

PECB Insights

ISSUE 43

ISO STANDARDS AND BEYOND

APRIL-JUNE 2023

CYBERSECURITY AND DATA PRIVACY

THE IMPORTANCE OF PRIVACY AND
SECURITY IN THIS DIGITAL ERA

GDPR Turns Five

Blockchain Technology
and Cybersecurity
How It Can Secure Your
Data and Transactions

Emerging Technologies and
Cybersecurity: How It Can
Secure Your Data

The Fundamentals of
ISO/IEC 27032 What You
Need to Know

LEADERSHIP THE STANDARD EXPERTISE TECHNOLOGY BUSINESS & LEISURE CAREER THROWBACK
WORK-LIFE BALANCE INTERESTING FACTS SUCCESS STORY OPINION BOOKS INNOVATION QUESTIONS AND ANSWERS

PECB Insights Magazine

Check out the previous edition

Issue
42

PECB Insights

ISO STANDARDS AND BEYOND

JANUARY - MARCH 2023

INFORMATION SECURITY AND RISK MANAGEMENT

ENSURING SECURITY MEASURES
FOR ORGANIZATIONS

The Rise
of ChatGPT:
Paving the Way for
Large Language
Model Adoption



Ways to Incorporate
Cyber Resilience in Your
Business

How Does ISO/IEC 27005
Relate to Risk Management
Within Enterprise
Networks?

Identifying the
Relationship
between Risk
Management and
Information Security

LEADERSHIP | THE STANDARD | EXPERTISE | TECHNOLOGY | BUSINESS & LEISURE | CAREER
WORK-LIFE BALANCE | INTERESTING FACTS | SUCCESS STORY | OPINION | BOOKS | INNOVATION |

Subscribe & find out more at

www.insights.pecb.com

In This Issue



6 The Standard

How Tech Giants are Building Cyber Resilience

10 The Expert

The IT and Security Leader's Guide to ISO/IEC 27032

14 Technology

Emerging Technologies and Cybersecurity: How It Can Secure Your Data

22 Innovation

Using ChatGPT And Python For Chatbot-Powered eCommerce Websites

28 The Expert

Blockchain Technology and Cybersecurity – How It Can Secure Your Data and Transactions

38 Throwback

Throwback to the First PECB Awards Gala

42 Technology

Dark Data or Data in Darkness

48 Interesting Facts

Interesting Facts on Cybersecurity and Data Privacy

50 Leadership

ChatGPT Draws Privacy Regulator Ban As the UK Government Sees AI as Good for Business

56 Work-Life Balance

The Art of Maintaining a Good Work-Life Balance

62 Opinion

The Fundamentals of ISO/IEC 27032
What You Need to Know

68 Business & Leisure

Tangier, Morocco: The New Eldorado in the African Continent!

76 The Expert

Establishing an Evolving Work Environment Through Security Measures

80 Questions and Answers

ISO/IEC 27001, Cybersecurity, and Risk Management – How to Avoid Data Breaches

90 Books

Gain a Deeper Understanding of Cybersecurity and Data Privacy Through These Books

94 Career

Top Five High-Paying Job Positions You Can Pursue with a GDPR CDPO Certification

96 The Expert

Building Resilience Against Cyber Threats

100 The Expert

GDPR Turns Five

The views and opinions expressed in the PECB Insights Magazine do not necessarily reflect the views of PECB Group.

© PECB 2023. All rights reserved.



Information is the oil of the 21st century, and analytics is the combustion engine. //

PETER SONDERGAARD

Senior Vice President and Global Head
of Research at Gartner, Inc.



How Tech Giants are Building Cyber Resilience

Distrust pushes us into self-limiting stigmas, but International Standards can help us be confidently vulnerable, and resilient.

What do Microsoft, Apple, Google, Intel, and IBM have in common? As well as all being Fortune 500 companies, these tech giants are all using [ISO/IEC 27001](#). With an increasing global uptake and on display at thousands of sites around the world, ISO/IEC 27001 has become the de facto standard for information security management systems.

To protect their critical data assets from digital threats and vulnerabilities, organizations need to adopt a cyber-resilient mindset.

Cyber resilience must be integral not only to technical systems but also to teams, the organizational culture, and daily operations. In fact, business leaders today are far more aware of the cyber threat than the year prior. According to the World Economic Forum's (WEF) [Global Security Outlook 2023](#), 91 % of respondents said they believe a far-reaching and catastrophic cyber event is "at least somewhat likely in the next two years".

Companies worldwide have responded to the pressures by implementing [ISO/IEC 27001¹⁴](#), the world's best-known standard for information security management systems (ISMS). It is a documented set of policies, procedures, processes, and systems that manages the risks of data loss from cyber-attacks, hacks, data leaks, or theft. "Organizations need to adopt a cyber-resilient mindset."

What is cyber resilience?

Cyber resilience is the ability of an organization to operate in the face of a cyber-attack or other cyber incident. It involves having the necessary technical and organizational measures in place to detect, respond to, and recover from such incidents, as well as the ability to adapt and learn from them to improve future resilience.



“Cyber resilience is what takes over when security prevention measures falter,” says Andreas Wolf, who leads the group of experts responsible for ISO/IEC IT security standards. “In the digital economy, the ability to transcend cyber disruption distinguishes market champions.

Organizations that turn vulnerability into strength will have the confidence to take healthy risks.”

Wolf is no stranger when it comes to security. He and his team are responsible for the new and improved version of ISO/IEC 27001 published in October last year to address global IT security challenges and improve digital trust. It benefits organizations by encouraging them to secure all forms of information, develop a centrally managed framework, reduce spending on ineffective defense technology, and protect the integrity, confidentiality, and availability of their data.

ISO standards and cybersecurity

But resilience doesn't just refer to an organization's internal workings; it must apply across all third-party partnerships and throughout the supply chain. Fortunately, [The Cyber Resilience Index \(CRI\): Advancing Organizational Cyber Resilience](#), also published by the WEF, seeks to serve as a reference framework to provide visibility and transparency on cyber resilience practices across industries, peers, and the supply chain.

The CRI provides public- and private-sector cyber leaders with a common framework of best practices for true cyber resilience, a mechanism to measure organizational performance, and clear language to communicate value. Under the CRI's principles, subsequent practices and sub-practices for healthy organizational cyber resilience is the use of recognized security frameworks and industry standards such as [ISO/IEC 27001](#).

“We can't afford to compromise on cyber resilience in the digital era.”

Vulnerability as a building block for resilience

Being transparent about internal practices and sharing information with competitors and policymakers can make organizations feel vulnerable. But it is this vulnerability that will lead to true collaboration and progress. We can't afford to compromise on cyber resilience in the digital era. There is a business case for it, too. Organizations that adopt cyber resilience through confident vulnerability quickly emerge as leaders in their industry and set the standard for their ecosystem. The holistic approach of ISO/IEC 27001 means that the entire organization is covered, not just IT. People, technology, and processes all benefit. Ellaut

Disclaimer: PECB has obtained permission to publish the articles written by [ISO](#).





PECB Awarded Global InfoSec Award 2023 for Most Innovative Cybersecurity Training

In the competitive category of "Cybersecurity Training," PECB has been recognized for its innovative and cutting-edge approach to education by receiving the "Best Cybersecurity Education Provider Award". This is a testament to PECB's commitment to providing top-notch cybersecurity training that equips professionals with the knowledge and skills they need to stay ahead of evolving threats.

We would like to express our sincere gratitude to all our valued customers. Thank you for trusting us with your cybersecurity training needs, and we look forward to continuing to serve you with excellence.

[LEARN MORE ►](#)





The IT and Security Leader's Guide to ISO/IEC 27032

 BY NAHLA DAVIES

THE EXPERT

The threat landscape is constantly evolving. Cyberattacks are becoming more frequent or more sophisticated, therefore, organizations need to adopt modern practices to manage information security. The globally recognized standard ISO/IEC 27032 provides guidelines for those involved with managing cybersecurity in today's digital era.

The level of safety and security of a company's assets [is critically dependent](#) on the skills of IT and security leadership. Becoming ISO/IEC 27032 certified shows their dedication to implementing cybersecurity best practices that hold up against the complex threats facing organizations today. Plus, the credential also gives aspiring security leaders the tools they need to have a competitive edge against other candidates.

ISO/IEC 27032 was specifically designed for IT and security leaders, but it is also a must-have certification for anyone that needs to improve their security skills.

What is ISO/IEC 27032?

The global standard ISO/IEC 27032 was [developed to outline best practices](#) for different cybersecurity roles, tools, and processes. This includes information security, network security, and critical infrastructure protection. The standard provides a framework that addresses modern security issues, such as establishing trust, exchanging information, and providing technical guidance for system integrations.

Here are some examples of the technical guidance and cybersecurity issues that are addressed under this standard:

- › Social engineering attacks
- › Unauthorized access
- › Malware, spyware, ransomware
- › Preparing for attacks



- › Cybersecurity detection and monitoring
- › Incident response policies
- › Information sharing
- › Coordinating between clients
- › Establishing trust
- › Secure information exchange processes
- › System interoperability requirements

The standard offers detailed instructions [on how to handle incidents](#), develop security policies, and how to implement cybersecurity processes across an organization and its third-party vendors and suppliers.

Why get certified?

Is it enough to read and understand the contents of the standard? Perhaps. But obtaining a certification shows an individual's commitment to security and proves that they have the skills necessary to contend against the cyber threats of today.

Last year, [cyber incidents were up 50%](#) compared to the previous year, but it is not simply the frequency of attacks that is alarming. The vectors that attackers are employing are different now compared to a decade ago. The new generation of cybercriminals is educated and takes a sophisticated approach to attack their targets at just the right moment.

Cybersecurity risks [are higher now than ever before](#), as companies put more and more of their trust in cloud computing and the amount of sensitive data stored by organizations is increasing rapidly. Perimeters are getting closer and closer to the edge, offering hackers more opportunities to access a company's networks.

ISO/IEC 27032 training and certification offers IT and Security professionals real-world solutions that are relevant to today's cyber environment. Protecting an organization from incidents such as phishing, data breaches, spyware, and other cyber threats is a number one priority as organizations increasingly take their operations online.

Here are a few benefits that come with being ISO/IEC 27032 certified:

- › Strengthen your cybersecurity skills
- › Learn how to establish and maintain a cybersecurity program
- › Protect an organization's data and privacy
- › Develop ongoing security processes and best practices
- › Respond to incidents more quickly
- › Recover from incidents [more effectively](#)
- › Build confidence in stakeholders regarding your organization's security program

Organizations of all kinds can benefit from having a security leader on board that is certified to combat today's most pervasive threats and attack vectors.

Who should get certified?

Business executives, IT, and security leaders that want to stay up to date on the most relevant cybersecurity practices to acquire the competencies to face threat actors should definitely consider having at least one leader who is certified against ISO/IEC 27032. But who should get certified to provide the most comprehensive security for your team?

Here are a few examples of personnel that should consider becoming ISO/IEC 27032 certified:

1. IT and Security Leaders

Who plays the most critical role when it comes to ensuring the security and protection of an organization? IT and security leaders are uniquely positioned to protect an organization's critical data and assets, especially when they achieve ISO/IEC 27032 certification.



Leaders in IT and security who become certified demonstrate their ability to establish and maintain a cybersecurity program that is effective against the most pervasive threats.

Another reason why IT and security leaders should consider getting certified is that it provides them with the knowledge that they need to [lead teams toward more efficient security](#) best practices. Leaders with this certification enable their organizations to prevent and respond to cyber threats with a wider scope of knowledge and ability.

2. Organizations that handle sensitive data

What types of organizations should have an ISO/IEC 27032 certified leader on staff? While all businesses can benefit from hiring personnel with this certification, organizations that handle sensitive data are particularly susceptible to a data leak or cyber threat. As such, these organizations will be better off hiring an ISO/IEC 27032 IT or security professional.

It is also important to consider how your company stores, organizes, and accesses data. For example, the Machine Learning market is expected to [achieve a CAGR of 38%](#) by 2029. Machine Learning tools help organizations make sense of large amounts of data, making it easier to provide reports and make data-driven decisions. However, these tools also offer hackers plenty of new vectors to execute a devastating attack.

3. Individuals looking for career advancement

Is it a good idea for entry-level and aspiring cybersecurity leaders to achieve this certification? Absolutely. Becoming ISO/IEC 27032 certified demonstrates unique cybersecurity abilities when it comes to protecting an organization's infrastructure from unauthorized access.

Job seekers with this certification [can expect greater success](#) with more interviews and a higher employment rate because of the advanced skill set that ISO/IEC 27032 training provides.

Those that want career advancement opportunities and to achieve a higher salary in cybersecurity should also consider getting certified. Entry-level workers in this industry can expect to make about \$70,000 per year, while those with advanced skills can [expect to make up to \\$200,000](#) per year, if not more.

Final thoughts

Getting ISO/IEC 27032 certified is essential for IT and security leaders, companies, and organizations that handle sensitive data and those that want to advance their careers in cybersecurity. This standard provides a framework for organizations to develop best practices to combat the unique threats that businesses face in an era of remote work, ransomware gangs, and cloud computing.

Becoming certified helps organizations stay on top of cybersecurity threats and trends, protecting their sensitive data and preventing unauthorized access to proprietary networks and systems. In a rapidly changing digital environment, ISO/IEC 27032 certification demonstrates a professional's expertise in the field amidst the advancement of more frequent and sophisticated threats.

Ready to take the next step? Learn more about [how to get ISO/IEC 27032 certified](#).



Nahla Davies
Software Developer

Nahla Davies is a software developer and tech writer. Before devoting her work full-time to technical writing, she managed — among other intriguing things — to serve as a lead

programmer at an Inc. 5,000 experiential branding organization whose clients include Samsung, Time Warner, Netflix, and Sony. You can reach her at: nahlawrites.com.





