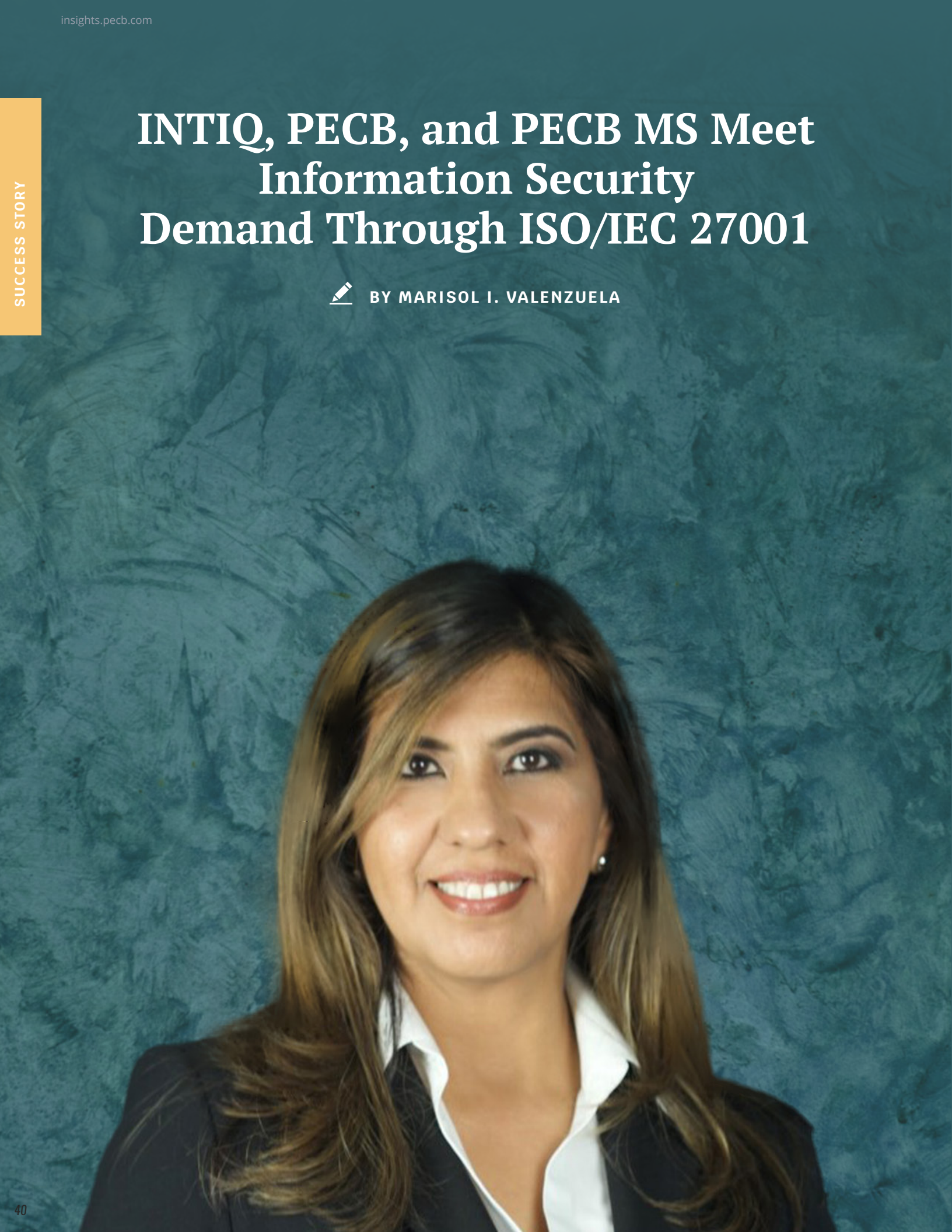
Because of the complexity of the applications, organizations cannot rely on automated scanners to identify all security issues. A manual approach by a skilled penetration tester with the correct toolset is needed to have a good understanding of the attack surface and the vulnerabilities.

Erwin Geirnaert
Co-founder & Chief Hacking Officer at Shift Left Security BV

Erwin Geirnaert holds an MSc. degree from Ghent University (1999). He is a Senior Security Expert with the main focus on offensive security. As a penetration tester with 20 years of experience, he knows how to attack an application and test for security holes. He is a recognized security expert and presents on application security topics at conferences like Eurostar, OWASP, Infosecurity, LSEC, etc. Geirnaert has started two companies: ZIONSECURITY (acquired in 2019 by Orange Cyberdefense) and Shift Left Security. He is an active bug bounty hunter for Detectify, Synack Red Team, Bugcrowd, and HackerOne.

INTIQ, PECB, and PECB MS Meet Information Security Demand Through ISO/IEC 27001

BY MARISOL I. VALENZUELA



We do business in an increasingly complex world of bytes, account numbers, and passwords. Nearly everything in our lives is now stored on a cloud.

But our reliance on technology has come at a cost, making us more vulnerable to cyberattacks. The Center for Strategic and International Studies (CSIS) in Washington, D.C. reported at least 85 "significant cyber incidents" around the world between January 2021 and the end of July 2021. These include cyberattacks on government agencies, defense, and high-tech companies as well as economic crimes with losses estimated at more than $1 million.

In July, the Japan 2020 Olympics suffered a breach of usernames, passwords, addresses, and bank account numbers involving volunteers and ticket holders, according to CSIS.

Cyberattacks have become a global threat to all organizations, no matter the size, type of business, or client base. If you use a computer, mobile phone, tablet, or any type of automated equipment or vehicle in your business, you are a potential target.

Our story

As president of INTIQ Solutions, it is a privilege to be able to share our story with you. We are a Subcontractor Key Location an authorized partner of PECB Management Systems (PECB MS) as well as a Platinum Partner of PECB Group, offering a full breadth of certification services around globally recognized business standards. These include ISO/IEC 27001 (Information Security Management Systems — ISMS), ISO/IEC 27701 (Privacy Management Systems — PMS), and ISO 22301 (Business Continuity Management Systems — BCMS). In addition, INTIQ is also working with Cybersecurity Maturity Model Certification CMMC and has been approved as a Candidate C3PAO — CMMC Third-Party Assessor Organization.

INTIQ Solutions was established in 2013 with a vision of adding value to management systems certification. Three years later, INTIQ partnered with PECB MS to offer accredited certification through independent audits and periodic surveillance visits. INTIQ is responsible for sales, customer care, and facilitating client audits with PECB Auditors, while PECB MS is responsible for the overall certification process including the certification decision.

In recent years, a growing number of organizations in the United States and countries around the world, have turned to ISO/IEC 27001, an internationally agreed-upon management system standard on information security management, as a framework for protecting sensitive data. This standard has become one of our most sought-after certifications, particularly among law firms, government agencies, and health care organizations.

This standard requires organizations to document key processes and regularly review the information security system for continued effectiveness through a combination of management reviews and regular internal audits. The system must incorporate corrective and preventive actions as well as risk assessments to ensure its continued relevance.

Essentially, ISO/IEC 27001 requires organizations to have a robust information security system in place with key controls to protect sensitive data. Organizations are less likely to fall victim to cyberattacks when they have considered their vulnerabilities and taken steps to guard against intrusions.

Because the system is based on international consensus standards, it is repeatable across multiple sites and even the organization's entire supply chain if desired.

Together with PECB MS, we at INTIQ have channeled our energy into high-value services for our clients. PECB MS maintains a pool of approved auditors around the world that allows us to service international clients with multiple locations. INTIQ provides the necessary support for PECB MS Auditors who work with our clients. We in turn work with PECB MS to find ways to improve our processes and incorporate best practices wherever possible.

COVID-19 challenge

The unprecedented COVID-19 pandemic created unique challenges for PECB MS Auditors and clients. INTIQ worked with PECB MS to develop procedures that ensured the health and safety of auditors and clients by minimizing the risk of exposure to COVID-19 while still maintaining compliance with certification requirements.

A PECB MS policy permitting remote audits was approved by the organization's accreditation body once accreditors were satisfied that the annual certification process and audit requirements would still be fulfilled. Considering that the majority of ISO/IEC 27001 clients already stored their documentation in the cloud, it was a relatively straightforward process to obtain access to the necessary audit documents via remote access. INTIQ and PECB MS remained committed to staying true to ISO/IEC 17021-1 as well as International Accreditation Forum (IAF) mandates.

INTIQ also had to make changes to the delivery of public training courses and certification programs, which we

offer in partnership with PECB Group. Programs were presented entirely online with self-study components that allowed us to continue operations during the pandemic.

Standards journey

My journey into the world of management systems began with the ISO 9000 family of quality management system standards, which were first published in 1987. I was introduced to ISO 9001 a few years later through a friend who was assisting Exxon with its implementation. I was working at United Cerebral Palsy on multiple programs for people with disabilities at the time.

After reading through ISO 9001, I began to see ways in which I could apply the standard to my programs at United Cerebral Palsy. The results were impressive, so much so that I began to assist other organizations with implementations primarily throughout Latin America. I quickly gained experience as an internal auditor though I found it challenging at the time to implement English requirements in companies that mainly operated in Spanish. Little did I know that I would play a role in addressing this issue later in my career.

Early adopters primarily wanted to ensure that they could meet customer requests for certification. In Latin America, certification was viewed as an opportunity to penetrate into American and European markets. ISO 9001 was seen as a tool to transcend entry barriers into new marketplaces while promoting confidence and creating a common language by which companies could communicate with other certified organizations.

It was interesting to see how ISO 9001 became a stepping-stone to industry-specific standards like ISO/TS 16949 for the automotive industry and AS9100 for aerospace companies. The use of industry-specific variations based on ISO 9001 subsequently fueled the global certification movement and led to an expansion of related standards like ISO 14001 for environmental management and ISO/IEC 27001.

My formal participation in the development of standards began shortly after the 9/11 attacks when I attended my first meeting of the U.S. Technical Advisory Group to International Organization for Standardization Technical Committee 176 (ISO/TC 176). The committee is charged with maintaining the ISO 9000 family of standards, including ISO 9001. The meeting was planned to be held in Crystal City, Virginia, steps away from the Pentagon, but was relocated. Only a small number of U.S. delegates were present in the meeting compared to other meetings that I would attend over the years. It was there that I was invited to represent the U.S. delegation on the international committee that would perform the first Spanish translations of key standards from ISO's official two languages, English and French.

This role required more than translation skills because it proved to be another opportunity for delegates to renegotiate critical requirements. The translation committee had to agree on the intent of each clause and understand how they should be applied in a real-world setting to reach a consensus on the most appropriate translations. To understand the nuances of the standards, I found it beneficial to attend the working groups in which the standards and their subsequent revisions were drafted. This allowed me to better participate in the international debate that contributed to the wording of each translation.

Some 20 Spanish-speaking countries were represented on the translation committee, including Mexico, Spain, and Argentina. Each had a different way of interpreting the requirements. We had to achieve consensus to carry out our translations and we worked through many obstacles. The biggest challenge was thinking through the intent of the standards, understanding concepts, and finding appropriate wording that would be understood in all Spanish-speaking countries.

In a very real sense, we helped decide the way the standards would be applied in Spanish-speaking countries. Our consensus laid the foundation for thousands of third-party certifications to ISO 9001 and subsequently to other key management system standards like ISO/IEC 27001, ISO 14001, and ISO 26000 on social responsibility.