Emerging Technologies and Cybersecurity: How It Can Secure Your Data

 BY ROHIT KUMAR

Organizations usually struggle to remember the difference between “information” and “data.” And mix this with the different levels of the attention span of the security teams in the ever-evolving threat world; we get a perfect storm brewing to take down even evolved security teams with defined standard-operating procedures! Jokes aside, the organizations thinking about the inside-outside, networks and micro segmentations, cloud and on premise, and other discussions tend to overlook that the whole organization is built around data and information, and their confidentiality, integrity, and availability is tantamount to their existence. Organizations usually generate tons of data on day-to-day operations. To some, that data is the information to bring down the organization, gain insider knowledge, gain a competitive advantage, or the loophole they were waiting for a very long time to exact profit. Thus, it is equally essential for the organization to know about data and have policies to handle them. Also, give their prized possession the attention they deserve and warrant, rather than depending on other security measures and declaring security-through-obscurity.

The previous statement should haunt organizations who still believe they can hide behind the obscurity present in their environment. The question that they should find the answer to: are they being truthful to the situation? No, they are usually not, but then they continue with their procrastination on the matter, without as much as making an actual attempt to handle the real questions at hands. To elaborate, the issues that organizations should be more concerned about should be:

1. Who can create data/information, and who owns it?
2. When data/information is created, who can access and update it?
3. How is it protected against unauthorized access or divulsion, at rest, in motion, or while processing?



4. How is data/information protected from accidental alteration or deletion?
5. How does the organization get rid of data/information that has reached its end-of-life and must be destroyed?

There are frameworks available to organizations that can help them derive their processes and operating procedures by carefully analyzing the organization's goals, deliverables, data, suppliers, consumers, participants, tools, and techniques. Some of these frameworks have been around for over 20 years (Strategic Alignment Model and the Amsterdam Information Model). They are being adopted and evolved by DAMA to create the DAMA-DMBOK Framework, which can help organizations visualize the relationships between different activities they must undertake to take account of, effectively manage, secure, maintain, integrity and interoperability, storage and operations, etc.

But before the organization gets deep into these discussions, they should be able to define the importance of data and assign a proper classification to the same. Though I just mentioned one line about data classification, all the activities would be rendered fruitless if the organization did not put in time and effort to understand the types of data they are working on and generating. Teams must take time and define data classifications, i.e., public, confidential, sensitive, personal, etc., which usually requires more manual intervention and patience than the teams have the liberty of.

Issues with no proper data classifications get exasperated once the other factors play in, such as cost and attention required to secure non-critical data, security alert/incident fatigue, etc. There is always a balance that organizations must strike without burdening the users of data, as well as burning out the security teams and their budget. Even though the situation may seem bleak, the cybersecurity industry has many solutions that use Machine Learning, supervised and unsupervised, to help organizations sift through TBs of data, structured and unstructured, to understand its nature and help teams move on with the day-to-day activities. Such solutions often do "Discovery," which allows the tools to access metadata, and sometimes data, to understand the type of data.

This information can then be used to classify data for owners or stewards and provide actionable intelligence. Thus, in-turn, these solutions can help organizations drastically

increase the speed of de-ployment of appropriate security measures based on the type and criticality of data.

Day-to-day activities of the cybersecurity teams for data protection teams can start from looking at data at rest and ensuring that it is secured from unauthorized accesses and that it is not copied or edited by anyone apart from the ones allowed in the first place. And even if access to data has been provided to people, it is reviewed periodically. In industry, we call these solutions Data Access Governance solutions, which are usually combined with the Access Governance solutions to provide a comprehensive solution to the security teams, who can find patterns of specific applications and the related data that the member should have access to. Creating and using data-to-process and data-to-role relationship (CRUDE - Create, Read, Update, Delete, Execute) matrices also help organizations and security teams to map data access needs and guide the definition of data security role groups, parameters, and permissions.

But again, these activities depend on the metadata the teams/solution have at their disposal while working with data. The importance of these aspects must jump from the formal documentation to the actual implementation and usage of the tagging mechanisms. With ever-evolving





solutions for data management, these activities can also be automated with the help of data profiling solutions and metadata repositories. Data profiling solutions can work on unstructured data, help explore data content, validate it against existing metadata, and identify data quality gaps/ deficiencies. Metadata repositories can store descriptive information about the data model, including data diagrams, definitions, lineage, and metadata imported from other tools and processes.

If this might seem too much to handle, cybersecurity teams have tools to get the job done rather than depend on documents to keep track of these complex interactions. These tools often help data architects to have a unified view of the interactions and integrations of data with the roles and system applications. They also provide security architects with much-needed clarity on the vulnerable surfaces, who can then work and device mechanisms that can be used to secure those surfaces. Security-related metadata becomes a strategic asset to the teams, increasing the quality of transactions, reporting, and business analysis while reducing the cost of protection and associated risks that lost or stolen information could cause the organization.

For the data at-rest or in-transit, data protection solutions have existed for a while now. It can range from encryption to offsite data stores, secure tunnels, and packet sniffing tools. Enterprises can very easily use the OS-based or native storage hardware-supported encryption of the drives on the endpoints. These mechanisms ensure that if the endpoints are lost or stolen, solutions will render data useless to

unintended people trying to access those endpoints. This could be extended to the servers, application servers, databases, etc., to help organizations attain peace of mind if the physical infrastructure or the cloud instances were attacked. However, these mechanisms have CPU penalties or are costly because of the use of hardware-enabled encryption modules. These trade-offs are essential for the organization to keep account of, as not all data are created equally, and the funds allocated for data protection must be spent judiciously!

A similar example goes for data in-transit. Secure tunnels (VPNs) have been for a long time and still hold their purpose in the “Work-from-home” policies that got all the limelight in recent years. However, the ZT Architectures, if implemented correctly, can help organizations move away from the need for such secure tunnels by using role-based and permission-based Data Access Management and Governance. These when combined with active fire-walls & packet-sniffing tools increasing the visibility of the security organizations and reduce surface area for the attackers. In recent years, with the mainstream usage of the Cloud, many organizations have the option to use access brokers that can help the security teams have better control over data and provide much-needed visibility with similar benefits across hybrid environments.

In order to handle sensitive employee and client data, cybersecurity teams can also use data obfuscation or masking solutions. These solutions shuffle or change the appearance of data without losing the meaning of data or the relationships data has to other data sets or systems,

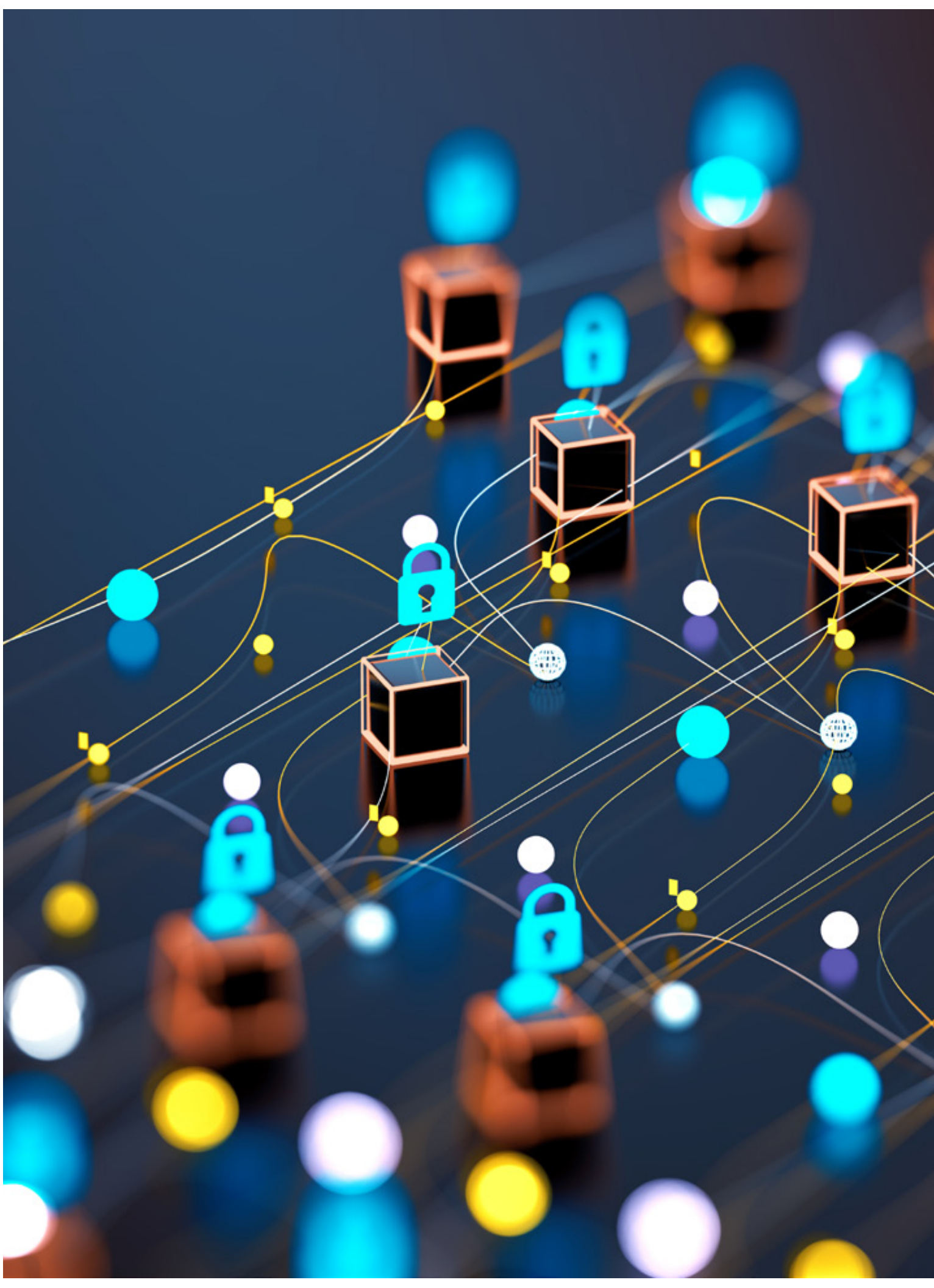


with the capability to reproduce the original data. These tools change the appearance of data to the end user without changing the underlying data, which means the solutions can mask the data in transit, at rest, and in use (dynamically). One such use case for these tools can be to display the information to the members who might need permission to view the complete data in the first place but need to due to the nature of their job (helpdesk). Once again, just enough privilege for the users to do their jobs, but not enough to cause any damage to the organization.

At this stage, it is time that we must look at data at rest from a different perspective as well. For a long time, we have depended on encryption to take care of data at rest. However, our secret weapon has been weaponized by the attackers for a couple of years now in the name of “Ransomware”! It was a wake-up call for the security leaders who now must use solutions used by military organizations, like data diodes, one-way data networks, and off-site data stores for other enterprises.

These ideas are no longer part of Hollywood movies but have been made regulatory compliance for Banking and Financial Services, and should, sooner than later, be taken up by other organizations like healthcare, manufacturing, oil & gas, etc., to make disruption of their services by attackers a whole lot less life-threatening. The criticality of data and IT infrastructure in general for these domains deserves a whole lot of attention, and the leaders, both internal and external, should pave the way to incentivize the implementation of critical security standards and solutions to gain back control from the ransomware attackers, rather than depending on the legal teams and insurance providers. With all these fundamentals out of the way, now let us see how an organization can take care of their data and embed these practices in its corporate culture:

1. **Data Security Requirements:** Organizations must define their business requirements clearly, allowing security teams to architect the environment efficiently. Also, organizations must be aware of the external regulatory restrictions that apply to them, analyze business rules and processes to identify security surfaces and keep these documents (documents that track Data-to-process and Data-to-role relationships) updated. Organizations must create a central inventory of all relevant data regulations and the data subject area each regulation affects. Regulations, policies, required actions, and data will change over time; thus, teams should keep these documents as live and updated as possible.



2. Data Security Policies and Standards: Organizations should create data security policies based on business and regulatory requirements. Security policies describe actions determined to be used by the security requirements and help security teams determine the step-by-step procedures that govern the response & recovery procedures from an incident. These policies are vital pieces of the puzzle as they help determine the team's behaviour and provide actionable objectives to the security requirement documentation. Standards supplement policies and provide additional detail on how to meet the intention of the policies. In the case of data security, they are often used to determine the following:

- › Data Confidentiality Levels
- › Data Regulatory Categories
- › Define Security Roles
- › Implementation of Controls and Procedures

3. Security Awareness Standards:

All the policies and standards can only be rendered helpful if members of the organization are aware of or follow the guidelines set by the security teams. Thus, it is of utmost importance that the policies are made aware to all the organization's members. This can be implemented using appropriate training exercises that every member must undertake. Formal or anonymous feedback surveys and interviews can help identify the organization's security awareness level. Also, it can help measure the number of members who have completed security awareness training within targeted role populations. Risk assessment findings can also enhance these reports, providing qualitative data that needs to be fed back to appropriate business units to make them more aware of their accountability for the data they manage.

And when the dust is just about to settle, teams must pull up their socks and work on the policies governing data's retention & deletion policies which are also critical for data security. This can simply help the security team at bay from the burn-out of managing and handling data that has lived past its usefulness to the organization.

There is no "one size fits all" retention period for data that organizations can find standardization about; however, for some organizations, there are regulatory requirements mandating to keep information for a certain amount of time. In other instances, there may be no such require-

ments, and the organization needs to determine the appropriate retention period, which can require case-by-case evaluations.

Once data has reached its retention period, it must be deleted securely. While the chosen disposal method depends significantly on the type of media used to store personal information, an organization must also consider the information's sensitivity and context.

Related to sensitivity, organizations must answer whether the storage media will remain within their control. A more robust disposal method should be used if the storage media are leaving their control. In the current cloud infrastructure scenarios, teams must ensure the cryptographic destruction of data storage or the VM containing the data.

All the care and attention that data gets in the organization is related to the value that it adds to the organization. In the present world where Data is the new Oil, organizations must take due care to make sure that their competitive advantage does not become their competition's prized possession, or worse, gets held by attackers for ransom, and all we can do is to make a bank run and still depend on the mercy of the attackers.

These scenarios have been happening at a rate that was not expected in the first place. But these incidents do allow us to, once again, highlight the importance of data security and make security practices part of organizations' DNA. With this in mind, considering the constant evolution of technologies that has led to an inevitable evolution of cyber-attacks and malicious acts, organizations need to act promptly and responsibly to keep their, and their consumers, data safe.