The international debate varied by how participating countries planned to use the various standards. European countries saw them as a replacement for regulatory requirements. As such, they wanted them to be as prescriptive as possible while countries like the United States wanted them to be much less prescriptive.

Based on my work at the national and international levels, I went on to establish the then American Welding Society's accreditation program for management system standards, which included ISO 9001 and ISO 14001. This led to my participation in the International Accreditation Forum (IAF), which governs the conduct of management system accreditation bodies around the world.

My participation in these groups helped me understand the importance of standards as well as the positive effects they have had on international trade.

They created a culture of doing things correctly, being ethical, and choosing not to cut corners. This contributed to improvements in the way we make our products, the way we monitor our environmental footprint, the way we protect our food supply, and most recently, the way we protect client data. I went on to work with several large, third-party certification bodies, including BSI America and Intertek.

Business relationships are key to successful growth

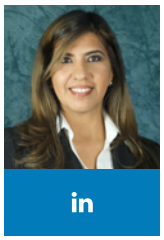
Partnerships thrive when built on a foundation of trust. Our success with PECB is a shared journey to create a future for both parties and the combined skills set a recipe for guaranteed success. Together, we are expanding our expertise and services and are continuously creating value through education and certification services around the world. INTI.Q has strategically partnered with PECB to offer training courses that will provide interested individuals with the tools that they need to advance in their career.

Developing great business relationships with PECB is an important element that we see as a catalyst to the overall success of our organization because no business can succeed without developing healthy relationships.

Last words

The lessons I have learned through my experiences have helped shape my desire to continually look for ways to add more value for my clients. Through our partnership with PECB MS, INTIQ strives to deliver excellent customer service and help clients exceed the minimum requirements of certification. Many of our new clients have contributed to the growing demand for ISO/IEC 27001 certification on information security, ISO/IEC 27701 certification on privacy, and ISO 22301 certification on business continuity.

Our world may have become smaller thanks to technology, but it has also become more challenging. Technology has changed the way we live and the way we see the world. We understand the inevitability of change as we race to keep pace with it. In many respects, management system standards allow organizations around the world to identify best practices that will help overcome the many challenges we face in today's business world.



Marisol Valenzuela
President at INTIQ Solutions

Marisol Valenzuela is president of INTIQ Solutions, an authorized partner of PECB Management Systems, which offers a full breadth of certification services around globally recognized business standards, including ISO/IEC 27001 (Information Security Management Systems) and ISO 22301 (Business Continuity Management Systems). She previously served as a U.S. technical expert for the International Organization for Standardization Technical Committee 176 (ISO TC 176), charged with maintaining the ISO 9000 family of quality management system standards. She has more than 25 years of experience in the field of management systems and has served on both the national and international committees responsible for translating key management system standards into Spanish. In addition to her technical work, Ms. Valenzuela has held senior business development positions with some of the world's largest management systems certification bodies. She is a former director of the then International Accreditation Registry (IAR) of the American Welding Society (AWS) and participated in the International Accreditation Forum (IAF) and International Laboratory Accreditation Cooperation (ILAC). She is also a former director of the International Auditor and Training Certification Association (IATCA). Ms. Valenzuela is a certified PECB ISO 9001 auditor and an approved PECB CMSA trainer. She can be reached via email at marisolv@intiq.biz or by telephone at 305.330.6337.

New Multiple-Choice Exams

PECB released the new multiple-choice exam format with high reliability, validity, and manageability.

The new multiple-choice exams developed by PECB evaluate candidates on a wide variety of learning objectives covered on the PECB training courses. All questions have three alternatives, of which only one is correct. They are based on scenarios that simulate real-life situations and are designed to provoke critical thinking in candidates. The new multiple-choice exam format is available for the following courses:

- ISO 37001 Lead Implementer and ISO 37001 Lead Auditor in English
- ISO 22301 Lead Implementer and ISO 22301 Lead Auditor in English
- GDPR – Certified Data Protection Officer (CDPO) in English

Future Multiple-Choice Exams that will be published by December 16:

- ISO/IEC 27005 Lead Risk Manager
- ISO/IEC 27005 Risk Manager
- ISO 9001 Lead Implementer
- ISO 9001 Lead Auditor

The transition end date for all the related essay-type exams will be December 17, 2021.

Stay tuned for future announcements!

Go to **List of PECB Exams** for more information.

Cybersecurity and the Role of Risk Management Techniques

BY BECHIR SEBAI, RABAH HACHICHI, ZIED SMAILI

Since spring 2020, cyberattacks have skyrocketed, and in a way, COVID-19 exposed new cybersecurity threats that organizations were not aware of, and not prepared to deal with. Not expecting to face cybersecurity crises and challenges, the majority of organizations had to improvise and improve their security.

With the emergence of new technologies, the number of cyberattacks is proliferating and their techniques are getting more sophisticated. Hackers have become better structured and meticulous in organized crime networks. They now have more efficient tools and can even offer their services in the Dark Web with distribution models such as MaaS (Malware-as-a-service) and other DDoS (distributed denial-of-service) products.

Reports from international organizations specialized in risk monitoring (ENISA, CVE, NIST, CIS, OWASP, etc.) classify digital risks as some of the most important risks organizations face today. Organizations have realized that in order to manage and better anticipate digital risk situations and other sophisticated threats, they must design and implement effective, and permanent risk management processes. To do so they are advised to implement a culture of data protection in the organization through the establishment of *Security by design* and *Security by default* processes.

In any case, one can make use of vulnerability assessments that are used to uncover weaknesses that could be exploited by a threat, or threat assessments that analyze how these threats could affect a particular asset, organization, or system.

Threat modeling involves examining all possible agents, actions or events, attack vectors, and vulnerabilities of a given system, asset, or process, and then modeling or simulating an example of how they might progress and see the damage they might cause.

When adapting the new risk management methodologies to address the challenges of immersive digital risks based on up-to-date attack threat scenarios, organizations should take into consideration the state-of-the-art threat identification framework, such as the MITRE ATT&CK Framework.

Detecting zero-day vulnerabilities is also another challenge for organizations. Proactive monitoring of infrastructure, networks, and systems, through SOC and CIRT monitoring, allows organizations to anticipate unclassified events that can turn into incidents. The risk management process provides the most effective security measures that should be implemented in order to protect an organization when anticipating any decision-making.

This requires first of all a precise mapping of the organization's systems and processes and then even more efficient processes of identification, analysis, and risk evaluation.

The consulting, auditing, and training firm ACG Cybersecurity has therefore developed its own methodology for digital risk management, in compliance with the ISO/IEC 27005 standard.

What makes this method so unique is the fact that it is well adapted to the best identification techniques of cybersecurity threats since it is based on Cyber Threat Intelligence and the latest attack techniques.

By thinking like hackers and unrolling the risk management process, organizations will be able to create a risk treatment plan that could prevent, detect, have response controls, and take action to remediate all types of attacks.

Our R&D teams continue their research to improve our unique methodology on the market.

Thus, by adopting this system, the company ensures continuous monitoring of threats and new attack techniques as well as technical vulnerabilities (including Zero Day).

The control of digital risks also requires alignment with security standards recognized by the market. In this area, the international standard ISO/IEC 27001 and its library of security measures ISO/IEC 27002, represent a solid security foundation adapted to the context and strategic priorities of the organization. The controls and requirements of those standards should be implemented in line with the logic of continual improvement, i.e. in a PDCA cycle (Plan, Do, Check, Act) to ensure that they are suitable to the context, risks, threats, and vulnerabilities that are in perpetual change.

We remind you that 100% security or zero risk does not exist, and in this case, preventing is better than curing.

Some statistics on emerging cybersecurity threats:

Top cyber threats in 2020 from the European Union Agency for Cybersecurity (ENISA) report:

1. Malware
2. Web-based attacks
3. Phishing
4. Web application attacks
5. Spam
6. Denial of service
7. Identity theft
8. Data breaches
9. Insider threat
10. Botnets
11. Physical manipulation, damage, theft, and loss
12. Information leakage
13. Ransomware
14. Cyber espionage
15. Cryptojacking

Top 10 risks for experts based on the AXA Future Risk report:

1. Climate change
2. Cybersecurity risks
3. Pandemics and infectious diseases
4. Geopolitical instability
5. Social discontent and local conflicts
6. Biodiversity and natural resource risks
7. New security threats and terrorism
8. Financial stability risks
9. Macroeconomic risks
10. Artificial intelligence and big data risks

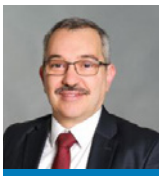
Some figures from the ENISA Threat Landscape 2020 report

- 400,000 detections of pre-installed spyware and adware on mobile devices
- 13% increase in Windows malware detections at business endpoints globally
- 71% of organizations experienced malware activity that spread from one employee to another
- 46,5% of all malware in e-mail messages found in '.docx' file type
- 50% increase in malware designed to steal personal data or stalkerware
- 67% of malware was delivered via encrypted HTTPS connections

Bechir SEBAI
Founder & CEO ACG Cybersecurity

PECB French Trainer of the Year 2019 & 2020

Bechir Sebai has more than 15 years of experience in strategic and operational consulting in security and cybersecurity for large private and public groups in France and other countries in Europe.



Rabah HACHICHI
Technical and Strategy Director

Rabah Hachichi has more than 25 years of experience in strategic and operational consulting in security and cybersecurity for large private and public groups in France and more, across Europe & Africa.

Zied SMAILI
Director of Operations

Zied Smaili has more than 15 years of experience in strategic and operational consulting in security and cybersecurity for large private and public groups in France and other European countries as well as Africa.

National Cybersecurity Awareness Month

Internet connects us all to everything and everyone. But sometimes people with malicious intents can use the internet to harm us. That is why now, more than ever, we need to be aware of the danger and be safe when online.

Do your part. #becybersmart

Cybercrime is up to 600% due to the COVID-19 pandemic (PurpleSec)

Many cybercriminals are now posing as the Center for Disease Control and Prevention (CDC) or World Health Organization (WHO) to trick recipients into clicking on suspicious links or downloading malicious attachments.

95% of cybersecurity breaches are a result of human error (Cyberint)

Every organization should provide its employees with proper training and appropriate tools to prevent cybersecurity breaches from happening.

More than half a million Zoom user accounts were compromised and sold on the dark web. (CPO Magazine)

Since Zoom became the leading video conferencing platform for organizations after COVID-19, cybercriminals have targeted platform users constantly.

Only 16% of executives say their organizations are well prepared to deal with cyber risk. (McKinsey & Company)

Adopting new technologies more than often leads to risks and breaches, and many executives find it challenging to stay up to date with cyber risk management.

Want to be more aware of the risks and dangers of cyberattacks?
Want to be a cybersecurity expert? You can learn more about cybersecurity with our cybersecurity training courses!

Explore our options

HAPPY WORLD STANDARDS DAY!