Rohit Kumar
CISSP, MSc – Cyber Laws

Rohit has over 12 years working experience with IAM and ZTA methodologies and is currently associate with EY as solution architect for emerging

technologies. He also has working experience on application virtualization, server virtualization, DevSecOps, and has worked with customers in various domains like BFSI, education, Oil and Gas, healthcare, etc.



PECB DATASAFE
SYMPOSIUM 2023

PECB DataSafe Symposium

12-13 June, 2023

PECB is thrilled to present the highly anticipated PECB DataSafe Symposium 2023, scheduled on 12-13 June, 2023. This symposium promises to be an exceptional event that will undoubtedly be worth attending. With an emphasis on topics such as Cybersecurity, Privacy, and Data Protection, the PECB DataSafe Symposium 2023 will feature panel sessions and discussions by some of the most influential panelists in the industry.

The PECB DataSafe Symposium 2023 provides a unique opportunity for professionals looking to expand their knowledge and network with other experts in their respective fields. Additionally, the program will be conducted in both English and French, to cater to a wider audience. For a detailed program of the Symposium, please click [here](#).

If you are looking to broaden your knowledge and extend your professional network, we invite you to seize this exceptional opportunity and register for the PECB DataSafe Symposium 2023.

Do not miss out on this exclusive chance to learn from top industry leaders, connect with other professionals, and gain valuable insights that can help you advance in your career.

Hurry up and register now for free!

REGISTER HERE



Using ChatGPT And Python For Chatbot-Powered eCommerce Websites

 BY JIGAR AGRAWAL

Today, each eCommerce store sells a wide range of products, and users are often confused and lost in the websites. In such scenarios, your business may suffer, and you will make fewer sales despite having all the products in stock. Moreover, customers do not like waiting in line to talk to a customer representative over a call, needing a quick solution to common questions. If you cannot cater to your customers quickly, you will often lose them to another eCommerce website that can do so.

The way out of such a dilemma is to have a chatbot that has extensive features. ChatGPT was released a few months back, and since then, it has taken the world by storm. Everyone is talking about its fantastic features. In this article, we will have a look at what ChatGPT is, what a chatbot is, and how you can build an eCommerce website with a chatbot feature using Python.

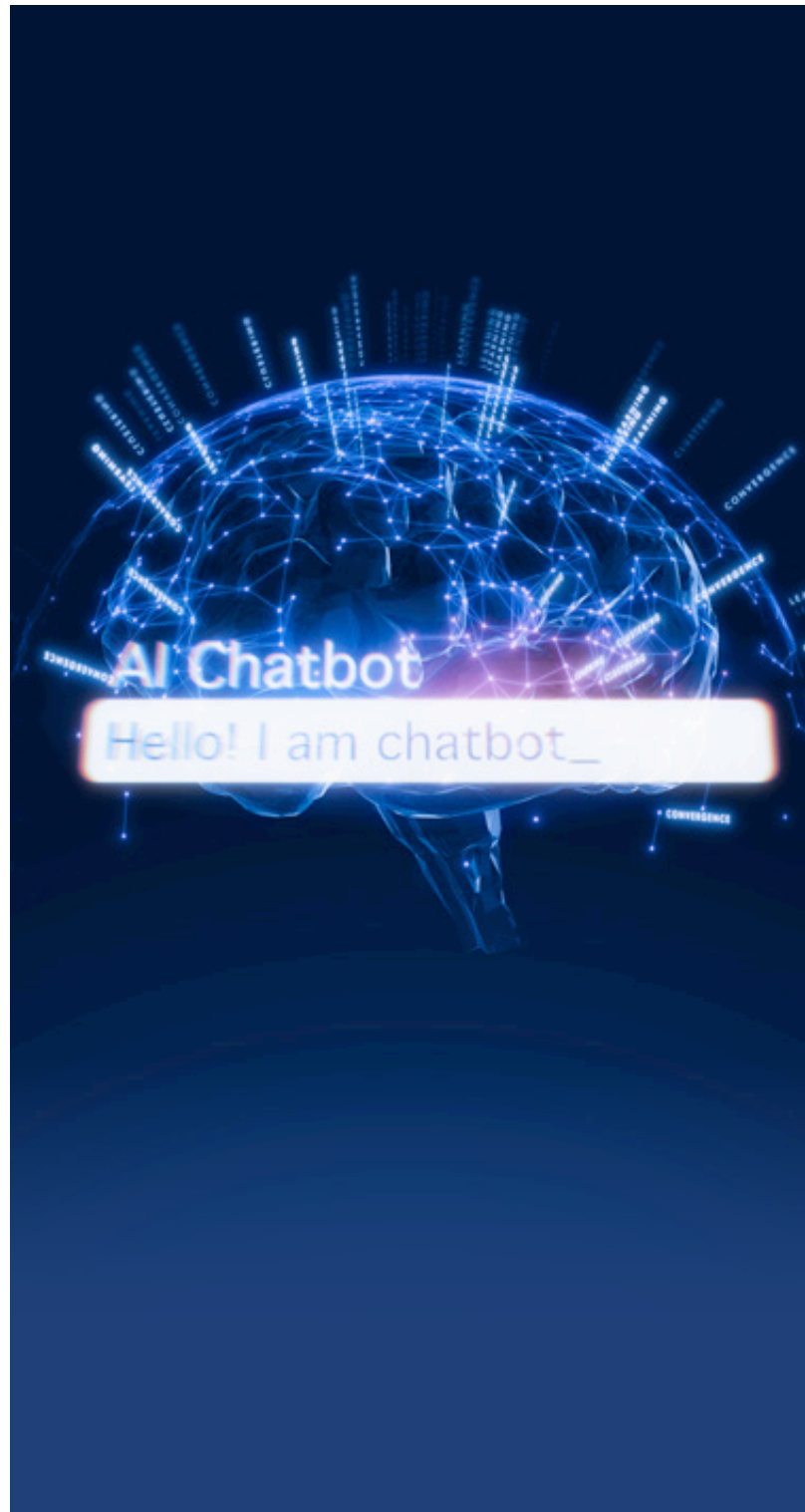
So let us get started by understanding chatbots.

What is a Chatbot?

A chatbot system uses conversational artificial intelligence to imitate a natural language discussion with any user via messaging applications, websites, or mobile apps. Such systems employ rule-based language applications to provide live chat capabilities and deliver real-time responses to users.

A chatbot has many different use cases, and it works well with eCommerce apps and websites. Creating a chatbot from scratch and training it for all the possible outcomes is a huge and time-consuming task. Moreover, such an approach to building chatbots is quite expensive, and you need a lot of experts. Instead, you can use a pre-trained natural language model to power your chatbots.

In the upcoming section, we will have a look at the latest language model that has had such a huge impact in recent months - GhatGPT.



What is ChatGPT?

ChatGPT is an NLP (Natural Language Processing) solution based on AI technology that allows you to have human-like discussions with the chatbot and much more. This [language model](#) can answer questions, aid you with chores, produce letters and articles, and even generate code.

This language model was created by OpenAI, an AI research company with a focus and expertise in developing AI products, and it has developed several products, such as OpenAI's Dall-E 2, an art generator that can create pictures out of your descriptions.

Having understood what ChatGPT is, it is better to look at why you should use chatbots in your eCommerce website.

Why Use Chatbots in eCommerce Websites?

1. Personalized Servicing to Customers

Personalization is essential in e-commerce, and chatbots are an excellent technique to establish a better, more relevant connection.

Chatbots may be used to collect data about the visitors to your eCommerce website and utilize that data to generate better product suggestions and recommendations. Understanding consumer queries, requirements, and preferences may assist you in personalizing product pages and increasing customer loyalty to your company.

Furthermore, clever chatbots may warn clients when their favorite things are out of stock and propose other products based on their tastes, all while notifying them of their projected delivery date and time as well.

2. Shift Customer Support Executive to L2 Operations

When you have a bustling eCommerce store, it is natural that your customers will have many queries, and they will need assistance.

To provide such assistance at a large scale, you need to hire many different customer support executives, and they all will be doing the same repetitive tasks. Such an approach is not efficient or feasible beyond a certain point.

That is where chatbots come into the picture. You can create and train chatbots for specific queries, and they can keep handling such queries forever.

Moreover, you can develop a single chatbot and deploy it across multiple websites, which will help you reduce the dependency and workloads of customer executives.

When the workload of your customer support executives decreases at the lower level, you can shift them to solve level 2 escalation queries. The faster you solve such queries, the better it is for your brand.

3. Fast and Cost-Effective Customer Support

When you go global, you cannot say that your work hours are over, and you cannot serve customer queries. A large number of customers require instant solutions to their issues, and if that is not available, they often head over to another eCommerce store.

Setting up human customer support executives for 24/7 quick solutions is not a feasible option either. You cannot scale such an operation as you grow your business; it is also quite costly. Chatbots are the only way that can provide you with instant customer support feature at significantly lesser prices.

AI chatbots can help in solving common customer requests quickly, and they can also learn from the conversations to provide better customer support each time. Moreover, there is no downtime in chatbots. And once they are installed, they can serve customer needs as and when they come.

4. Set Up a Knowledge Base

Scrolling through documents or reading documentation pages is a thing of the past. Today, there are very few customers who prefer that way to understand or gain information regarding anything. You cannot expect your customers to review entire documents before making an eCommerce transaction, as there are easier ways to educate them. Chatbots act as a great knowledge base, and when you program them and keep them updated with new data every time, your chatbots can help more users in understanding the products.

When your customers can understand the products quickly, the chances of dropping a transaction decrease significantly.

5. Collect and Act on Feedback

One of the best and tested ways to improve your business is by collecting and acting on feedback. If you have an eCommerce store where you have a feedback form, you are likely to get very few responses. On the other hand, having a chatbot collect feedback from visitors has a better success rate.

Chatbot can complete conversations with visitors and, in the end, ask for feedback for the conversation.

This way, the chatbot can understand whether it served the customer correctly or not. Even if you do not develop a self-learning chatbot, you can use that feedback data and understand where your services lag. Once you know the areas of improvement, it becomes much easier to improve your services without doing unnecessary work.

By now, you know why chatbots are important for an eCommerce website. Now, you might be excited to build your own chatbot, and that is what the next section is all about.

How to Make an eCommerce Website Chatbot with Python and ChatGPT?

In this section, we will have a look at building an eCommerce chatbot using Python and ChatGPT. So let us start with setting up the environment.

To get started on your chatbot development, you will need Python's Flask web framework. Moreover, we will also use ChatGPT's PyTorch implementation in this project.

If you do not have Flask and PyTorch installed in your system, use the below commands in your terminal to install the packages.

- › Pip install flask
- › Pip install torch
- › Pip install transformers

Once you run these commands, the required packages will be installed in your system, and you can proceed. Create a Flask project by creating a new Python file and adding the below code in that.

- › from flask import Flask, request, jsonify
- › import torch
- › from transformers import GPT2Tokenizer, GPT2LMHeadModel

Once you have imported the required packages, it is time to use the pre-trained ChatGPT model and create a chatbot for your eCommerce website. Use the below code to select the transformer and initialize the model.

- › tokenizer = GPT2Tokenizer.from_pretrained('gpt2')
- › model = GPT2LMHeadModel.from_pretrained('gpt2', pad_token_id=tokenizer.eos_token_id)

Now that your model is initialized, you need a function that can be called to use the model and return a response to the users. Copy the upcoming Python function and paste it into your file to accept queries and return responses.

```
def generate_response(prompt):
    input_ids=tokenizer.encode(prompt,return_tensors='pt')
    output = model.generate(input_ids, max_length=50,
num_return_sequences=1, no_repeat_ngram_size=2,
early_stopping=True)
    response = tokenizer.decode(output[0], skip_special_
tokens=True)
    return response
```

The above function will take prompts from the user, and it will process the prompt using the ChatGPT model that you initialized earlier. Moreover, it will also return the generated response to the calling function.



To use this function on your website, you need to develop the Flask app, which is pretty simple. Use the below code to create a Flask app and call the function to return helpful responses to users.

```
app = Flask(__name__)

@app.route('/')

def home():

    return 'Welcome to our e-commerce website!'

@app.route('/chatbot', methods=['POST'])

def chatbot():

    data = request.json

    prompt = data['prompt']

    response = generate_response(prompt)

    return jsonify({'response': response})
```

There are two endpoints/URLs that can be invoked by a visitor. In the above code, the user will have to send a POST request on the /chatbot endpoint with a prompt to get a response from your chatbot. To test the chatbot and get a response, you can use the below code.

```
import requests

response = requests.post('http://localhost:5000/chatbot',
    json={'prompt': 'What products do you sell?'})

print(response.json()['response'])
```

The above code will send a request to your /chatbot endpoint with a prompt, and the route will return the response by invoking the GPT model function.

Conclusion

Coming to an end, you have finally understood [how to create a chatbot](#) and the latest ChatGPT language model. You can retrain this model with data that is relevant to your eCommerce store to support more personalized conversations and services on the platform.



Jigar Agrawal
Digital Growth Hacker at
eSparkBiz Technologies

Jigar Agrawal is Digital Marketing Manager at **eSparkBiz Technologies**. He is passionate about anything related to Digital Marketing and he wants to unlock the world of technology and Social Media, where every day there is a chance of new possibilities as well as many new innovations.

Boost Your Learning With Our Updated eLearning Courses

Information Security has become a fundamental need for organizations and individuals alike. The importance of staying up-to-date with the latest updates and news is becoming more evident each day.

Therefore, finding ways to develop professionally while maintaining a good work-life balance can be a struggle for some, in the hastiness of today's busy world.

PECB offers eLearning training courses which you can follow in the comfort of your own home.