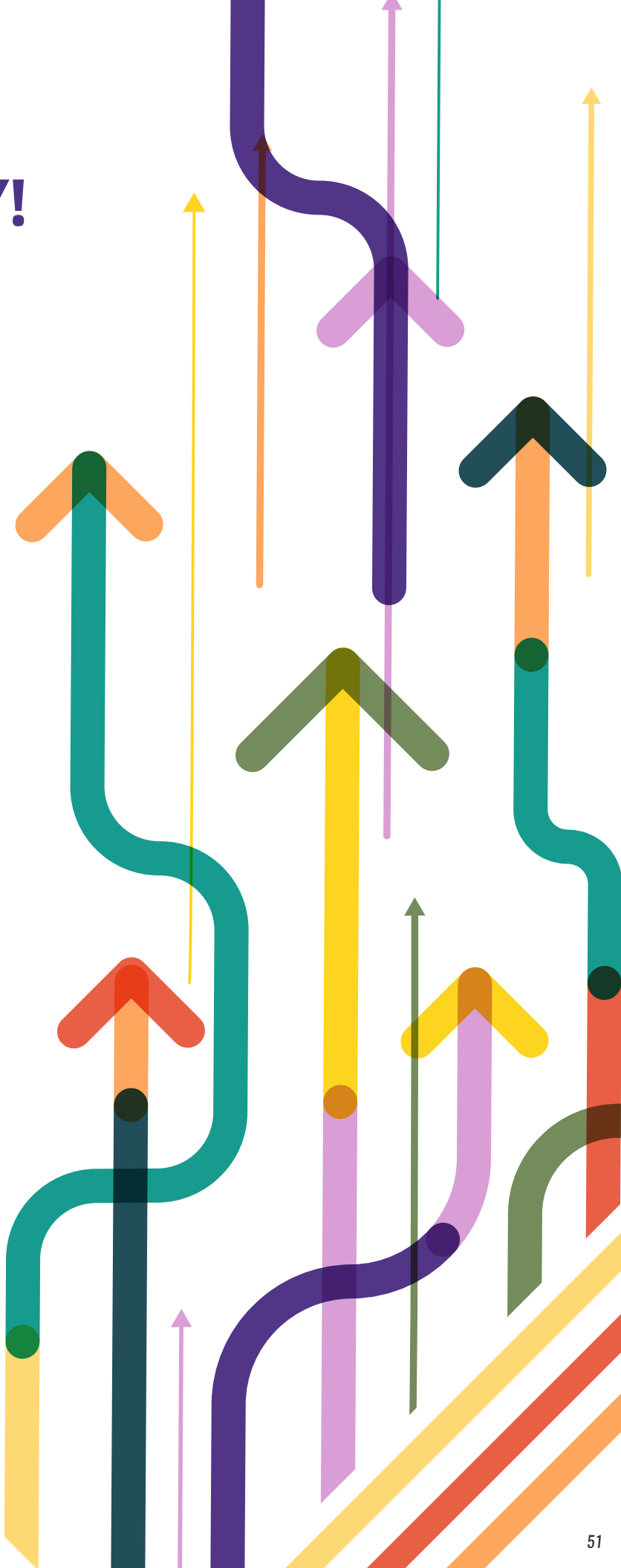
The COVID-19 pandemic showed us all why we need standards. International standards were created for the purpose of creating a common language for organizations and individuals alike. This year, we honor the experts worldwide who develop and make International Standards possible.

Developing a sustainable economy, address inequalities and, slow climate change are all included in the Sustainable Development Goals (SDGs). But to achieve those, we must all do our part to help.

World Standards Day 2021 theme is a shared vision for a better world, and now more than ever the world needs all of us to join and work together for a better future.

PECB offers training courses that reflect the latest standards, technologies, approaches, most innovative methods, and practical examples.

Browse through the PECB page and find the one you need.



How can AI be used to Automate Ethical Hacking

BY MARIO BOJILOV

Digital Technology use has been steadily rising over the last decade, but COVID-19 significantly accelerated this trend. Due to widespread lockdowns, leading to a rise in "work from home" arrangements, companies and individuals were forced to use digital solutions on a never-before-seen scale. For example, before COVID-19, Zoom, one of the leading videoconferencing apps, had 82,400 business customers. In 2020, its business customers increased to 470,100, an increase close to 600%. Similarly, neobanks – financial institutions not previously connected to banking infrastructure, are projected to increase their revenue from $3.6Bn in 2020 to $6.8Bn in 2021.

Unfortunately, the increased use of digital technology provides opportunities for legitimate businesses and malicious actors, such as large cyber syndicates, individuals, and small criminal groups. According to ScamWatch, an initiative of the Australian Government, in 2019, there were 53,882 reported attempts for stealing personal information. In 2020 the number rose to 82,182, while for just the first eight months of 2021, the number is 81,618. Malicious actors are targeting not just individuals but also organizations. The Internet Crime Complaint Center reported one successful attack every 1.12 seconds in 2020. At the same, CyberEdge Group says 86.2% of surveyed organizations were affected by a successful attack.

Considering the above statistics, it is easy to understand why individuals and senior managers in various organizations are very concerned. As a result, the budgets for managing digital risks have increased together with the number of approaches in fighting cyber-crime. These approaches include employee training, changes in policies and procedures, and increased use of ethical hacking.

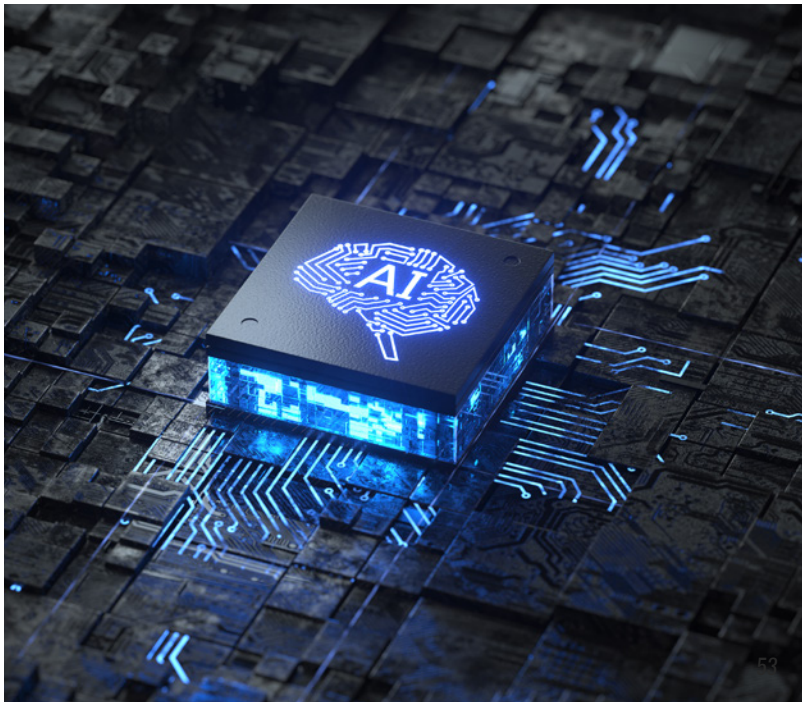
An introduction to cybersecurity and hacking

Ethical hacking involves trained cybersecurity professionals carrying out activities to penetrate an organization's cybersecurity defenses with the organization's permission. These cybersecurity professionals are also known as “white hat hackers”. The white hat hackers use the same skillset, approaches, and tools as the black hat hackers. The main difference between the two groups is motivation and intent. Black hat hackers carry out their activities with malicious intent. When a black hat hacker discovers a vulnerability, they exploit that for their gain. Their motivation can be financial, political, or a combination of these. White hat hackers are employed by an organization. While they usually work undercover to obtain a more accurate picture of the situation, their intent is not malicious. Any vulnerabilities discovered by white hat hackers are reported back to the organization to be promptly addressed. White hat hackers sometimes are also known as penetration testers.

The approaches used by all hackers include no-tech, low-tech, and high-tech activities. No-tech activities include shoulder surfing, social engineering, and dumpster diving. A hacker will try to gain valuable information like passwords or personal details during shoulder surfing by glancing inconspicuously at someone's screen. Dumpster diving involves going through rubbish containers and finding valuable documents that were thrown out instead of being shredded. Finally, using social engineering, a hacker pretends to be someone they are not to get sensitive information from another party. One of the best-known hackers, Kevin Mitnick, used social engineering extensively in his pursuits.

Low-tech hacking involves limited and very often ingenious use of simple technology or gadgets. Examples of low-tech hacking include using aluminum strips from cans to pick locks; standard utilities like ping to see if a specific network address exists and accepts connections; or Google Hacking, where common Google queries are enhanced to provide additional information to hackers.

High-tech hacking, while usually complemented by no- or low-tech activities, is decidedly different. This type of hacking involves the use of various tools to automate and enhance the discovery of vulnerabilities and exploiting them. Examples include: installation of various types of malware like rootkits - software providing the highest level of privileges; ransomware - programs blocking device or data access; and botnets - computer networks used to send spam or mount distributed denial-of-service (DDoS) attacks.



An introduction to artificial intelligence

Considering the vast array of constantly evolving approaches and tools used by cybercriminals, it is logical to assume that at least the same level of innovation is required in the fight against cybercrime. One of the technologies steadily rising in popularity amongst ethical hackers is Artificial Intelligence (AI). The main goal of AI is to mimic the behaviors of a human. These include the capability to generalize, learn, and constantly adapt.

Some examples will make the above points more straightforward. For instance, when a human sees digit '1' written in different ways, as shown in figure 1, they will recognize it 98% of the time. The same set of digits, however, will look like five different objects to a software program. We see the same thing because of our ability to generalize, derive characteristics and classify objects based on our earlier experience.

Figure 1. A set of handwritten digits '1'

Humans also constantly learn and adapt their behaviors. For example, if a child starts eating hot cereal and burns their tongue slightly, the child will start waiting until the cereal cools down after several such occurrences. In the process, the child will begin grouping or clustering in AI parlance objects into hot and cold and respond appropriately.

However, what seems natural to us is anything but to a computer. Replicating human behavior within a computer system is what AI aims to achieve. AI as a field of research and implementation has been around since the mid-1950s. With big hopes and promises, academics, programmers, and engineers worldwide have worked tirelessly to advance AI and make it applicable in everyday activities. This endeavor was not straightforward and contained numerous ebbs and flows. Over the last ten years, the revival of AI applications has been due to the increased computing power available, mainly because of cloud computing advances to individuals and organizations.

Current AI technologies are based on several approaches contained within each other, as shown in figure 2.

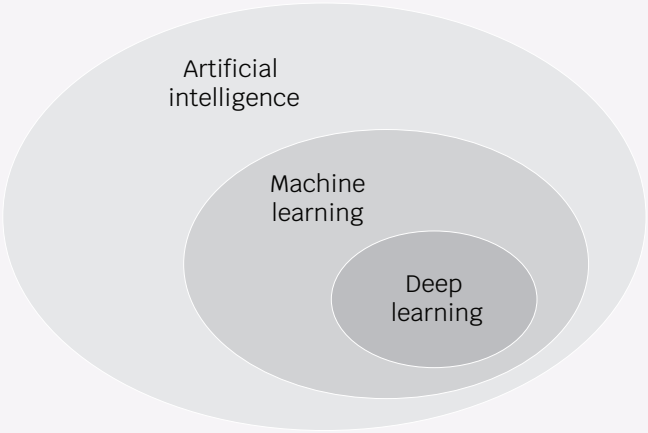


Figure 1.1 Artificial intelligence, Machine learning, Deep learning

(Source: Deep Learning with Python)

Machine learning is one of the most popular types of AI currently in use and includes discovering patterns within datasets. It is a bottom-up approach because a problem is not entirely defined, but it is up to the system to identify missing relationships and patterns. Two of the most widespread machine learning technologies are decision trees and neural networks.

Deep learning is gaining popularity but is still in its infancy. It is a specific type of machine learning, neural networks, and is based on the idea that including additional layers in a neural network will improve its capabilities.

Deep learning became feasible because of the significant increase in available computing power in the last several years.

Artificial intelligence is the broadest concept and, in addition to machine learning and deep learning, includes technologies like expert systems, search engines (Google), speech recognition (Alexa, Siri), etc.

Using artificial intelligence in ethical hacking

As mentioned above, three key characteristics of AI are the ability to learn, the ability to adapt, and the ability to generalize. These characteristics make AI a necessity in ethical hacking activities. The main reason behind this is that black hat hackers constantly change their strategies, tactics, and actions. In turn, white hackers need to adapt to identify issues and vulnerabilities and address these continuously. Here are some examples of how ethical hackers can use AI.

Analyzing user activities

One of the activities ethical hackers do is send phishing emails to all employees to test their awareness and attention. Hackers widely use phishing emails to obtain sensitive information or to gain unauthorized access to a system. A phishing email entices users to click on a link or visit a web page through promises, threats, or both. Once they do that, either a piece of malware is installed and executed, or confidential information is requested.

When a phishing awareness campaign finishes, user responses are analyzed, and policies and procedures are adjusted accordingly. By using machine learning, specifically decision trees, ethical hackers can identify the characteristics of users more likely to become victims of phishing and, therefore, represent a high risk to the organization. For example, employees from specific departments, particular age groups, or certain educational backgrounds may be twice more likely to be deceived than the rest of the organization. In such cases, these employees will have to undergo additional training to reduce their susceptibility to fraud.

Identifying new attack patterns

All computer networks management tools currently include a logging mechanism. Log files are rich information sources that record and show user activities, network access attempts, system, application issues, etc. When a successful attack occurs and is subsequently detected, its characteristics, such as origin, time, type of hardware, and others, are recorded in the log files. By analyzing those attacks using decision trees, a kind of machine learning, ethical hackers can identify specific vulnerabilities and address those.

For example, if all successful attacks on a network originate in Sierra Leone, a recommendation would be to restrict all traffic from Sierra Leone in some way. Of course, this is an oversimplified example, but it demonstrates how the approach works in an actual situation. Due to its effectiveness, this type of analysis is already part of all popular intrusion detection systems (IDS).

Increasing cyber defense accuracy

It is a well-known fact that no cyber defense is 100% effective. There always will be cases when legitimate access is classified as hacking and blocked; so-called false positives or actual intrusions are allowed through – false negatives. Over time, these occurrences accumulate, and a library of them exists in an organization. By using neural networks, a type of machine learning, it is possible to build and train a parametric model of an intrusion. Afterward, the neural network will automatically classify network access as legitimate or not, improving the overall accuracy of ethical hackers' activities.

In addition, a system based on neural networks will be highly adaptable. This adaptability will be achieved by including all the new mistakes in a training dataset and training the neural network again. This approach is valuable since black hat hackers are constantly changing their actions, and ethical hackers are doing the same to remain effective.

Mario Bojilov
CEO of Meta Business Systems,
Lead Instructor at MBS Academy

Mario Bojilov is a Certified Information Systems Auditor and a Lecturer in three major Australian Universities. He has worked in Data Analytics and Business Improvement since 1994. Mario founded Meta Business Systems (MBS), incorporating MBS Academy, in 2004, where he is currently the Chief Executive Officer. The company focuses on business improvement, performance monitoring, and technology governance.

Over the last 15 years, Mario Bojilov and MBS Academy have taught 1,500+ university students and 450+ professionals in the areas of Finance, Digital Technologies, Digital Risk, and Audit. In addition, the company delivered industry training in Australia, South-East Asia, and the Gulf.

PECB CMMC Foundations

Show your attitude for success! Get the PECB CMMC Foundations Credential!

The CMMC Foundations training course is ideal for individuals interested in learning about the principles of the CMMC model.

This training course will introduce you to the core concepts of the model and teach you how to implement and manage it efficiently. With this training course, you will be able to foster a culture of cyber resiliency efficiently.

PECB CMMC Foundations Training Course offers you:

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

Now is the best time to begin!

LEARN MORE

Lead Cloud Security Manager training course

Ensuring security and compliance and minimizing risks within the cloud computing environment is a challenge that many organizations face.

Do you want to help your organization minimize those risks and ensure their security?

Take our Lead Cloud Security Manager training course and get your certification now!

GET IN TOUCH WITH US!

EXPLORING THE CAPI

STOCK

TAL OF SCANDINAVIA

KHOLM

With world-renowned culture, history, and an abundance of outdoor activities, tours, restaurants, and cafés, Stockholm is an impressive place that will make you want to return again and again. Made up of fourteen islands between the Lake Mälaren and the Baltic Sea, it is a charming city and it is no wonder why it is a favorite travel destination, which manages to satisfy both corporate travelers, as well as tourists.

Getting around Stockholm

Stockholm has an excellent public transport system, so by metro, bus, and/or tram, it is easy to access most areas of the city. One of the popular options for getting around is biking, considering that the city has numerous bike lanes and paths.

If you are planning to stay a little longer you can buy the Stockholm Pass, which comes in four variations - 1, 2, 3, and 5 days. This pass is a good value because it also covers around 60 attractions that you can visit.

Where to stay

There are a lot of great places and neighborhoods to stay considering that Stockholm is made up of 14 islands, and each of these areas has its own unique feel and attractions. As long as you are staying in any central areas you will be fine. However, some of the best areas recommended are Kungsholmen, Östermalm, and Södermalm, as they have great access to all the typical business districts of the city.

Radisson Blu Waterfront Hotel – With minimalist Scandinavian style rooms and freshly renovated bathrooms, the hotel is known for its convenient location since it is located in the heart of the city, right next to the Congress Centre and Central Station. Enjoy a better experience by upgrading to a business room for better views, a Nespresso machine, and a host of extras that make all the difference.

Nobis Hotel - Accommodated in two stylish 19th-century buildings on Norrmalmstorg Square, the hotel is located in a perfect location next to main shopping districts and restaurants. The famous attractions, The Royal Palace and historic district of Gamla Stan, are less than a kilometer away. A must-visit is The Noi restaurant which offers delicious food and a cozy atmosphere, as well as the Gold Bar for great snacks and cocktails.

Where to eat

There is a huge selection of good restaurants, starting from traditional Swedish dishes to Michelin-starred restaurants, so it is difficult to choose a favorite restaurant. Known for its innovative culinary scene, everyone can discover a delicious restaurant for their taste in Stockholm.

Something that should not be missed is to have the *fika* which is an important part of the Swedish culture. It means having a coffee or tea break with cinnamon buns. To some it might be just a coffee break, however, to Swedes it is much more than that.

A great place for the *fika* is **Under Kastanjen**, located in the Gamla Stan, Stockholm's Old Town, under a chestnut tree with both an indoor and outdoor seating area. It is a lovely cozy coffee with amazing pastries and a calm and peaceful atmosphere.

Ekstedt is a Michelin-starred restaurant with an innovative menu, which perfectly blends the Swedish cuisine with modern flavors with dishes prepared in its wood-fired oven and fire pit. The restaurant has a traditional Scandinavian interior. You can take a single fixed menu each night—either 3-courses or 7-courses. In addition to the menu items, though, several other pre-dinner bites and dessert treats are also served.

Wedholms Fisk is the place if you are looking for the finest seafood. You can choose between the ever-changing weekly lunch menu, à la carte, and Wedholm's Tasting Menu. We suggest that you take the 6-course Wedholm's tasting menu together with the wine pairing. The ambiance is quiet and refined and the whole experience is quite unforgettable.

It has an interesting architecture, an impressive grand hall, lots of historical objects and artworks, and highly ornamented rooms. Take a guided tour to learn about the history of the palace and the royal palace and to see the main rooms.

Another city experience not to be missed is a visit to the magnificent **Storkyran Cathedral**. Dating back to the 13th century, the cathedral is located in the Old Town, in between the Royal Palace and Stortorget. It has a gorgeous interior and a fascinating history. The statue of Saint George and Dragon makes the cathedral even more special.

A Scandinavian experience is not complete without enjoying its unique landscape. If you are staying in Stockholm for a shorter period, go for a ferry tour around the Stockholm Archipelago on an excursion that includes Fjäderholmarna, Vaxholm, Gustavsberg, and Värmdö.

These are within an hour's reach from downtown Stockholm and are easily accessible by local transportation or ferry.

Got extra time during your business stay?

If you have come to the city for a conference or a training event and if your schedule allows, we suggest that you extend your stay and explore Stockholm on your own time.

Gamla Stan is the charming old town island of Stockholm and it's a go-to destination. Walk through the narrow cobbled streets and enjoy the numerous hidden gems in history, coffees, and shops. One of the cafes you should not miss is the little café Fika - a lovely place with pastries.

The Vasa Museum is a 17th century ship which sank at the bottom of the archipelago. The ship is very impressive to see. The tour guides are great and the explanations are available in several languages. This is an unforgettable experience that should be on everyone's bucket list.

The Royal Palace is a beautiful palace on the edge of Gamal Stan with around 600 rooms.

Business

Stockholm is the largest Swedish city and the center of equality, innovation, and sustainability, and is continuously ranked as one of the most business-friendly countries in the world. Being a business hub, it is known for its stable economy making it a great place for companies who are interested to expand.

According to the World Bank's Doing Business report for 2020, Sweden is ranked in the 10th place out of 190 economies for ease of doing business. In addition, the nation is known for the lowest corporate taxes in the EU.

Known for its dynamic business climate, Stockholm enables everyone from startups to large corporations to fulfill their full potential. Being home to world-known companies such as Ikea, Volvo, Ericsson, and H&M for a start, the city become a popular destination for international business travelers.

The “ISO 22301:2019 Auditing Guide” eBook is here!

Do you want to understand the role of an auditor in a Business Continuity Management System audit?

PECB recently launched the eBook – ISO 22301:2019 Auditing Guide: A simple and practical guide to auditing a Business Continuity Management System (BCMS).

This guide provides the fundamental audit concepts and principles, and it aims to enable readers to understand the role of an auditor and can be used as a tool when conducting a BCMS audit.

BUY IT NOW

Expected Changes in the Newest Version of the ISO/IEC 27002 Standard

In a world where data security is essential for every organization, the implementation, and management of information security is highly important. The ISO/IEC 27002, together with ISO/IEC 27001, and ISO/IEC 27002, serves as the foundation for developing a privacy information management system (PIMS).

The ISO/IEC 27002 is currently under review at the DIS (Draft International Standard) stage. What are the key changes expected to be in this new version as compared to ISO/IEC 27002:2013 version?

12 new controls will be introduced, that will reflect the evolvement of technologies and industrial practices.

Existing controls will be regrouped into four categories instead of 14. In addition, the total number of controls in the DIS version will be reduced to 93 compared to the 2013 version, where they were 114 controls.

You can read more about the new expected changes by clicking **here**.

An ISO/IEC 27002 certification shows that you are able to:

- Implement, manage, and maintain the information security controls
- Support an organization in effectively implementing the ISO/IEC 27001 requirements
- Enhance security awareness within an organization
- Enhance organizational reputation

PECB is updating both the ISO/IEC 27002 and ISO/IEC 27001 training courses to reflect the changes in the standard.