Check out the recently updated ISO/IEC 27001:2022 training courses in English:

- ▶ ISO/IEC 27001 Lead Implementer **UPDATED**
- ▶ ISO/IEC 27001 Lead Auditor **UPDATED**



#BeyondClassrooms

Blockchain Technology and Cybersecurity - How It Can Secure Your Data and Transactions

 BY CHRISTIAN GRAFENAUER

Blockchain technology has gained significant traction in recent years, as the backbone of cryptocurrencies like Bitcoin. However, its potential applications extend far beyond digital currencies, presenting transformative opportunities for cybersecurity, data privacy, and transparency. As data breaches and cyber threats continue to rise, organizations and individuals seek innovative solutions to protect their digital assets. Blockchain technology offers an array of opportunities to enhance security, ensure privacy, and promote transparency in various sectors. In this article, we will delve deeper into these opportunities, exploring how blockchain technology can secure your data and transactions while reshaping the cybersecurity landscape.

Decentralization and Security

At its core, blockchain is a distributed ledger technology that records data across a network of computers, eliminating the need for a central authority. This decentralized architecture makes it inherently more secure and resistant to cyber-attacks, as there is no single point of failure. In contrast to traditional centralized systems, attackers cannot easily compromise the entire network, which significantly reduces the likelihood of data breaches and system failures.

Immutable Data Records

Blockchain ensures data integrity and prevents unauthorized tampering by using cryptographic hashing. Each block in the chain contains a unique hash that corresponds to the data it stores. As new blocks are added, they also include the previous block's hash, creating an interlinked chain. Altering any data would require changing the hash of all subsequent blocks, making tampering virtually impossible.



Transparency and Trust

The public nature of blockchain and its consensus mechanism fosters trust and transparency between parties. All transactions are visible to network participants, reducing the need for intermediaries and decreasing the likelihood of fraud. This increased trust can streamline processes and eliminate inefficiencies in industries like finance and supply chain management. However, it is essential to recognize the current limitations in the usability and accessibility of blockchain-based services for mainstream adoption.



Many blockchain-based services have not yet reached a stage where they are conveniently usable by the average consumer. The technology's complexity and the required technical literacy can create barriers for widespread adoption by end-users, if they are exposed to the technology without certain quality of life and risk-mitigating features. While blockchain networks promote transparency and trust, their user interface and experience often lack the simplicity and intuitiveness found in traditional systems. This leads to the logical conclusion that for mainstream adoption, companies with technical literacy and an already-established level of trust can fill the role of harnessing the potential of this technology and providing advantages to their customers in an indirect way.

Ensuring that blockchain-based services cater to the needs of end-users is crucial for driving adoption and realizing the technology's full potential. This includes not only improving user experiences but also solving the existing problems regarding privacy, data control, and regulatory compliance.

To overcome these challenges, developers and stakeholders must invest in creating user-friendly interfaces, simplifying the onboarding process, and providing comprehensive educational resources to help users navigate blockchain systems safely and reliably. Additionally, collaboration between the blockchain community, regulators, and consumer advocacy groups can ensure that consumer interests are prioritized and adequately addressed.

By tackling these usability and accessibility challenges, blockchain technology can become more appealing to the mainstream, enabling broader adoption and facilitating its potential to improve cybersecurity and secure data and transactions across various industries.

Secure Identity Management

Blockchain technology has the potential to revolutionize digital identity management by enabling self-sovereign identity (SSI) systems. SSI is a user-centric approach to identity management, allowing individuals to own, control, and share their personal information without relying on a centralized authority. By combining blockchain technology with SSI, we can create secure, privacy-preserving, and legally binding digital contracts in the digital world.

Blockchain and Self-Sovereign Identity

In a blockchain-based SSI system, individuals can store their digital identity credentials, such as birth certificates, passports, and driver's licenses, on a secure, decentralized ledger. These credentials are cryptographically signed by the issuing authority (e.g., government agencies, educational institutions) and can be verified by relying parties (e.g., banks, employers) without disclosing the underlying data.

When an individual needs to provide identity information to a relying party, they can do so using verifiable credentials. These credentials are tamper-proof, cryptographically secure digital attestations that can be shared and verified easily. The individual maintains control over their data, sharing only the necessary information with the relying party. This approach enhances privacy and reduces the risk of identity theft and unauthorized access to personal information.

Enabling Legally Binding Digital Contracts

The combination of blockchain technology and self-sovereign identity paves the way for legally binding digital contracts.

Smart contracts, which are really to be understood as self-executing agreements with terms directly written into code, can be employed in conjunction with SSI to create secure digital contracts. When parties enter into a digital contract, they can use their blockchain-based SSI credentials to authenticate their identities and sign the contract using their private keys.

These digital signatures are cryptographically secure, ensuring that the contract is signed by the intended parties and providing non-repudiation. The smart contract's terms can be automatically enforced upon meeting predefined conditions, reducing the risk of human error, fraud, and disputes. By leveraging blockchain technology, SSI, and smart contracts, we can create a robust framework for digital contracts that are secure, privacy-preserving, and legally binding. This framework has the potential to revolutionize various industries, such as finance, real estate, and legal services, by streamlining transactions, reducing costs, and enhancing trust between parties.

In conclusion, the integration of blockchain technology with self-sovereign identity and smart contracts has the potential to reshape digital identity management and enable legally binding digital contracts. The combination of empowering individuals to own and control their data, enhancing privacy, and facilitating secure transactions, can drive significant advancements in cybersecurity and data protection.

Smart Contracts and Secure Transactions

Smart contracts are self-executing agreements with the terms directly written into code, which are stored on a blockchain network. They offer several advantages over traditional Web 2.0 infrastructure in terms of security, transparency, and efficiency. In this section, we will explain in more detail how smart contracts work and how they lead to more secure transactions compared to traditional Web 2.0 systems.

How Smart Contracts Work

Smart contracts are designed to automatically execute transactions when predefined conditions are met, without the need for intermediaries. An example of this is enabling trustless, automated insurance payouts upon the occurrence of a predefined event, such as a flight delay, without requiring manual processing, intervention from an intermediary or the passenger having to request the refund in the first place. These smart contracts are written using programming languages like Solidity (for Ethereum) or other blockchain-specific languages.



Once deployed on the blockchain, smart contracts are immutable, meaning they cannot be altered or tampered with.

Each smart contract contains a set of rules that dictate how the contract will behave under specific conditions. These rules are encoded in the form of "if-then" statements. For example, a smart contract for a rental agreement might include a rule stating that if the renter pays the deposit, then the keys will be released to them. When the conditions outlined in the contract are satisfied, the contract automatically executes the corresponding actions, such as transferring funds or releasing digital assets.

Security Advantages Over Traditional Web 2.0 Infrastructure

Web 2.0 infrastructure refers to the centralized, server-based architecture that underlies the current Internet, where data and services are primarily controlled by a limited number of intermediaries. Smart contracts offer several security benefits compared to traditional Web 2.0 infrastructure:

1. **Decentralization:** Unlike traditional Web 2.0 systems that rely on centralized servers, smart contracts are stored on a decentralized blockchain network. This architecture eliminates single points of failure, making it more resilient against cyber-attacks, data breaches, and system failures.



Protection Against DDoS Attacks

Blockchain's decentralized nature also offers protection against Distributed Denial of Service (DDoS) attacks. Distributed Denial of Service (DDoS) attacks are a type of cyber-attack where multiple systems are used to flood a targeted server, network, or website with an overwhelming volume of traffic, rendering it unavailable to its intended users. These attacks can cause significant downtime, disrupt services, and result in financial losses for affected organizations. In this section, we will explain how blockchain technology can effectively protect against DDoS attacks.

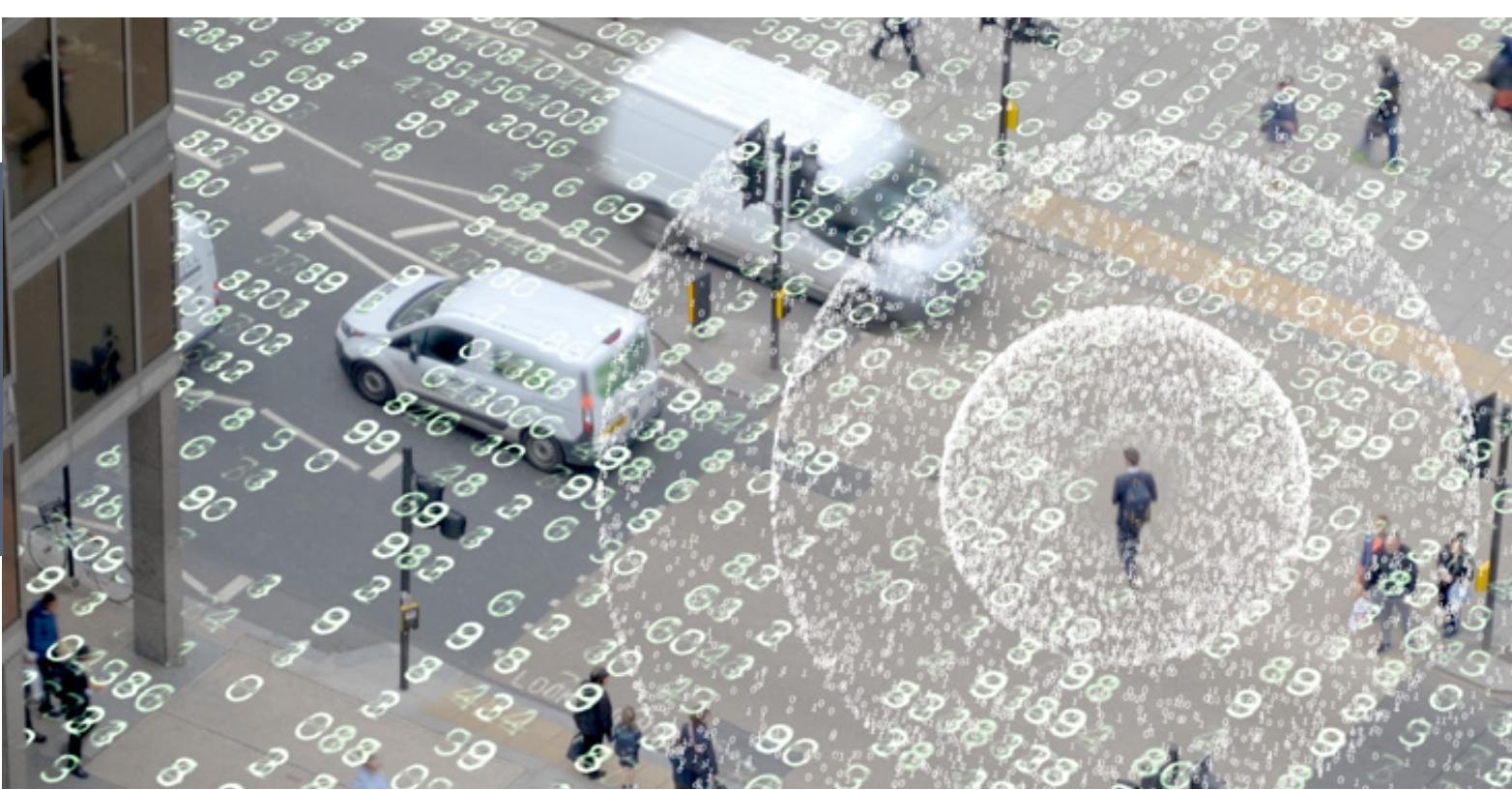
How Blockchain Technology Protects Against DDoS Attacks

Blockchain's decentralized nature and unique architecture offer several advantages in combating DDoS attacks:

1. **Decentralization:** Blockchain networks operate on a distributed ledger, which means that data is stored across numerous nodes (computers) rather than a single centralized server. This decentralization eliminates single points of failure, making it more challenging for attackers to target and overwhelm the entire network. As a result, blockchain networks are more resilient against DDoS attacks.
2. **Consensus Mechanism:** Blockchain networks employ consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to validate transactions and maintain network security. These mechanisms require participants to expend computational resources or stake digital assets, creating barriers for potential attackers. Launching a successful DDoS attack on a blockchain network would necessitate overpowering the network's combined resources, which is often prohibitively expensive and difficult to achieve.
3. **Redundancy:** Since all nodes in a blockchain network store a copy of the entire ledger, the system is inherently redundant. In the event of a DDoS attack targeting specific nodes, other nodes in the network can continue to operate and maintain the network's functionality. This redundancy enhances the network's resilience against DDoS attacks and ensures that services remain available even during an attack.
4. **Cryptographic Security:** Blockchain networks utilize cryptographic techniques, such as digital signatures and hashing, to secure transactions and data. These techniques make it more challenging for attackers to inject malicious traffic or manipulate data during a DDoS attack, further enhancing the network's security.

2. **Immutability:** Once a smart contract is deployed on the blockchain, it cannot be altered or tampered with. This feature ensures that the contract's terms and conditions remain consistent and secure throughout its lifecycle.
3. **Transparency:** Smart contracts are inherently transparent, as their code and transaction history are publicly visible on the blockchain. This transparency enables all parties involved to verify the contract's integrity and reduces the likelihood of fraud or manipulation.
4. **Automation:** Smart contracts automate transaction execution, reducing the risk of human error, fraud, and delays. By removing intermediaries and automating transactions, smart contracts streamline processes and enhance efficiency.
5. **Trust:** Since smart contracts are enforced by the blockchain's consensus mechanism, parties can trust that the contract will execute as intended without the need for a trusted third party. This trust minimizes disputes and enhances security in the transaction process.

By leveraging smart contracts, businesses and individuals can take advantage of a more secure, transparent, and efficient transaction process compared to traditional Web 2.0 infrastructure. As a result, smart contracts have the potential to transform various industries by enhancing cybersecurity, trust, and privacy.



In summary, the decentralized architecture, consensus mechanisms, redundancy, and cryptographic security of blockchain technology provide robust protection against various cyber attacks. By leveraging these features, blockchain networks can maintain their availability and resilience even in the face of sophisticated cyber threats, offering a more secure alternative to traditional centralized systems.

Data Privacy and Confidentiality

Blockchain technology can provide concrete benefits for data privacy and confidentiality through the use of privacy-focused solutions such as zero-knowledge proofs, confidential transactions, and privacy-preserving smart contracts. These techniques enable secure data validation without revealing the underlying information, ensuring both data integrity and privacy. In this section, we will explore the specific benefits that blockchain technology can offer in terms of privacy.

1. **Selective Disclosure:** Blockchain-based privacy solutions allow users to disclose only the necessary information to verify a transaction or fulfill a smart contract's conditions without revealing their entire data set. This selective disclosure enhances privacy by minimizing the exposure of sensitive information to third parties.
2. **Confidential Transactions:** Some blockchain platforms, such as Monero and Zcash, use advanced cryptographic techniques to obscure transaction details, such as the sender, recipient, and amount.

This ensures transaction privacy and protects user data from potential surveillance or tracking.

3. **Privacy-Preserving Smart Contracts:** Privacy-focused blockchain networks can implement smart contracts that preserve data privacy during execution. This allows users to engage in secure, private transactions without disclosing sensitive information to other network participants or third parties.
4. **Identity Anonymization:** Blockchain technology can facilitate pseudonymous or anonymous transactions by using public keys as identifiers instead of personal information. This approach reduces the risk of identity theft and enhances user privacy during transactions.
5. **Data Sovereignty:** Blockchain's decentralized architecture empowers individuals to retain control over their data, allowing them to manage access permissions and share information on a need-to-know basis. This ensures that data privacy is maintained, and users retain sovereignty over their personal information.

By harnessing these privacy benefits, blockchain technology can provide robust protection for sensitive data and enable secure, private transactions across various industries.

As adoption continues to grow and privacy-enhancing solutions become more sophisticated, blockchain technology will play an increasingly crucial role in preserving data privacy and confidentiality in the digital world.



Real-World Applications

Blockchain technology has moved beyond cryptocurrencies, finding applications in various industries and transforming the way we conduct transactions and secure data. In this section, we will explore five famous use cases where blockchain is already being used in our daily lives.

Supply Chain Management

Blockchain technology is being used to enhance traceability, transparency, and efficiency in supply chain management. Companies like Walmart, IBM, and Maersk have implemented blockchain solutions to track goods from their origin to the end consumer, ensuring product authenticity and reducing the risk of counterfeit products. This real-time visibility into the supply chain helps businesses optimize their operations and respond to issues more effectively.

Digital Identity Management

As mentioned earlier, blockchain technology can facilitate secure identity management through self-sovereign identity (SSI) systems. Platforms like uPort, Sovrin, and Civic leverage blockchain to enable users to create and manage their digital identities, controlling who has access to their personal information. This approach enhances privacy, reduces the risk of identity theft, and streamlines the identity verification process for various services, such as banking and e-government.

Cross-Border Payments and Remittances

Blockchain technology is revolutionizing the way we send money across borders by providing faster, cheaper, and more secure transactions. Companies like Ripple and Stellar offer blockchain-based solutions that enable instant, low-cost international money transfers. By eliminating intermediaries and leveraging the decentralized nature of blockchain, these platforms reduce transaction fees and processing times compared to traditional methods.

Healthcare

Blockchain technology is being used to improve data security, interoperability, and patient privacy in the healthcare sector. Platforms like Medicalchain, Solve.Care, and BurstIQ enable secure storage and sharing of electronic health records (EHRs) on a decentralized ledger, allowing patients to control access to their medical data. This approach can streamline data exchange between healthcare providers, enhance patient privacy, and enable more personalized care.

Voting and Governance

Blockchain technology is being leveraged to improve the transparency, security, and efficiency of voting systems.

Projects like Voatz, Horizon State, and Follow My Vote use blockchain to ensure the integrity of election results by making voting records tamper-proof and publicly verifiable. This can reduce the risk of fraud, increase voter confidence, and promote more transparent and accountable governance.

Heavily Regulated Industry

In heavily regulated industries like aerospace, where human safety and reliability are critical, machines equipped with sensors can record torque levels for each screw on a blockchain-based system, ensuring tamper-proof, transparent documentation of essential manufacturing data, while facilitating real-time monitoring, traceability, and compliance with stringent quality standards.

These examples showcase the diverse applications of blockchain technology in our daily lives, demonstrating its potential to enhance security, transparency, and efficiency across various industries. As technology continues to mature, we can expect even more innovative applications that further improve data privacy and transform the way we interact in the digital world.

Challenges and Limitations

As promising as blockchain technology is, it faces several challenges, including scalability, energy consumption, and the need for standardization. In this section, we will discuss potential solutions that will help us overcome those problems, while blockchain technology matures with ongoing research and further prototype development.

Scalability: Inter-Blockchain Communication and Mesh Networks

Scalability remains a critical concern for blockchain networks, as they need to handle increasing transaction volumes to compete with traditional systems. Two examples of potential solutions to improve scalability include Inter-Blockchain Communication (IBC) and mesh networks.

IBC

IBC refers to the seamless exchange of data and value between different blockchain networks. By enabling cross-chain communication, IBC can help distribute transactions across multiple networks, alleviating congestion and improving overall throughput.

Mesh Networks

Mesh networks, on the other hand, involve a decentralized network topology where nodes connect directly to each other, allowing data to be routed through multiple paths. This approach can enhance network efficiency and capacity by spreading transaction loads across the network more evenly.

Energy Consumption: Alternatives to Proof of Work

Proof of Work (PoW) is the consensus mechanism used by many blockchain networks, including Bitcoin. However, it is associated with high energy consumption due to the intensive computational power required to mine blocks. To address this issue, alternative consensus mechanisms have been proposed, such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Authority (PoA). These mechanisms consume significantly less energy than PoW while still providing a secure and decentralized consensus.

Standardization: ISO Efforts and Regulatory Guidance

To ensure interoperability, security, and widespread adoption, blockchain technology requires effective standardization.



The [International Organization for Standardization](#) (ISO) has established a technical committee, ISO/TC 307, to develop global standards for various aspects of blockchain technology, including terminology, architecture, privacy, and security.

These efforts aim to create a standardized framework for blockchain implementation, paving the way for meaningful regulatory guidance and best practices.

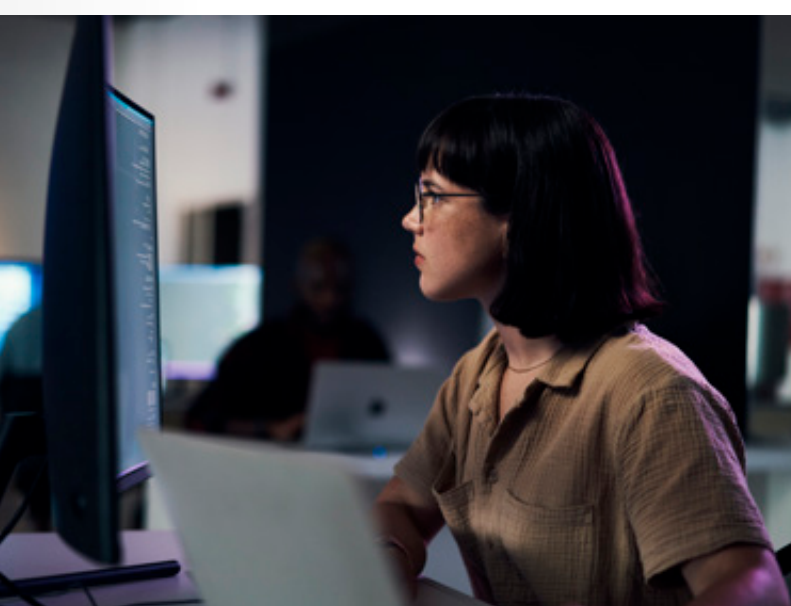
As the blockchain ecosystem continues to evolve, addressing these challenges and developing robust solutions will be crucial for its long-term success. By focusing on scalability, energy efficiency, and standardization, the industry can move towards more sustainable, secure, and accessible blockchain solutions that benefit various sectors and users worldwide.

Future Outlook

As blockchain technology matures and becomes more widely adopted, it has the potential to revolutionize the way we interact in the digital world, enhancing security and privacy while providing new business models and opportunities for innovative companies. In this section, we will provide an elaborated future outlook that explores how blockchain can transform our digital landscape, focusing on its core applications and benefits.

Enhancing Security and Privacy

Blockchain technology offers several features that can significantly improve cybersecurity and data privacy. Its decentralized architecture, cryptographic security, and tamper-proof nature make it more resilient against cyber-attacks, data breaches, and fraud.



By adopting blockchain-based solutions, businesses and individuals can benefit from increased security and trust in digital transactions, secure identity management, and enhanced data privacy through selective disclosure, confidential transactions, and privacy-preserving smart contracts. As global concerns over data privacy grow, we can expect blockchain technology to play an increasingly crucial role in securing our digital lives. By offering more robust protection against cybersecurity threats and enabling secure, private transactions, blockchain can pave the way for a safer and more transparent digital ecosystem.

Unlocking New Opportunities and Business Models

Blockchain technology can also unlock new opportunities and business models by fostering innovation, reducing operational costs, and streamlining processes. For instance, industries like supply chain management, healthcare, and finance can leverage blockchain to enhance transparency, efficiency, and security. Decentralized finance (DeFi) is another promising area, offering an alternative to traditional financial services and expanding access to financial tools for the unbanked and underbanked populations.

Smart contracts are also poised to transform various industries by automating the execution of transactions and legally binding contracts. This can reduce the need for intermediaries, lower transaction costs, and accelerate processes across sectors such as real estate, insurance, and legal services. In such cases, parties would only need to agree on the particular contract flow to apply and the rest would be automated. Furthermore, blockchain technology's ability to enable cross-border payments and remittances with minimal fees and instant settlement can reshape the global financial landscape, facilitating more accessible and cost-effective financial services for individuals and businesses worldwide.

Looking ahead, we can anticipate more innovative applications of blockchain technology that capitalize on its unique features and benefits. As technology continues to evolve, we can expect to see the emergence of novel use cases and business models, driving growth and creating new opportunities for organizations that embrace this cutting-edge technology.

Blockchain technology has the potential to transform our digital world by enhancing security, privacy, and trust, while providing new business models and opportunities for innovative companies.

As adoption continues to grow, and blockchain-based solutions become more sophisticated, we can look forward to ever more secure, transparent, and efficient digital ecosystems.



Christian Grafenauer

Anonymization Expert, Privacy Engineer, Data Protection Officer, LegalTech Researcher (GDPR, Blockchain, AI)

Christian Grafenauer is an accomplished privacy engineer, anonymization expert, and computer science specialist, currently serving as the project lead for Anonymity Assessments at TechGDPR. With an extensive background as a Senior Architect in Blockchain for IBM and years of research in the field since 2013, Christian co-founded Privacy by Blockchain Design to explore the potential of blockchain technology in revolutionizing privacy and internet infrastructure.

As a dedicated advocate for integrating legal and computer science disciplines, Christian's expertise in anonymization and GDPR compliance enables innovative AI applications, ensuring a seamless fusion of technology and governance, particularly in the realm of Smart Contracts. In his role at TechGDPR, he supports technical compliance, blockchain, and AI initiatives, along with anonymity assessments.

Christian also represents consumer interests as a member of the National Blockchain and DLT Standardization Committee at DIN (German Standardization Institute) in ISO/TC 307. In early 2020, he contributed to the development of the world's first standard for "DIN SPEC 4997 Privacy by Blockchain Design: A standardized model for processing personal data using blockchain technology." Christian's vast experience and commitment to privacy engineering and anonymization make him a valuable asset in shaping the future of secure and privacy-preserving digital technologies.

GET WELL-INFORMED IN YOUR CHOSEN FIELD

Open your doors in the field of your interest through the PECB Store, where you will be able to find the tools and materials that you need to enrichen your learning experience and strengthen your competencies.

Toolkits are an efficient way to get yourself started, containing all the information, documents, and materials you need.

Check out some of the toolkits in the [PECB Store](#) below.

CHECK OUT NOW ►

ISO/IEC 27701 Toolkit

The toolkit contains documents needed for the implementation and auditing of a Privacy Information Management System (PIMS).

PECB GDPR Implementation Toolkit in French

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

Throwback to the First PECB Awards Gala

 BY PECB

As we continue to celebrate remarkable moments in PECB's history, we take a nostalgic journey back to the inaugural PECB Awards Gala. This prestigious event, held on June 29th, 2017, as part of the PECB Insights Conference 2017 in Montreal, Canada, brought together industry leaders, professionals, and organizations from around the globe to honor excellence, innovation, and dedication in the field of Information Technology, Security, and Privacy. Let's delve into the highlights of this unforgettable evening and relive the excitement that marked the first PECB Awards Gala.