Follow us on **LinkedIn** or **Facebook** to stay updated with the latest changes that come out, or contact us at **marketing@pecb.com** for more information on our **ISO/IEC 27002 training courses**.

Ethical Hacking Essential Reads

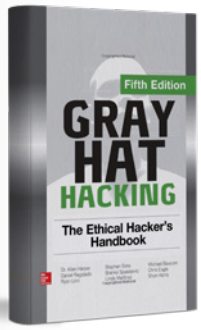
A profession that used to have a bad reputation in the past is now increasingly becoming one of the most wanted and highest paid jobs in the market. While in the past, hackers were often persecuted and risked jail time when caught, nowadays, big companies are hiring skilled hackers to break into their system and expose the flaws before the bad guys get to it.

Check out the most helpful books that offer a better understanding of how it is all connected, how it works, and why you should care to know in the first place.

RTFM: Red Team Field Manual By Ben Clark

The Red Team Field Manual (RTFM) is a definite must-have in your backpack if you are a Red Team Member, who is constantly undertaking tasks without Google or has no time to scan through pages. The RTFM contains the basic syntax for commonly used Linux and Windows command-line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. Having this manual will save you the time of looking up Windows nuances such as Windows *wmic* and *dsquery* command-line tools, key registry values, scheduled tasks syntax, startup locations, and Windows scripting.

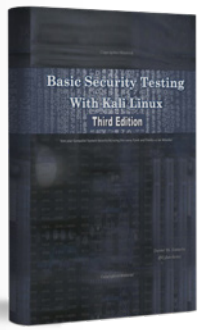
RTFM is rated as one of the best manuals and is so highly recommended by all experts, it should teach you some new red team techniques that are guaranteed to come in handy.



Gray Hat Hacking: The Ethical Hacker's Handbook by Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, Linda Martinez, Michael Baucom, Chris Eagle, and Shon Harris

Gray Hat Hacking: The Ethical Hacker's Handbook is a deep and detailed book meant for readers who want to understand the inner workings of Windows and Linux-based systems and the tools and techniques needed to secure them. The book covers the main hacking concepts, social engineering, physical security, network security, and it illustrates it all with virtual examples and potent tools that are sure to be helpful to all readers.

Rather than just focusing on the software tools, the authors emphasize the importance of understanding how systems operate and what their vulnerabilities are. Through that, they show how these systems can then be exploited. But more importantly, they detail what needs to be done to secure these systems. This book is a highly technical, hands-on reference to ethical hacking and definitely a valuable resource for security professionals to use to secure their networks.



Basic Security Testing with Kali Linux, 3rd Edition by Daniel W Dieterle

Every ethical hacker and security professional is familiar with the Kali Linux 2 (2016); the platform that allows them to use the same tools and techniques that a black hat would use, and that enables them to find security issues before the bad guys do.

Though there is no such thing as a completely "Hacker Proof" computer, knowing how a hacker operates is certainly helpful to get on the right track of securing your network! If you want to learn the basics of how hackers find out information, weaknesses in your security, and how they gain access to your system, then this book is the one you'll need.

Malware Analyst's Cookbook: Tools and Techniques for Fighting Malicious Code by Michael Ligh

As we continue to depend more and more on computers, the risk of malware increases along with it. This book is the perfect guide to find the solutions to various problems you might come across.

A how-to book for fighting malicious code and analyzing incidents written by field experts, this manual will help security professionals classify malware, understand packing and unpacking, dynamic malware analysis, decoding and decrypting, rootkit detection, and more. It also includes generous amounts of source code in C, Python, and Perl to extend your favorite tools or build new ones. Malware Analyst's Cookbook is essential to malware researchers, IT, forensic analysts, incident responders, and security administrators.

The Role of the Human Factor: Social Engineering

BY JAN CARROLL

In cybersecurity, humans are often seen as the weakest link, as attackers use social engineering techniques to infiltrate organizations, so they can launch ransomware or cause a data breach. According to the ENISA Threat Landscape 2020, 84% of cyberattacks rely on social engineering.

So what can we do to protect against the human factor? Well, we all have a part to play in order to flip our role from being the weakest link, to becoming the strongest defense in our fight against cyberattacks.

NIST SP 800-63-3 defines social engineering as "the act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust." Attackers use different methods, tools, and tactics to deceive, ranging from spamming emails, to very personalized and targeted attacks on particular individuals.

Phishing attacks and social engineering may target anyone. As such, we need to be aware of the risks of such threats. If your social media is hacked, there could be a message sent to all your friends or contacts, from you, which includes a malicious link. To mitigate such risks, it is recommended to comply with strong password policies.

COVID-19 changed the theme of phishing emails, but not the methods. The attacks still preyed on human nature and psychology to manipulate individuals into doing something or revealing information that would compromise the security of their organization.

The types of malicious actors who use phishing techniques are opportunists and will adapt the attack for different situations, individuals, and current events.

Social engineering methods:	
Pretexting	Attackers use a pretext or a backstory to build rapport with the victim and gain their trust, so they can manipulate the victim into carrying out a required action.
Baiting	Attacker entice the victim into carrying out a required action by offering easy access to something that the victim wants. An example would be sending an infected USB to a victim through the mail, masquerading it as free marketing material from a known vendor.
Shoulder surfing	The victim is observed over the shoulder by a person or a camera. The attackers steal sensitive information such as passwords, PINs, etc.
Tailgating/ piggybacking	The attacker follows an authorized person into a building (often an employee or delivery person). The attacker exploits the politeness of the authorized person. The victim holds the door for the attacker, as it can be considered rude not to hold a door open for the next person.
Dumpster diving	The attackers search sensitive information which could be used in a cyberattack within a victim's domestic or business waste. That's why it is so important to shred sensitive documents.

What is phishing?

Phishing is a tactic to persuade victims to reveal sensitive information or carry out an action. Usually involves a combination of social engineering and deception. Attackers use different methods for phishing attacks, such as email, text, phone calls, URL redirects, and social media. Often these attackers await for the victim's response so will communicate in real time often impersonating a person known to the victim.

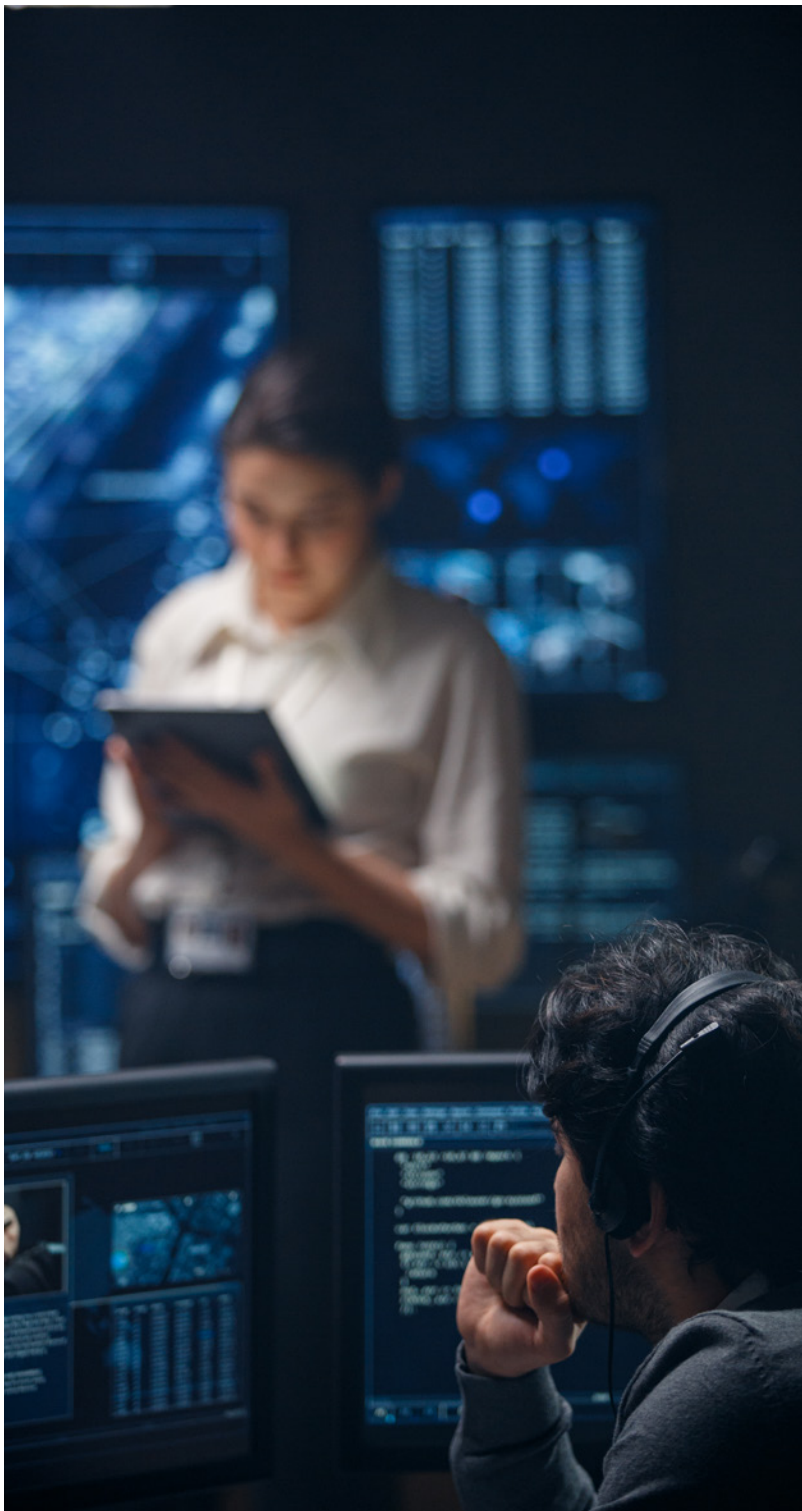
An example of a phishing attempt is that convincing email from your energy service provider telling you that you will be cut off if you don't pay in the next hour.

Other examples would be an SMS text message from a courier for an upcoming delivery, or even a phone call from your work IT Department asking if you recently changed your password. While social engineering and phishing attacks are getting more advanced and sophisticated, the good news is that there are certain flags we can look out for to protect ourselves.

Types of phishing	
Pharming	Attackers use a cloned website to retrieve login details.
Spear phishing	Such attacks are targeted phishing attempts. The message will be personalized and likely will appear to be from someone the victim knows.
Whaling	A targeted phishing attack on a senior-level executive.
Smishing	An SMS/text phishing attempt which includes malicious links or app downloads.

How to spot a phishing attempt

Most of us can identify the obvious bad spelling and outlandish stories, however, we recommend to trust your instinct too and look out for these red flags:



How to spot a phishing attempt	
Urgency	Urgency is a key element often used in phishing attempts. The attacker wants you to act before you think. If you cannot check with the sender, take 20 minutes before acting on such an email.
Unusual requirements	If you receive a message which requires you to do something, ask yourself the following questions: Would this person usually require such a thing? Is the person requiring something from you following the usual processes and procedures? Am I being asked to ensure discretion?
Authority	If you receive a request from a person appearing to be from a higher rank, ask yourself: Is this person exerting their authority or 'pulling rank'? This may be especially evident if the victim is reticent in carrying out what the attacker wants.
Consequences	Phishing attempts often use the element of consequences. Messages from attackers often state that if the victim does not comply, there will be negative consequences. In addition, there are also cases where attackers use positive enticements.
Praise and flattery	Attackers also use praise and flattery to build rapport and psychologically make the victim more cooperative and likely to carry out the intended action.
Reciprocity	If you do this for me, I'll do something for you. The attacker may claim that they have already done something for you, and you owe them.
Social Proof	The attacker tries to persuade the victim to fulfill a request by implying that 'everyone else' is doing it. The victim often does not want to be the odd one out or the 'difficult' person, and falls into the social proof trap.
Too good to be true	As the old saying states "If it seems too good to be true, it likely is." We cannot win competitions we do not enter. Be aware of messages that claim that you have won a reward.

Preventing social engineering attacks

Preventing social engineering attacks requires a combined effort of people to implement processes and ensure technical support as much as possible. Implementing administrative, physical, and technical controls does not suffice, organizations must also fill in the gaps with training to raise the awareness of employees regarding social engineering attacks. The best social engineering attackers will manipulate humans to override the controls in place. As such, to prevent social engineering attacks, organizations must take preventive measures for the following:

Preventing social engineering attacks	
People	Employee Buy-in Employee Awareness Cybersecurity Training Cybersecurity Policies
Process	Incident Planning and Responses Password Policies and implementing MFA
Technical	Network Security Security Monitoring

Security Culture

In organizations, a security culture is one of the best methods of minimizing the impact of attacks and increasing your organization's security posture. Maintaining a security culture in an organization means that cybersecurity is everyone's problem, not just a problem of the IT team. While the CEO is ultimately responsible for the security of the organization, everyone within the organization or interacting with the organization can do their part. Make security awareness engaging and reward employees for doing the right thing regarding security.

Training and awareness

Regularly conduct relevant training and awareness sessions for everyone in the organization. Ensure your employees are cyber aware citizens, as attackers do not clock off at 5 p.m., so employees should be aware of cybersecurity risks even after they leave the organization.

Employees should be aware of phishing attacks and social engineering attempts that target them, but also the organization where they work. This ensures that individuals are cyber aware all the time and extend that awareness to their families and communities, which in turn, makes the whole society safer from cybercrime. There are resources from organizations such as the Cyber Readiness Institute which provides training regarding passwords, phishing, updates, and removable media. Such trainings can be an excellent starting point for employees on their cyber awareness journey.

No blame

There should be no negative consequences if an employee suspects that an email may be a phishing attempt and they make the call to verify. On the contrary, this practice should be encouraged and rewarded. Likewise, if a client is contacted to verify a change of bank account request, this should be seen as evidence of how seriously the organization takes the client's business. If an employee does click on a malicious link, there should be no negative consequences, and it should be treated as a learning opportunity.

How can I support my team?

To become a cyber champion and reinforce cyber awareness training among your team, you do not need to hold a technical role. A passion for supporting your team and doing your part in your organization's security culture is enough. Here are some suggestions to improve the awareness of your team regarding cybersecurity:

- Make yourself aware of your organization's cyber incident response plans and ensure your team knows what to do in the event of an attack.
- Integrate cybersecurity on the agenda of all your team meetings.
- Encourage your team to stay up to date with current cyber news and incidents. Your National Cyber Security Centre will send a weekly email alert and offer you advice on dealing with incidents.

Conclusion

Social engineering is an enduring attack vector and it will continue to be exploited as long as it remains a successful tactic for cyber attackers.

The role of the human factor is that we all have a part to play in ensuring that attackers do not use our human nature against us to obtain information and use it for malicious purposes. Rather than seeing the employees as the weakest link which attackers exploit, we need to flip that, and the employees the strongest link.

Through trainings and awareness sessions, organizations must prepare their employees on how to deal with cybersecurity issues, as they are often the first line of defense when facing cyberattacks. With constant support, a security culture, and training, employees will get more adept at recognizing, impeding, and preventing social engineering attempts of malicious actors, thus maintaining the security posture of their organization.

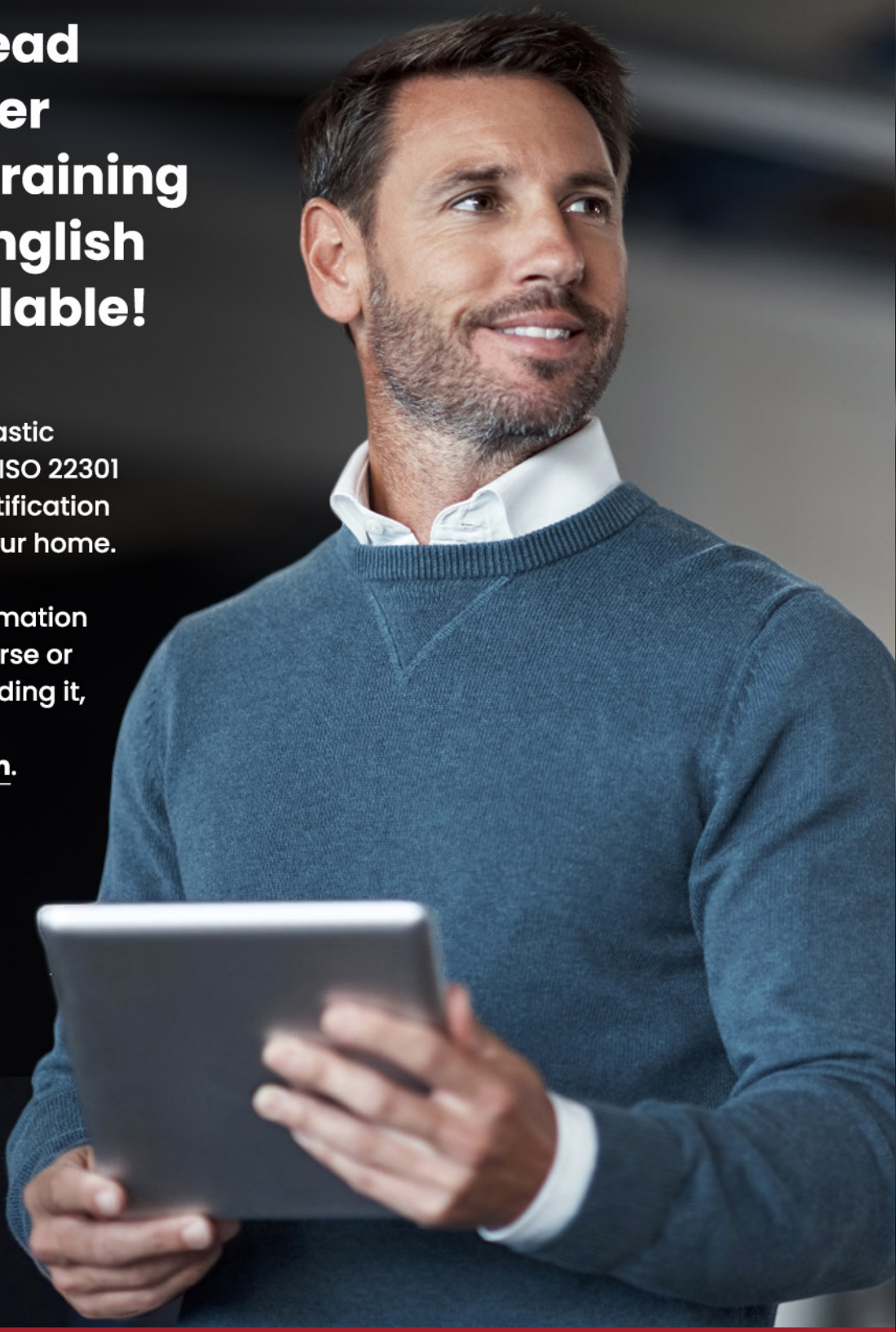
Jan Carroll
Lecturer and Course Creator at UCD Professional Academy

Jan Carroll is a lecturer and course creator at UCD Professional Academy and budding entrepreneur (Fortify Institute). Jan has a passion for teaching and learning, and is relentlessly working to close the cyber skills gap by encouraging more women and underrepresented groups into the security industry.

Jan holds an MEd and MSc in Cybersecurity and is an unceasing student who loves nothing more than adding another certification, qualification, or credential to her collection. Jan works with SMEs rebuilding and securing their businesses after the impact of COVID-19, and mentors women who, like Jan, got an interest in the field of information security after the age of 40.

https://twitter.com/ThePlanJan

ISO 22301 Lead Implementer eLearning training course in English is now available!



This is a new and fantastic opportunity to pursue ISO 22301 Lead Implementer certification from the comfort of your home.

If you need more information about the training course or are interested in attending it, please contact us at **marketing@pecb.com**.

PECB eLearning

#BeyondClassrooms

DO NOT MISS
NOVEMBER'S WEBINAR!

The CIA (Confidentiality, Integrity, and Availability) triad is essential in data governance, information security, and privacy. It provides important security features that help organizations avoid compliance issues and reputational damage.

To learn more about the role and importance of the CIA triad, register for our upcoming webinar this November.

Topic: CIA Triad in Data Governance, Information Security, and Privacy: Its Role and Importance

November 17, 2021 at 3:00 PM CET

PRESENTERS

ELENA ELKINA
Partner, Co-founder
at Aleada Consulting

ANTHONY ENGLISH
Director Of Operations
at Big Cyber

REGISTER NOW

PECB WEBINARS

The Impact of Ethical Hacking and Cloud Computing on Businesses

BY CHRISTODOULOS PAPADOPOULOS

Ethical hacking and cloud computing have been continuously developing and improving over the years, and they have become essential services in today's technological and business world.

As millions of people started working remotely during the COVID-19 pandemic, organizations are using the cloud more and more to increase their overall profit. Its importance increased significantly as it enabled organizations to adapt and remain resilient in the new business environment. Businesses can easily access their data from anywhere, and employees have more flexibility and freedom overall, which is something that makes operations run more smoothly. But how secure is cloud computing? Can it be hacked? It is important to note that cloud hosts monitor the security system closely. However, any technology connected to the internet can be hacked. That is why it is important to know how to protect yourself and your organization, to the best of your abilities.

How can a hack occur?

There have been instances where attackers have managed to attack service providers and, as a result, the clients as well. They compromised their accounts using phishing emails, and through that, they gained access to sensitive customer data. If the cloud is hacked, hackers can move from one account to the other, and customers will have little control over the cloud environment. As scary as that sounds just thinking about it, do not get anxious over it because, with the right measures, this is something that can be prevented and contained.

What happens if the cloud is hacked?

Manav Mital, who is a cybersecurity expert, told The Washington Post that even though the cloud is physically more secure, its ease of usage has led to a boom in new applications and databases, as well as increasingly complex configurations, which make it more difficult to manage and monitor. If a cloud configuration is difficult to monitor, there will be more opportunities for vulnerabilities. If more applications are stored in the cloud, more people need access to it.

This way, it becomes easier to grant them that access by unlocking some security tools, such as firewalls. Unwanted individuals can go through these openings with ease, which immediately puts sensitive data at risk. Such security-bypassing cloud attacks have led to breaches at high-profile organizations, including Instagram and Docker Hub, to name a few. However, the cloud has proven more secure and at a lower risk of getting hacked, and it also has the advantage of being able to recover all your data in case of any disaster and perform damage control.