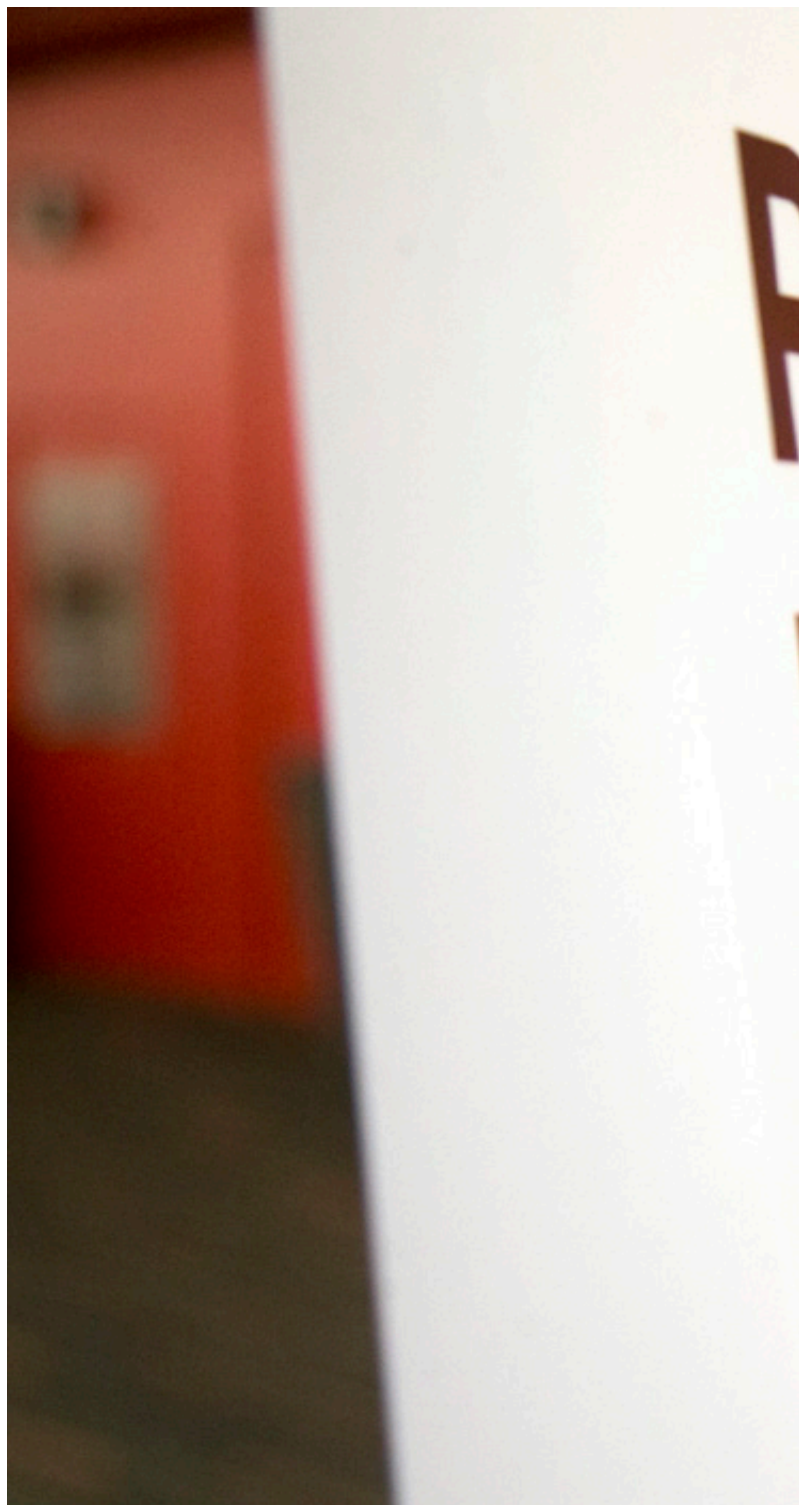
The heart of the evening was dedicated to honoring excellence in various categories that showcased outstanding achievements and contributions. During the night, awards of different categories have been delivered including Trainer of the Year Award, Auditor of the Year Award, Audited Business of the Year Awards and Reseller of the Year Award.

The PECB Awards Gala recognized the remarkable efforts of individuals, organizations, and teams who demonstrated exceptional dedication, innovation, and impact in driving forward the standards and practices. The deserving winners were celebrated for their significant contributions, inspiring others to reach new heights of excellence.

The first PECB Awards Gala was an evening filled with unforgettable moments. From the announcement of winners and heartfelt acceptance speeches to the vibrant ambiance and joyous celebrations, every element of the event contributed to an atmosphere of pride, inspiration, and unity within the industry. Attendees left the gala with memories that would forever remain etched in their minds.

You can check out the winners of our first PECB Awards Gala by clicking below!

WINNERS ▶



Looking Ahead

The success of the first PECB Awards Gala set the stage for future editions, promising even greater moments of celebration and recognition. PECB remains committed to honoring excellence and fostering a culture of continuous improvement within the industry. As we reflect on the memories of the inaugural gala, we eagerly anticipate the future, where we will gather once again to celebrate outstanding achievements and inspire further advancements.

The first PECB Awards Gala was a milestone event that brought together industry leaders, professionals, and organizations in a celebration of excellence and innovation.

From captivating ceremonies and inspirational speeches to the jubilant atmosphere of celebration, this gala left an indelible mark on the hearts and minds of all attendees. As we cherish the memories of this remarkable evening, we look forward to future galas that will continue to honor exceptional achievements and drive progress!







PECB Received Hot Company Cybersecurity Training Award!

We are excited to present that we have received the prestigious Cyber Defense Global InfoSec Award for Hot Company Cybersecurity Training. Our CEO, Tim Rama, proudly accepted the award together with our Senior Commercial Director Zeki Veliu, and Senior Training and Product Development Director Artan Mustafa, at the annual RSA Conference in San Francisco, which brings together top cybersecurity companies and professionals from around the world.

This recognition emphasizes PECB's commitment to providing high-quality training that meets the evolving demands of the industry and our motivation to continue contributing to the industry by ensuring that our training courses cater to the needs of professionals in the field of information security.

[VIEW SPEECH ►](#)

Dark Data or Data in Darkness

 BY DANIEL SUCIU

Dark data can be defined as all the data that exists within an organization but is currently useless or unusable, either because it is redundant, forgotten, ignored, hidden, simply unknown to the organization at a given point in time, or which may be difficult to find, manage, or exploit for valuable insights.

Where Do These Data Come From, and Why?

These data are either collected by the organization for a certain purpose (but not clearly defined or implemented), or produced by people or IT systems, during normal operations, but not used or useful anymore, or even produced by IT systems without the organization's knowledge. Other reasons can be:

- From processing the same data by multiple stakeholders.
- From processing the same data in multiple systems or by multiple functions.
- Due to changes in applications/IT systems.
- Due to improperly managed business processes.
- The existence of incorrectly configured or managed applications/IT systems.
- Due to the lack of data cleansing processes resulting from normal business processes.
- Due to the lack of validation criteria for collected or processed data.
- Poorly defined or monitored systems configuration, administration, or incorrect backup and archiving processes.
- Overall, the absence of a data governance framework.

Examples of "Dark Data"

Often we can overlook, or even forget, data we have collected for a project, a report, a presentation, etc. However, all this data is still in our operational systems. Some cases where dark data may come from or be stored:



1. Attachments to old emails, often sent to large groups, resent, saved in various locations
2. Intermediate files used in the elaboration of a report or presentation, with various comments and revisions
3. Raw data used to produce a report, presentation
4. Operating system logs, databases, applications, or IT/network system journals that extend over a period of time that is too long, or of which we are unaware and which are not used or useful anymore
5. Databases of outdated IT systems that have been replaced but have not been migrated and cannot be used anymore
6. Data collected by an IT system, transmitted to others for processing but stored by both systems in the same format
7. Erroneous data, which cannot be used for planned purposes, but has not been deleted
8. Temporary files created by certain applications or IT systems, kept long after the processing purpose has been fulfilled
9. Data that is behind access restrictions, of which we are unaware and cannot be accessed
10. Archived files, that although have been extracted, and the files used have not been deleted;
11. Data from projects that have been started and abandoned or put on hold for a long time
12. Data belonging to former employees that can no longer be accessed or are no longer useful or relevant
13. Archived data that is still being kept in operational systems
14. Archived data whose storage/archive time has expired but has not been deleted
15. Multiple backups, or backups kept for longer than the efficient usage duration
16. Data collected for a defined purpose but never materialized
17. Data collected "just in case" may be useful for something in the future

Why Should We Care About Them? – Individual Use

At a personal level, I suppose it is not only me that feels annoyed when searching for an old document created some time ago, and trying to figure out which the last version is. To be sure, I will check sent emails, where I found even more versions than anticipated. I assume I am one of many to see a message that notes that there is not enough space and that some files should be cleaned up.

That is the best-case scenario, the worse being when the system crashes or runs very slowly due to a lack of disk space.

Some of us are aware of the need for periodical clean-up, but we still are surprised when we see the number of temporary or large files, we had not accessed for years.

Of course, this counts those pictures we took on several occasions, events, trips, or those with our children, which are never too many, and are never protected enough. Therefore, just in case, we are saving them in several locations, we have them in our phones, our computers, in cloud(s), plus sent (and stored) in emails or any messaging application.

The most curious of us are looking at systems or application logs/history, and we are amazed about the volume and the timeframes we have information about. Information we are never using.

Those aware and up to date with technological risks are doing periodical back-ups of their computers, phones, or accounts. This is a good thing, however, not as good if we are keeping and storing all back-ups from the past 10 years.

The multitude of data we are storing can be continued to be described, which are not only useless but also harming our effectiveness or efficiency. These are the so-called "dark data".

At An Organizational Level

Unfortunately, all the previous, but in a higher order of magnitude, in terms of data source, volume, and potential use, are applicable at an organizational level just as much.

Moreover, we have additional reasons to care about them. In fact, many other reasons, which could be irrelevant for an individual, but are critical for business.

Some of which are:

- › Meeting legal requirements
- › Complying with assumed standards
- › Rising unproductive, direct and indirect, costs of managing data
- › Managing security and business continuity risks
- › Impacting work efficiency
- › Organizations may lose customer trust
- › Missing new business opportunities

The reasons look obvious, so one could ask why these were not already addressed if these could cause such hassle to an organization. If so, why? Because these are not known by the deciding factors, or at least not the magnitude of the volume or impact of these data. This is the reason we are calling them “dark data”.

What Can Or Should We Do With Them?

All people in an organization, all the systems, and all the processes are collecting or generating masses of data and some of them will inevitably become “dark data”. We cannot ignore it, and we should even aim to eliminate all of the “dark data”, as the costs could be higher than living with them. However, we should try to minimize them, keeping them at a level which does not impact business effectiveness and efficiency.

An approach to treat “dark data”, or any data which looks like “dark data”, would contain several logical steps, such as the following:

- › Dark data identification
- › Quantitative evaluation
- › Classification
- › Impact estimation
- › Identification of (probable) causes
- › Decide on “dark data” treatment
- › Implement measures to avoid/minimize dark data volume and impact
- › Continuous monitoring of data.

Now, let us take a deeper look at them one by one:

“Dark Data” Identification

As the name suggests, these are not always obvious, at least if we are not looking for them. So where could we start? Based on the examples proposed here, or the classification proposed later in this material, we should try to look for them, source by source, process by process, system by system. Of course, using automated tools would make our life easier, and there are a lot of them on the market, including many free ones. Your IT team or admin could also help. In fact, without IT help, this initiative is almost doomed, as aside from their access rights, they have the knowledge of where to look and how to do it.

The beginning could be more difficult, but as you start to discover them, the easier it will be, to apply similar search patterns and logic for other processes or IT systems.

Quantitative Evaluation

As we mentioned earlier, we should not aim to get rid of all “dark data”, as the cost could easily be higher than the negative impact. So we should aim to remove the most critical ones, which could have a real impact.

So, the first criterion would be the volume of data. The more data that we do not need or use, the worse it is. However, the overall volume is not the only criterion. For example, 10,000 small (10Kb) files could have a larger negative impact than a 1GB file, even if the overall volume is ten times lower.

Moreover, the quantitative aspect is not the only criterion. Sometimes one single small file, in the wrong place, containing sensitive information, could be the subject of the clean-up.

Classification - The “Classical” Way

The first attempt to classify these useless or unused data was the ROT data.

The term "ROT data" is derived from the acronym "ROT", which stands for "redundant, obsolete, or trivial" data. This term has been used for many years in the information management industry to refer to data that is no longer useful or relevant but is still being stored and managed by an organization.

All of these concepts have been included in the scope of this article as they overlap with the concept of 'dark data'.

Classification means to assign them to different categories and subcategories, based on different criteria. The criteria could vary from the perception of data, to the source of data, and the impact of data, based on the specific job requirements of the person doing the classification.

An example could be the following:

- › **Useless Data:** Unusable data, Redundant data, Outdated data, Trivial data, Low-quality data, Temporary data.
- › **(Just) Unused Data:** Hidden data, Inaccessible data, Ignored/forgotten data, Data on hold/awaiting, Data collected "just in case".

However, this is not an easy task as the classification depends on the purpose, source, organization, knowledge of people and functions involved, in processing and analysis, as usually data crosses many functions from generation and collection to processing, storage, analysis, etc.





A More Effective Way of Classifying Dark Data

Taking the same sample of “dark data” and asking different people from different functions is likely to give completely different results. Most likely, IT, Marketing, Legal, Finance, Operational, Compliance, etc., would have different classifications. Even within the same department, like IT, a system or application admin would have a different classification than a cybersecurity specialist, a project manager, a business analyst, or IT management.

The first attempt in classifying “dark data” would be to separate those which are clearly useless and those just unused, but could be potentially useful. The question is “useful for who”? Not always, or rarely, the person responsible for collection is also the main beneficiary of the data.

Thus, a better alternative to pure classification is using keywords to describe certain characteristics used in classification. This way, using as many keywords as we feel relevant, from all relevant stakeholders, we will not need to fit into a certain category, and it even gives some hints about the perceived issues with these dark data and the possible solutions to address the issue.

Some possible keywords could be (not exhaustive and in alphabetical order):

- › Abandoned, awaiting, broken, conflicting, counterproductive, disorganized, disregarded, fragmentary, hidden, ignored, impractical, inaccessible, incomplete, incongruent, inconsistent, insignificant, irreconcilable, irrelevant, low-quality, masked, meaningless, messed-up, negligible, not understood, omitted, out of view, outdated, out-of-date, partial, pending, purposeless, redundant, scrambled, substandard, temporary, too complex, transitory, uncertain, undecided, undetected, unknown, unnecessary, unorganized, unreachable, unstable, unstructured, unusable, unverified, unwanted.

However, we will see that perception is different, and what is useless to one could be useful for other stakeholders, and what is too complex for one could be trivial for another. But all this information together would give important hints for the next steps.

Impact Estimation

Once we classified the data, or even before, the order in this case not being of paramount importance, would be to estimate the impact. Estimating the impact would consist of two different pieces of information: where the impact is higher (like compliance, legal, operational, finance) and the magnitude of the impact.

For each impact area, thresholds should be defined to decide what is worth to be addressed and what is not. However, this is an iterative work, and it would be easier to accomplish.

Identification of (Probable) Cause

In order to decide what to do with them, we should understand why these “dark data” are there. Are they a normal artefact of a business process, which we should delete after a while, are they due to a misconfiguration of an IT system or a broken process (especially a cross-functional one), or a result of the changes in the IT systems or the business process? This is important to know, in order to prevent their generation after we clean up the mess.