Types of hackers

There are three main types of hackers:

- The white hat hackers
- The black hat hackers
- The gray hat hackers

The white hat hackers are known as the "good guys," who ethically use their skills. They break into a system in order to improve it. This process is also known as penetration testing. White hat hackers are individuals who are contracted by clients to hack into systems while complying with laws, the agreement with the client, and ethical standards. They find vulnerabilities in clients' systems and present them to the client, along with suggestions on how the client can improve their cybersecurity.

The black hat hackers try to maliciously break into a network to collect as much information as possible to cause harm to a person or a company. They attack systems for personal reasons, such as money or prestige. They are skilled programmers and computer experts who search for vulnerabilities and weak points for malicious intentions. Black hat hackers may work alone or within a criminal network.

The gray hat hackers operate as freelancers using their own terms to break into a system and expect reimbursement for their efforts. They break into a system and find a vulnerability without asking the owner of the system. While this act is illegal, gray hat hackers will not use any information to hurt the system or its owner. They do this to solve a challenge, have fun, or even suggest improvements to the owner. Gray hat hackers are not bound to contracts or ethics. They may act illegally if they need to pursue certain goals.

Ethical hacking

Ethical hacking, or in other words, known as penetration testing, is a technique used to detect vulnerabilities, risks, and flaws in a security system, as well as to implement countermeasures against attacks. Ethical hackers are practically authorized to gain unauthorized access to the system or network. They are required to follow specific steps to complete a penetration test, whether that is internal penetration testing, external penetration testing, web applications testing, or Wi-Fi penetration testing.

Ethical hacking is split into three different categories: the white box (known information, provided by the company), black-box (unknown information not provided by the company), and gray box (a mixture of both known and unknown information) before ethical hackers start penetrating any network(s).

It is recommended for organizations to conduct penetration testing at least twice a year to test their security and identify any areas of vulnerability that can be exploited by malicious attackers that seek to cause harm and steal critical information.

Ethical hacking can also contribute to raising the awareness of the employees within the company. Ethical hackers can launch a phishing simulation attack, which is commonly used to trick users to enter their personal information from emails such as credit cards, ID, etc. This will help employees understand how such emails can cause harm from a personal and business-related perspective.

Cloud computing

Cloud computing is related to computing system resources, applications, storage databases, and other systems which handle large amounts of data over multiple locations on the internet. There are four different types of cloud service: Infrastructure-as-a-Service (networking and storage resources), Platform-as-a-Service (provides users with a platform for applications to run), Software-as-a-Service (provides users with a cloud application), and Function-as-a-Service (an execution model to allow developers to build and run applications).

Cloud computing is a pay-as-you-go-service in which organizations only pay for the services they use, thus minimizing the costs and enabling them to run their infrastructure more efficiently. Many businesses utilize cloud services since it enables their employees to work from other geographical locations with a secure encrypted connection. Another major advantage of the cloud from which organizations benefit is the prevention of data loss. On-premises infrastructure has higher possibilities for hardware failures, and this is where the cloud serves as a backup service to provide such capabilities if such a failure occurs. Moreover, disaster recovery can also contribute to the success of a business when there is a downtime of services since it provides efficient data recovery. Cloud also saves time for the IT personnel, which is vital for a business.

Cloud applications update themselves automatically with the latest technology, including up-to-date versions of software.

Both ethical hacking and cloud are important for any industry as they have a huge impact and play a major role in the overall security of an organization. Organizations should hire ethical hackers to find any vulnerabilities in their security and improve their overall security levels. In addition, organizations can further improve their data security by utilizing cloud services to ensure that their data is backed up.

How should you prepare?

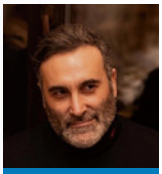
Ethical Hacking and Cloud have also positively impacted Information Security services provision. Here at geevo®, we have already utilized various Cloud technologies to our advantage. geevo® has become a leading Managed Security Services Provider (MSSP), catering to various needs of markets participants, such as NOC/SOC-as-a-Service, IaaS, web application vulnerability assessments, etc.

There are many ways an organization can prepare for such changes. The first thing you must do for your organization is to prepare the right budget and hire professional ethical hackers, as well as cloud services.

Additionally, IT teams must be aware, well educated, and prepared psychologically so that they ensure the businesses reach satisfactory levels of security, following suggested recommendations for Penetration Testing reports, as well as cloud deployment services.

Lastly, it is important to understand that cybercrime is becoming more and more common, especially since two years ago, as more employees now work from home due to the ongoing issues of COVID-19, and therefore, they are exposed to attacks. It is crucial to defend your company's data from external attackers that can lead to severe consequences for both the company and the employees.

Specific improvements can help companies become less vulnerable to attacks and prevent data losses.



in

Christodoulos Papadopoulos
Founder & CEO CPbros Group, geevo®

Chris is an innovative thinker and entrepreneur with broad-based expertise in information security – InfoSec (incl. cybersecurity), data privacy, operations, finance, sales, and business development.

He holds a Diploma in Electrical Engineering from the Cyprus Higher Technical Institute and a Bachelor of Science in Electrical Engineering (specializing in Computer Engineering) from the Budapest University of Technology and Economics. His career has centered on the provision of innovative information technology solutions for various industries holding senior management positions in several firms.

Having 20+ years of post-qualification professional experience, he is an expert in the field of Financial Technologies, Information Security, Data Privacy and Operations, IT Risk Advisory, etc. During his career, Chris has performed various audits of information systems and related processes and review related security policies and procedures.

Currently, he is a certified PECB Trainer, PECB Certified Data Protection Officer (CDPO), PECB ISO/IEC 29100 Lead Privacy Implementer, ISO/IEC 27032 Senior Lead Cybersecurity Manager, and more.

He founded CPbros Group in 2010, with the vision of becoming one of the leading Management Consulting firms in the region.

HOW TO PLAN THE

DUB

DUBLIN TO CARL

ARTICLE BY SIDEWALKSAFARI.COM

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

Carlingford Lough is an area of great natural beauty located less than a 2-hour drive north of Dublin. Spending a weekend in Carlingford town on the Cooley Peninsula is a fantastic way to explore the area. Carlingford walks in and around the Cooley mountains are a major highlight.

Did you know that Carlingford Lough is nestled between the Republic of Ireland and Northern Ireland? This Carlingford road trip covers the drive from Dublin, including stops along the way as well as points of interest on both the north and south sides of Carlingford Lough. Buckle up, and let's get on our way!

Getting To Carlingford Lough with UFO Drive

Carlingford is most easily accessible by car. If you have a car, great! You're ready to embark on your Carlingford road trip. If you don't own a car, you could go with a traditional car hire from the likes of Hertz or Sixt. Alternatively, you could plan to ride in style as we did and rent a Tesla from UFO Drive. UFO Drive operates out of Stephen's Green Shopping Centre Car Park in Dublin City and is entirely app-based.

Create an account, book a car, and then use the UFO Drive app to collect your key and unlock the vehicle. We hired a Tesla once before for a day trip from Dublin to Kildare, but this is the first time we'd used UFO Drive for a long weekend trip.

Our 4-day rental cost approximately 100 EUR a day and included a total of 650 km driving distance. This may sound expensive, but Teslas are electric so you won't need to pay for petrol. Tolls are also included with the rental. This includes tolls on the M50 and Dublin Port Tunnel. We also felt it was worth the splurge for a sweet ride on our first weekend away in quite some time.

Where to Stop on the Way to Carlingford Lough from Dublin

Now that you've got your car lined up, you can discover why getting there is half the fun of any road trip. We planned a few stops on the way between Dublin and Carlingford to make the most of our drive.

Battle of the Boyne Visitors Centre

In 1690 Williamites and Jacobites faced off in the largest battle ever fought on Irish or British soil. William was victorious in a battle that would shape the future of Ireland. Stop at the Battle of the Boyne visitors' center to learn more about this period of history. You'll find fascinating

dioramas, interactive exhibits, and a film that recreates that Battle of the Boyne.

After touring the visitor's center, take a walk in the walled garden.The Battle of the Boyne Visitor Centre is located in the Boyne Valley, which includes attractions like the Hill of Tara, Monasterboice, and Trim Castle.

The combined attractions of the Boyne Valley can also be visited on an organized day trip from Dublin

Blackrock in County Louth

Next up, we stopped in Blackrock, a lovely seaside village in County Louth. Indulge in ice cream from Storm in a Teacup, and then shop for some lovely and local handmade crafts at The Crafty Rock. We picked up some soap and an artsy glass swizzle stick before finishing our visit with a walk by the sea.

Proleek Dolmen

Proleek Dolmen was definitely a major highlight of our Carlingford road trip. Park at Ballymascanlon House Hotel and walk across the golf course following the signs until you reach the dolmen. It takes about 10-15 minutes on a well-marked path.

It was absolutely worth the detour to see Proleek Dolmen and wedge tomb on the way to Carlingford. This is the tallest and most impressive dolmen I've seen in Ireland! Proleek Dolmen is a Stone Age tomb dating back to 2000- 3000 B.C. The capstone weighs 40 tons. Thinking about how the ancient people constructed the dolmen truly captures the imagination.

The grounds and walled gardens at Ballymascanlon House Hotel are also worth exploring on the way back from Proleek Dolmen to the parking lot.

Where to Stay in Carlingford Town

Once you arrive in Carlingford, the next important question becomes: where to stay in Carlingford Town? We booked ourselves a room in the main house at Ghan House Hotel. Ghan House is located in a lush green and walled oasis just outside the gates of Carlingford Town. You can easily walk from Ghan House Hotel to the center of Carlingford Village in less than 5 minutes.

Carlingford can get pretty busy with stag and hen parties on the weekend. If you don't feel like joining in the revelry, make your way back to Ghan House and sip a glass of wine or a gin and tonic by the pond. If it's cold or raining, grab a seat on a couch in the atmospheric front room.

Make sure to take some time to explore the grounds of Ghan House. I found a small staircase covered in weeds that led to a point on the wall with views of Slieve Foye in the Cooley Mountains and Carlingford Lough.

We paid approximately 200 EUR per night for our 3-night stay in Carlingford. We were simply delighted by Ghan House Hotel. Our room was spacious and quiet. I also loved the kitties wandering around outside. I counted at least four during our stay. The Ghan Fry for breakfast is included in your stay and lays a solid foundation for a hike in the Cooley Mountains near Carlingford.

Ghan House is also home to two electric vehicle charging stations which was another reason we chose to stay here. Plug in at night, and you're fully charged and ready to go in the morning.

Where to Eat in Carlingford Town

The next question to address is where to eat in Carlingford Town. Carlingford is pretty small and the main places to eat are clustered around Market Street.

There are a limited number of restaurants to choose from so make sure to book in for dinner somewhere to avoid disappointment.

McKevitt's Village Hotel

We sat down for a couple of pints and some local mussels in white wine garlic cream sauce at Lil's Bar in the beer garden at McKevitt's Village Hotel in Carlingford. The beer garden was a quiet oasis in the heart of Carlingford Town.

Ghan House Hotel

Dinner at Ghan House is an easy choice if you are looking for an upscale meal. On the weekends, you'll get four courses for 55 EUR. Book dinner when you reserve a room at Ghan House Hotel, and you can save a few euros. During the week, the chef offers a 6-course tasting menu for a lower price. We enjoyed a salmon appetizer with beetroot, *feta*, *kadaif* pastry, duck with asparagus, and fondant potato, and pork with Vietnamese flavors.

Feeley's Fish and Chips

There is nothing like fish and chips to invoke a sense of being on vacation in Ireland. In Carlingford, head to Feeley's for fish and chips. Feeley's fish and chips are so fresh and very popular! You can even buy a bottle of their vinegar with your order. Take your fish and chips to go and eat your dinner overlooking Carlingford Lough.

Things to do in Carlingford Town

Base yourself in Carlingford Town, and you'll find a variety of things to do without having to get behind the wheel of a car.

Take a Carlingford Photowalk

Carlingford Ireland is perfect for a photo walk. Definitely take a walk around Carlingford during golden hour for some spectacular photo opportunities. Carlingford is so colorful!

If you really want to have Carlingford to yourself for a photo walk, head into town at 10AM on a Monday morning. You won't be bothered by cars and won't have to contend with people blocking that perfect shot.

Visit Carlingford Priory

Carlingford Priory is pretty marvelous and definitely a sight to behold. Dating back to the 12th century, the ruins are

spectacular on a sunny day. There is even an old mill on an overgrown trail behind the priory.

Watch the Sunset over Carlingford Lough

Time a walk along Carlingford Lough for sunset. The Mourne Mountains across the water in Northern Ireland create a moody backdrop. Look for pale orange rays lighting up King John's Castle.

Carlingford Walks

Pick out a hike to suit your level of fitness. We embarked on the Commons Loop Trail, which takes less than two hours.

This Carlingford walk starts with a vigorous uphill hike from Carlingford Town. We were rewarded with breathtaking views of the Cooley and Mourne Mountains and Carlingford Lough. The Commons Loop Trail threads through a couple of sheep pastures, and we made some new friends along the way, including a curious lamb. We also spotted content cows, chirping stonechats, and a lazy little goat on our Carlingford walk. If you like birdwatching, keep an eye on the bracken (dense ferns) in the Cooley Mountains above Carlingford. You'll be delighted by the little birds you see (like stonechats and goldfinches).

Tour King John's Castle

For a fiver, you can take a 45-minute tour of King John's Castle. Sometimes referred to as Carlingford Castle, you can only get inside the castle ruins by joining the daily tour that begins from the Carlingford Tourism Office. King John's Castle dates back to the Norman period.

Drive the Mourne Coastal Route in Northern Ireland

Carlingford Town is an excellent home base for a drive around Carlingford Lough in Northern Ireland. Hop in the car, and let's explore the Mourne Coastal Route!

Take the Carlingford Lough Ferry to Northern Ireland

Book a ticket for the Carlingford Lough Ferry from Greenore to Greencastle. The ferry departs once per hour, starting at 10:30 AM, and the ride across Carlingford Lough takes about 20 minutes. You can get out of the car and have a look at the surrounding mountain scenery. We even spotted a few dolphins!

Explore Kilbroney Park

Kilbroney Park near Rostrevor is worth a stop on your drive around Carlingford Lough in Northern Ireland. We hiked the Narnia Trail at Kilbroney Park along the Mourne Coastal Route. C.S. Lewis credits the area as the inspiration for Narnia. There is also a lovely Fairy Trail along a babbling stream.

Tour the Quotes in Rostrevor

Kilbroney Park exits into Rostrevor, which is just the cutest town. Not only did it inspire C.S. Lewis' Narnia, but it also has fabulous doors.

I loved all the inspirational quotes posted around Rostrevor by Poetic Action Rostrevor. For example: "Sometimes we win, and sometimes we learn".

Visit Ross Monument

There is a well-placed parking lot on the water just across from a giant obelisk between Rostrevor and Warrenpoint in Northern Ireland. Pull over and check out the ostentatious Ross Monument.

Ross Monument was built in honor of Major General Ross, whose claim to fame was burning down the U.S. president's house (this act pre-dated the White House) and inspiring the American national anthem during the War of 1812.

Grab a Coffee in Warrenpoint

Warrenpoint is a good stopping point on the Mourne Coastal Route for a coffee. Get a cappuccino to takeaway at Fulla Beans and then walk along the shore and through the park, which is home to a gorgeous Victorian-era bandstand.

Stop at Narrow Water Keep

What have we here? Narrow Water Keep guards the entrance to the Newry River about a kilometer from Carlingford Lough. There is also a cool round tower across the river.

Victoria Lock and the Greenway

On a whim, we pulled in at Victoria Lock and discovered the Greenway in the middle of the Newry River. The views were simply idyllic. Catch a glimpse of the Cooley Mountains as you walk the gravel path. We spotted an adorable wren singing a sweet song on the Greenway near Victoria Lock.

Go for a walk on the Greenway to stretch your legs after a day of driving around Carlingford Lough.

Omeath

Last stop of the day before returning to Carlingford: Omeath! Omeath is back in the Republic of Ireland. We enjoyed views of Warrenpoint in Northern Ireland from across Carlingford Lough. We grabbed a sneaky pint of Guinness at Hotel Granvue and picked up a delicious slice of strawberry cheesecake at Cafe Rosa. Note that while we visited Omeath by car, one of the most popular outdoor activities on the Cooley Peninsula is to cycle from Carlingford to Omeath along the Carlingford Lough Greenway.

Where to Stop on the Return from Carlingford Lough to Dublin

If getting there is half the fun, why not make the return trip from Carlingford just as awesome? There are lots of fun and historic sites to see on the drive from Carlingford Lough to Dublin.

Castle Roche

Castle Roche is a great stopping point on the way from Carlingford to Dundalk. The castle is easy to spot on a hill, but it's on a tiny road with essentially no parking. There is a small bump-out you can pull into for a few minutes. Make sure to put your flashers on and then walk up the hill and onward through what was once the drawbridge, and transport yourself back to life in the 13th century in your imagination.

Dundalk

Dundalk is the largest town in County Louth. Park in Dundalk (pay and display) on the return from Carlingford for a wee wander around. Highlights include the cathedral, cool and colorful Georgian doors, and the Dundalk windmill. The windmill dates back at least to 1790, but it may have been constructed as early as the 12th or 13th century. Dundalk is also an epicenter of Irish mythology with the great warrior hero of Medieval Irish history, Cú Chulainn, hailing from Dundalk. Dundalk is a great stopping point for lunch. Grab an outdoor table at Cafe Adelphi. We enjoyed well-crafted cappuccinos with a giant chocolate chip cookie with Nutella dollop (I'm a big fan of eating dessert first!) followed by halloumi salad and a falafel wrap.

Dromiskin Round Tower and Monastery

Make time for a stop at Dromiskin round tower and monastery, which dates back over 1500 years. The site has a Celtic cross that was built in the late 800s. The monastery was plundered by Viking and Irish armies in the 10th and 11th centuries.

A Detour to Kells

I'll admit, Kells is a bit out of the way, but is a good detour on your return from Carlingford to Dublin, especially if you want to time your arrival in the capital to avoid rush hour. Kells is about a 45-minute drive (50 km) from Dromiskin and will add about 45 minutes to an hour to your drive back to Dublin over what it would have been if you had skipped this stop.

The abbey in Kells is the namesake of the famous Book of Kells. We saw a really cool remnant of a Celtic high cross. Just outside the cemetery next to the Garda station is St Columcille's House which dates back to the 10th century. Such a sturdy stone house! It's rare to see a house with a stone roof like this in Ireland.

There is an ESB charging station near Supervalu in Kells, so plug in that Tesla and get a bit of juice before setting out on foot to explore the town. There is also a state-of-the-art rest area just a couple of minutes away by car: Park Rí. You'll find a convenience store, fast-food restaurants including the punnily named "Cook of Kells" and clean toilets. Fuel up here for the final leg of your return trip to Dublin.

A university is the beginning of everything you want!

At PECB University you will

- Save time & money
- Advance your career
- Learn from the best
- Practice new skills
- Expand your network

Choose any of the programs and continue your education with PECB University

- Executive MBA Programs
- Graduate Certificates
- Graduate Diploma

Visit **PECB University** to get more information, or contact the PECB University counselor at **university.studentaffairs@pecb.com**.

PECB UNIVERSITY

Recognitionem in Veritate

LEARNING IS THE BEST INVESTMENT!

PECB gives you the opportunity to develop and achieve enhanced qualifications that will advance your career.

Elevate yourself by building on your knowledge with our training courses on multiple fields, including:

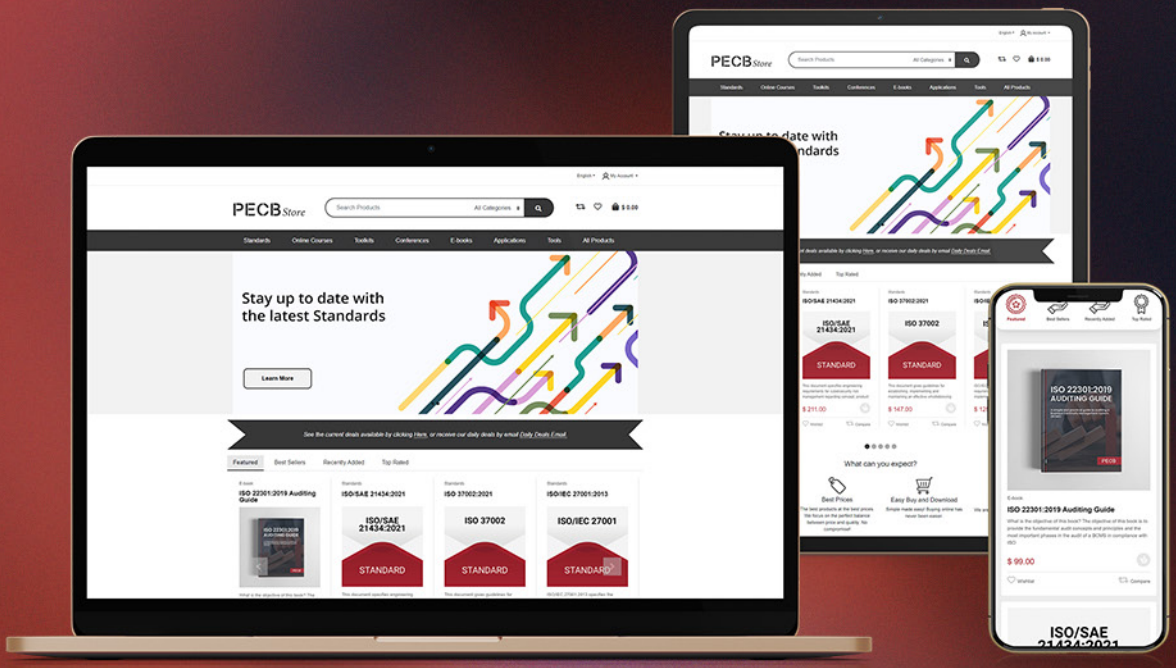
- **Information Security and Resilience**
- **Governance, Risk and Compliance and Privacy**
- **Quality and Sustainability**

Learn more about our training courses!

PECB STORE ANNIVERSARY
2 YEARS WITH YOU!

We invite you to take a tour of the PECB Store and discover the products and tools of the highest quality that we offer.

Everything you need for your path to development and success you can find it here.



Fast service | Affordable prices | User-friendly interface | Convenient

SHOP NOW!

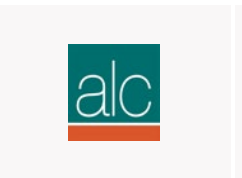
PECB Store

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.

SAFEGUARD YOU DATA SYSTEM

GET IN TOUCH WITH US!

Learn more about our **Ethical Hacking** Training Course