Decide On “Dark Data” Treatment

After we have a quantitative estimation of these data, impact estimation, probable cause, and classification, we can decide what to do with them. Generally speaking, we have to choose from the following alternatives:

- › Let them be - when quantity/impact is irrelevant
- › Keep them at a minimum - when we need them, but not for a long period of time
- › Delete them - when nobody sees a use for them, or they are causing more trouble
- › Archive them - when they are not needed for operational purposes, but there are legal requirements to keep them
- › Organize them - when these could be useful for a certain function
- › Improve quality when possible
- › Process them - when these would be useful, but not in actual format/status

Of course, the decision is not always obvious, but the keywords used in classification could give a hint about the needed actions.

For example:

Abandoned, awaiting, disregarded, ignored – ask the intended usage owners to decide: delete/organize for use

Broken, fragmentary, incomplete, inconsistent, insignificant, counterproductive, impractical irrelevant – delete

Negligible – delete or let them be

Disorganized, irreconcilable, incongruent – label, analyze, then decide

Hidden, masked meaningless, omitted, too complex – analyze possible usage, then decide

Inaccessible – get access and analyze or delete/archive

Implement measures to avoid or minimize dark data volume and impact

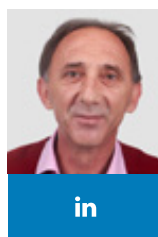
After we have treated the data, it would be more efficient to implement the needed changes into the business processes or IT systems configuration in order to minimize these “dark data”, or at least to identify them in due time, for proper treatment.

Implementation of data management and governance framework, in case one is not implemented, would definitely make this process easier, or some categories would not even be present, being discovered and treated, in due time.

In case you have one, after this effort, it would be useful to update your business glossary, data dictionary and catalog.

Continuous Monitoring Of “Dark Data” Categories

It seems we have done everything that needed to be done. Not quite. There still remains one activity to be performed: to monitor the “dark data” existent in our business environment. IT systems are continuously changing, and business processes change as well, not to mention people. As a result, what yesterday was under control, tomorrow could become a problem. Monitoring those we know about, or overall categories, like application logs, implementing similar controls for new systems or initiatives, as soon as possible, could save us a lot of time and money.



Daniel Suciu

IT, Data Protection, and Governance

Specialist with 35 years in Business Process Management, Change Management, Data Governance/Management/Quality, Data Protection, Software Development, IT Administration and Support, Risk Management, Quality Assurance, and

Internal Audit, but also Project and People Management, with measurable results at the intersection of systems, technology, processes, people, and data.

Manage, coordinate, and support change management and process improvement which helps people support the business. Continuously challenging the status quo and taking care of external challenges and opportunities.

Relevant experiences include:

Managing, coordinating, and supporting organizational initiatives and projects in Information Security, Data Management and Governance, Project Management, Business Process Management, Change Management, Quality Assurance, Internal Audit, and Risk Management in large multinational companies.

Performing auditing and consulting engagements for NGOs and various companies, from small to large businesses across various industries.

Implementing products, solutions, and processes from the concept phase to implementation, administration, and operational support.

Working closely with other business functions (HR, Marketing, Sales, Legal, Customer Service, Contract Management, and Security and at all levels, from execution to top management, at the company or group level. Practical experience in implementing various international methodologies and frameworks in different domains - Cobit, ITIL, BS 7799, ISO/IEC 27001, CMMi, PMP, Prince 2, Lean, Six Sigma, ISO 9001, SoX, BPM, COSO, GRC, etc.

Interesting Facts on Cybersecurity and Data Privacy

 BY PECB

In today's digital age, cybersecurity and data privacy are more important than ever. Cybercrime is on the rise, with devastating consequences for individuals, businesses, and governments. Here are ten interesting facts about cybersecurity and data privacy that highlight the urgent need for better protection.

1. The first computer virus was created in 1971 by a programmer named Bob Thomas. Known as the "[Creeper virus](#)," it was harmless, but it laid the foundation for more malicious viruses to come.
2. Cybercrime is expected to cost the world [\\$10.5 trillion annually](#) by 2025. This staggering amount includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, and more.
3. The [Yahoo data breach in 2013](#) was the largest in history, affecting all three billion Yahoo accounts. The breach was not discovered until 2016, and it took until 2017 for Yahoo to publicly disclose it.
4. The [WannaCry ransomware attack in 2017](#) affected more than 200,000 computers in 150 countries. It spread rapidly by exploiting a vulnerability in Microsoft Windows and demanded payment in bitcoin to unlock users' files.
5. The average cost of a [data breach in 2020](#) was \$3.86 million. This includes the cost of detection and escalation, notification, response, and lost business.
6. Cyberattacks on healthcare organizations increased by 45% in 2020, according to a report by [Check Point Software](#). The COVID-19 pandemic made healthcare systems particularly vulnerable, as hackers targeted medical research and vaccine development.
7. International Data Corporation (IDC) says AI in the cybersecurity market is growing at a CAGR of 23.6% and will reach a market value of [\\$46.3 billion](#) in 2027.



8. Research by [Pew Research Center](#) found that only 52% of Americans use two-factor authentication to protect their accounts, even though it significantly reduces the risk of unauthorized access. Using strong and unique passwords, along with two-factor authentication, is crucial for protecting personal and sensitive information.
9. The cybersecurity job market is expected to grow by 31% from 2019 to 2029, according to a report by [Burning Glass Technologies](#). This growth is driven by increasing demand for professionals with cybersecurity skills across all industries.
10. The [Internet Crime Complaint Center](#) (IC3) received a record 791,790 complaints of suspected Internet crime in 2020, with reported losses exceeding \$4.2 billion. The most common types of reported crimes were phishing and extortion.
11. Phishing attacks account for 90% of data breaches, according to [Cisco's 2021 Cyber Security Threat Trends report](#). These attacks target the weakest link in security: users.

Conclusion

These eleven facts demonstrate the critical importance of cybersecurity and data privacy in today's world. From the first computer virus to the growing cybersecurity job market, it is clear that this field is constantly evolving. It is essential for individuals, businesses, and governments to take cybersecurity seriously and implement effective measures to protect sensitive information.

Therefore, to ensure the needed security and protection, organizations need to constantly stay up to date with the latest news, trends, regulations, and policies.



ChatGPT Draws Privacy Regulator Ban As the UK Government Sees AI as Good for Business

 BY TIM HUNT

ChatGPT has hit the headlines again as serious data privacy concerns have surfaced about potentially damaging personal information being used to feed the world's first free general Artificial Intelligence (AI).

ChatGPT is a web-based virtual assistant that can understand and respond to questions and conversations like a human, and its launch sent tidal waves around the world when it was released by its owners, OpenAI, without warning.

To make the ChatGPT brain work, OpenAI developers allowed the AI to gorge on 45 terabytes of text data which is equivalent to billions of words and sentences from a wide variety of sources, such as books, articles, and websites, as well as scrape data from a variety of publicly available sources.

When ChatGPT appeared, Privacy Regulators – like most of the world – were stunned by its performance but were immediately under pressure to understand how this complex technology worked and determine if it was safe.

Italy's Privacy Regulator – the Italian Data Protection Authority – was quick to investigate and the [first to respond publicly](#). They discovered that data used to train ChatGPT contained personal information of its citizens and immediately issued a ban citing concerns over inappropriate content and privacy violations with the General Data Protection Regulation (GDPR) – a law established across Europe in 2018 to protect individuals' personal data and privacy.

One step behind the Italian Regulator, Canada announced on April 5th that it [had launched an investigation](#) alleging the collection, use, and disclosure of personal information without consent was not in keeping with their laws. Its Privacy Commissioner, Philippe Dufresne, stated:



“We need to keep up with and stay ahead of – fast-moving technological advances.”

Keeping up with AI appears to be a much harder job when the way the ChatGPT black-box brain processes data and spits out its responses stumps even the brightest scientists. Furthermore, ChatGPT is not alone, but just one of a host of new Generative AIs launching at speed to market, and each is trained, computes, and responds differently depending on algorithms, the data they are trained on, and the controls set by the developers.

Across Europe, Data Protection Authorities have yet to unite and decide how to react to ChatGPT and other generative AIs, but there may be pressure from the central coordinating European Data Protection Board in Brussels for all 26 EU Regulators to quickly consider a joint approach.

Britain’s Reaction

Back on British soil, the UK Government is almost certain to not support any type of ban against ChatGPT or any AI technologies.

The Government’s Department for Science, Innovation, and Technology and the UK Data Privacy Regulator (the ICO who report directly to Parliament with sponsorship by the Department for Digital, Culture, Media, and Sport) are aligned, and even share the same sentiment when describing British compliance laws as a “burden.”

[On March 29, the UK Government](#) launched a white paper on the use of Artificial Intelligence stating that: “... organizations can be held back from using AI to its full potential because a patchwork of legal regimes causes confusion and financial and administrative burdens for businesses trying to comply with rules.” However, the white paper also emphasises that AI must comply with “existing laws” and not discriminate against individuals or create unfair commercial outcomes.

This is all very laudable, but this is where the white paper loses its brilliance.

The Role of the Government and the ICO

The UK’s privacy law is known as the Data Protection Act 2018 (DPA18), and it is, essentially, the UK’s implementation of the EU General Data Protection Regulation (GDPR).

If the Government truly has the DPA18 in its crosshairs to make changes for the betterment of business, what does the independent UK Regulator, the Information Commissionaires Office (ICO), have to say about it?

The answer came just 24 hours later on March 30, in [an ICO email newsletter](#) that arrived from the ICO who are responsible for enforcing the DPA18 (UK-GDPR).

In that, the ICO stated: “In our ICO25 strategic plan, we said we would create a practitioner forum as part of our efforts to reduce the burden and cost for organizations of complying with the laws we regulate.”

It is uncanny that the Department for Science, Innovation, and Technology, and the entirely separate body of the ICO, seem to share the same narrative – even down to the same word – and that both consider the current UK Privacy law a “burden” to business. The fact is, the DPA18 (UK-GDPR) was never designed around creating business benefits but was set to protect the fundamental rights and privacy of personal data of individuals within the UK.

A Necessary Change

Technical progress is essential for the development of the economy of Britain. However, AI feels very different in terms of speed to market, speed of adoption, and its claims of accelerated productivity. It is also a threat to jobs, incomes, our rights to privacy, and the fundamental way we conduct our lives.

More than 1,800 signatories of a letter calling for a six-month pause on the development of AI systems “more powerful” than that of GPT-4 (ChatGPT’s successor) was [signed by Elon Musk](#), scientist Gary Marcus, Apple co-founder Steve Wozniak, and computer engineers from Amazon, DeepMind, Google, Meta, and Microsoft. What this letter will achieve is unknown, but it seems a fair request if only all countries signed up for it and AI was halted – which they will not – and it has not.

Without a doubt, AI is here to stay and will have a significant impact on stimulating future growth and the competitiveness of UK businesses, but the trade-off in terms of privacy and its affecting lives negatively is critically important to debate and places us all in a moral dilemma.

The Achilles Heel of the Government’s Plan

It is not hard to understand the Government’s motivation to try and move Britain ahead of the competition but tinkling with the Data Protection Act to try and shoehorn AI benefits for business into this law, but the Government’s approach may be both deeply flawed and a naïve ambition.

Even if the UK adjusts its Privacy laws to make it easier for British businesses to play with AI, the UK does not exist in a vacuum, and any organization within Britain that processes, stores, collects, or sucks up any personal data of citizens of another country, may need to comply with the respective other country's Privacy laws.

GDPR has extraterritorial reach beyond its own geographic boundary. And, there are several other data privacy laws worldwide that have the same global powers. Thus, no matter what UK officials alter within the DPA18 (UK-GDPR), British companies will still have an obligation to manage any 3rd country's personal data in compliance with all those other foreign laws. Therefore, why not just stick within the global gold standard of GDPR and have done with it?

Currently, countries with extraterritorial reach include; Canada with its Personal Information Protection and Electronic Documents Act (PIPEDA), Brazil's Lei Geral de Proteção de Dados (LGPD), California's Consumer Privacy laws (CCPA/CPRA), and myriad other global-effect privacy laws in Australia, Japan, China, and this list is ever increasing.

UK Adequacy Also at Risk

Additionally, there are further and deeper concerns that may dampen the enthusiasm of the UK Government and British businesses keen to tinker with the UK version of the GDPR.

Currently, Britain sits in a privileged but very precarious position in terms of EU personal data flowing in, out, across, and between the UK and the European Union countries. Post Brexit, the European Commission agreed to provide the UK permission to continue open data flows with the EU because, at that time, the UK's privacy laws were consistent with the EU's General Data Protection Regulation (GDPR), although Britain rebranded this as the UK DPA18.

However, this adequacy agreement with the EU is not permanent and was provided with a four-year sunset clause for review in 2025. Hence, if the European Commission gets an inkling that Britain is making changes to the DPA18 before that deadline – and those changes no longer provide a similar level of data protection for EU citizens – the European Commission can revoke or suspend the adequacy decision immediately resulting in a new and endless waltz of paperwork, red tape, and rubber stamps that will cost British businesses dearly in time and money.



Twenty-Six EU Regulators on the Hunt

In addition to battling the complexity of retrofitting laws to the tune of AI, there is also another thunderous Data Privacy storm about to blow across Europe, but this time driven by real humans called the European Data Protection Board (EDPB).

The EDPB in Brussels is leading a coordinated campaign with 26 European Data Protection Authorities charged with targeting and assessing any organizations they deem fair game – large, medium, and super-sized – to find out which are failing to provide company Data Protection Officers with adequate resources, seniority, tools, training, staff, budgets, and executive support to meet their day-to-day Data Privacy tasks as mandated by the GDPR.

This is a clear signal that the EDPB are displeased that GDPR has been taken off the boil for too long, and by too many organizations since its launch in 2018, which indicates that the EDPB know that companies are failing to resource their Privacy teams properly, resulting in poor compliance with the GDPR.

Part of the drop in focus on GDPR and data privacy can be blamed on COVID-19, the pressures of business change, and remote working. Additionally, the volume of hacks, ransomware, and other IT vulnerabilities seems to have won far more attention and budget from Boards nowadays, and the funds have likely been reallocated away from the Data Privacy Officer (DPO) to the Chief Information Security Officer (CISO).

To Privacy Regulators, however, these commercial challenges are of little concern. Privacy Regulators are charged with focusing on protecting the privacy rights of individual data subjects – not business operating costs – and they want to see organizations invest appropriately by using Articles 37 to 39 of the GDPR as the stick to take organizations to task for not supporting their DPOs effectively.

What to Do Next

There was a reason why GDPR was launched to a grand fanfare five years ago, and that purpose is in front of us today.

GDPR is fundamentally about protecting human rights and the privacy that we all want and value. Right now, we need to trust that GDPR – and DPA18 in the UK – is fit for purpose, and we must trust in Regulators to enforce this for the benefit of individuals and society as a whole.

In terms of the next steps for businesses considering what to do:

AI technologies like ChatGPT are here to stay so understand their value and innovate consciously to ensure progress remains consistent with corporate values and compliant with the GDPR and other privacy laws that apply.

In terms of decision-making, as well as the technical and usual teams that are involved in innovation, include ethics, corporate social responsibility, risk, and compliance, and not only ask “What do we think” but also “How do we feel” as there are moral dilemmas to debate as well.

Data privacy has never been more important than in this AI evolution because the guiding Regulation is the GDPR, and there is a great benefit – and risk mitigation – in bringing a DPO with a proactive, positive, and commercial mind-set to the top table to offer advice and help to navigate this.

A great deal has changed since GDPR came into effect five years ago, so look again at your internal Privacy Office and assess if it is still able to deliver against the essential compliance requirements today and that privacy by design is integral to any innovation or change.

Most useful is to carry out a high-level Privacy Audit to help the Board understand what gaps exist, what to do to close those gaps, what the priorities are, and identify where future efforts, funds, and personnel need to be deployed.

AI has significantly increased the stakes in terms of opportunity and risk – so rather than do what you have done before, seek out new ways to face these new challenges.



TIM HUNT

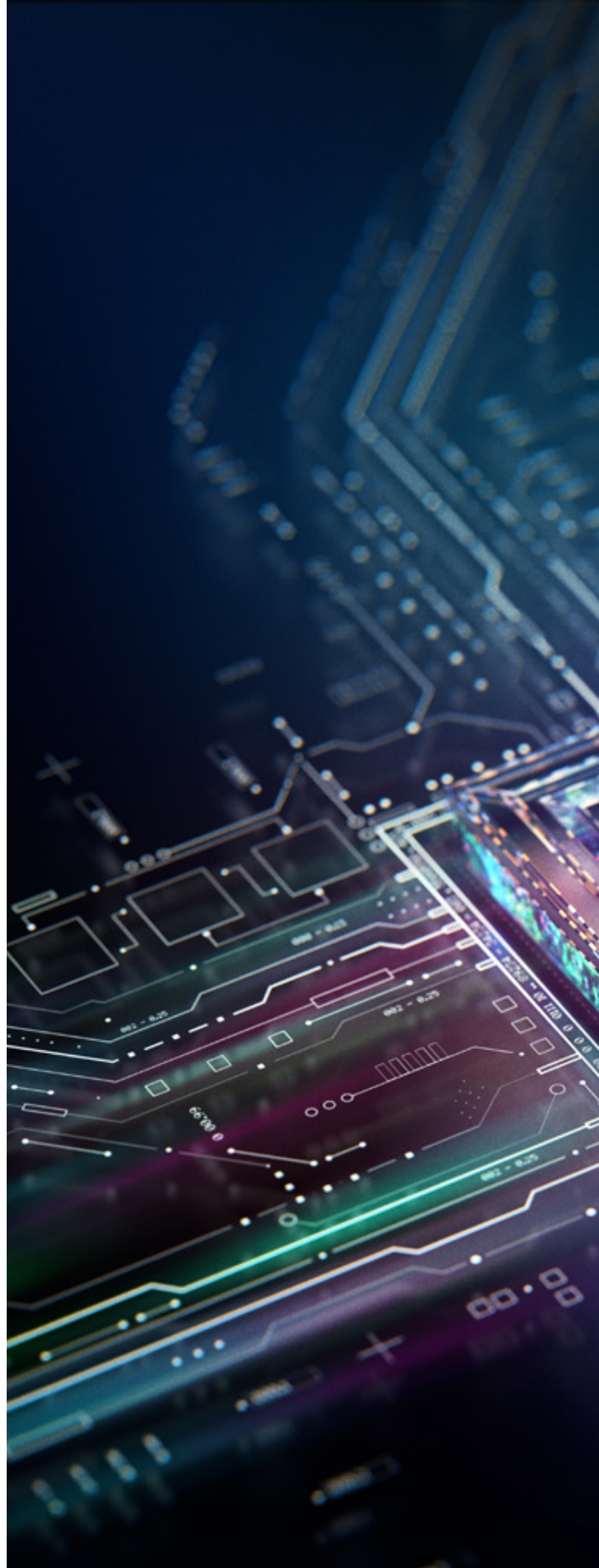
CIPP/E, Independent Data Privacy, and Data Protection Specialist - DPO

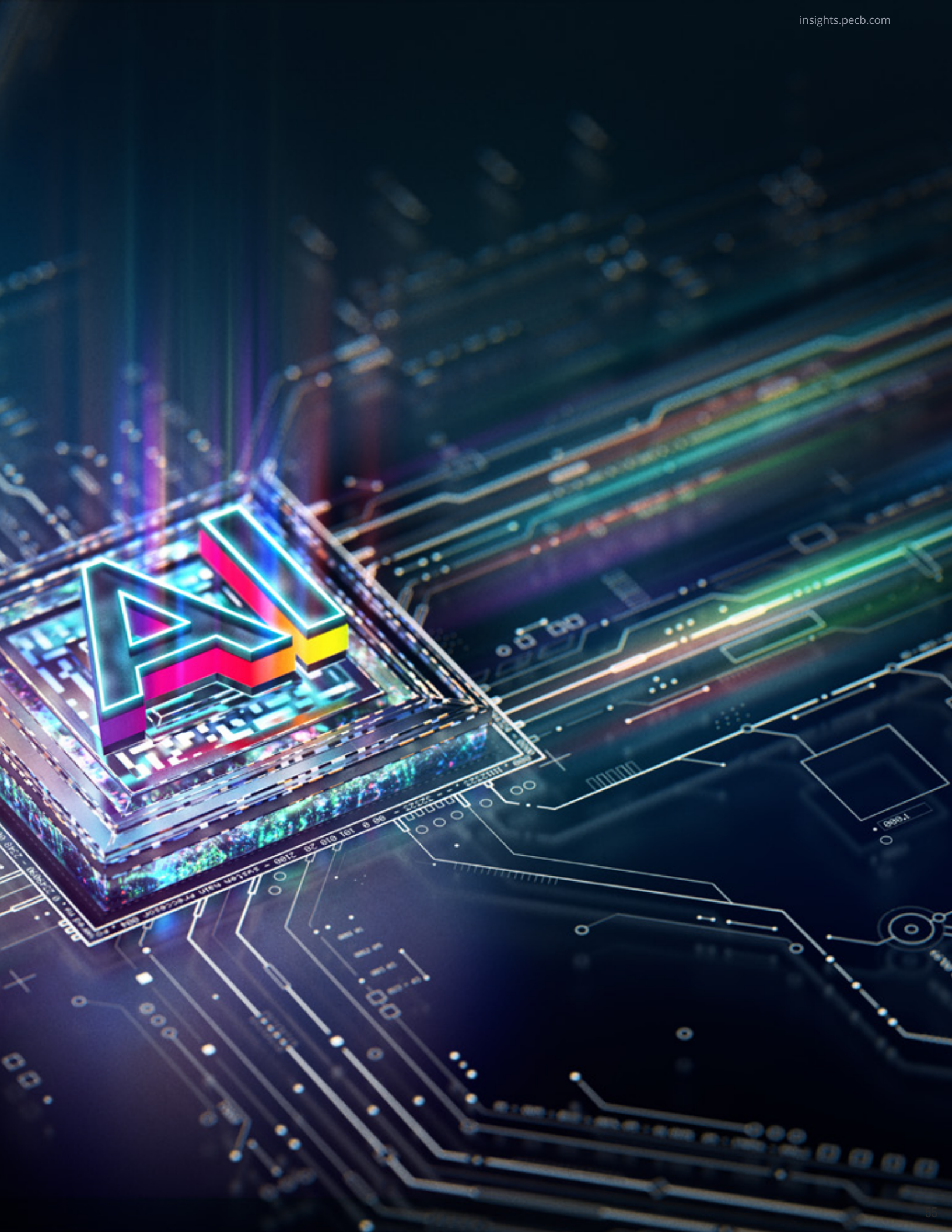
in

Tim Hunt is an experienced Data Privacy specialist who has worked with a dozen-plus UK, EU, and international organizations since the rise of GDPR

in 2018, and delivers a wide range of independent DPO services from audits, assessments, and privacy-by-design consultancy to developing frameworks, delivering training, advising on breach and DSAR handling, as well as executing ROPAs, PIAs, LIAs, policies, notices, and much more.

Prior to specialising in Data Privacy, Tim enjoyed a successful corporate career in technology and marketing and was appointed CMO of two international Boards, as well as co-founded a UK IT Managed Services company. You can reach him at: timhunt@thdpo.com





The Art of Maintaining a Good Work-Life Balance

 BY PECB

In today's fast-paced world, finding a balance between work and personal life has become increasingly challenging. The demands of our professional lives often seep into our personal time, leading to stress, burnout, and a diminished quality of life. However, attaining a healthy work-life balance is not an impossible achievement. By adopting effective strategies and prioritizing self-care, individuals can reclaim control over their lives and enjoy the benefits of a better-balanced lifestyle.

This article explores the importance of work-life balance, provides practical tips to achieve it, and highlights the positive impact it has on our well-being.

Understanding the Importance of Work-Life Balance

Work-life balance refers to the steadiness between one's professional commitments and personal life. It involves distributing time and energy to various aspects, such as work, family, friends, hobbies, and self-care. Maintaining a good work-life balance is essential for several reasons. Firstly, it promotes mental and physical well-being, reducing the risk of stress-related illnesses and burnout. Secondly, it enhances productivity and job satisfaction, as you are more focused and motivated when you have time for relaxation and personal pursuits. Lastly, a healthy work-life balance strengthens relationships and fosters a sense of fulfillment and happiness.

Here are some key reasons why work-life balance matters:

- **Health and Well-Being:** Maintaining a good work-life balance is essential for our overall health. Continuous stress, long working hours, and neglecting personal needs can lead to burnout, fatigue, and various health issues. By finding a balance between work and personal life, we can reduce stress levels, improve our well-being, and enhance our ability to cope with challenges.
- **Increased Productivity and Performance:** Contrary to popular belief, working longer hours does not



necessarily equate to increased productivity. In fact, overworking can lead to diminishing returns, as fatigue and stress can hamper cognitive function and creativity. When we prioritize time for rest, self-care, and personal activities, we replenish our energy and motivation, leading to higher levels of productivity, focus, and efficiency when we do work.

- › **Enhanced Relationships:** A healthy work-life balance allows us to nurture and invest in our relationships with family, friends, and loved ones. Strong personal connections provide emotional support, a sense of belonging, and contribute to our overall happiness. When we have time for meaningful interactions and shared experiences, our relationships thrive, and we feel more connected and fulfilled in our personal lives.
- › **Personal Growth and Fulfillment:** Achieving work-life balance enables us to pursue personal goals, hobbies, and interests that contribute to our personal growth and fulfillment. Engaging in activities outside of work allows us to explore our passions, develop new skills, and expand our horizons. It nurtures our sense of identity beyond our professional roles, leading to a greater sense of purpose and satisfaction.
- › **Prevention of Burnout:** Burnout is a state of chronic physical and emotional exhaustion that results from prolonged work-related stress. It can lead to decreased motivation, cynicism, and reduced job satisfaction. Maintaining a work-life balance helps prevent burnout by providing opportunities for rest, relaxation, and rejuvenation. It allows us to recharge our energy and maintain a sustainable level of engagement and enthusiasm in our work.
- › **Increased Happiness and Well-Rounded Life:** Striving for work-life balance is ultimately about creating a happier, more fulfilling life. It allows us to enjoy the fruits of our labor while still having time for personal pursuits, hobbies, and experiences that bring us joy and fulfillment. It enables us to lead a more well-rounded life where we can excel professionally while also nurturing our personal needs and relationships.
- › **Role Modeling for Others:** By prioritizing work-life balance, we set an example for our colleagues, peers, and future generations. We show that success does not have to come at the expense of our well-being or personal lives. By role modeling a healthy work-life balance, we inspire others to seek their own balance and challenge the long-ongoing notion that work should consume all aspects of our lives.

Understanding the importance of work-life balance empowers us to take charge of our lives, make intentional

choices, and create a sustainable and fulfilling lifestyle. It is a continuous journey of self-awareness, evaluation, and adjustment. By striving for a better work-life balance, we prioritize our well-being, nurture relationships, and create a meaningful and satisfying life that encompasses both professional success and personal fulfillment.

Setting Priorities and Boundaries

To achieve a good work-life balance, it is crucial to establish clear priorities and set boundaries. Start by identifying your core values and what truly matters to you. Determine the activities and relationships that bring you joy and fulfillment outside of work. Once you have a clear vision of your priorities, communicate them effectively to your employer, colleagues, and loved ones. Negotiate realistic expectations and establish boundaries regarding working hours, availability, and personal time. Utilize time-management techniques to optimize your workday. Prioritize tasks, delegate when possible, and learn to say no to non-essential commitments that could infringe upon your personal time. By setting these boundaries and sticking to them, you will create a healthy separation between your professional and personal life.

Here are some key aspects to consider when setting priorities and boundaries:

- › **Reflect on Your Values and Goals:** Take the time to reflect on your values, long-term goals, and what brings you fulfillment in life. Understanding what truly matters to you will help you identify your priorities. Consider your personal life, relationships, health,



career aspirations, and personal growth. This reflection will serve as a guide when making decisions and allocating your time and energy.

- **Communicate Your Priorities:** Once you have identified your priorities, it is crucial to communicate them effectively to those around you. Share your goals and commitments with those that surround you. Articulate your boundaries and expectations regarding schedules, free time, and set apart time. By communicating your priorities, you establish clear expectations and create a foundation for a healthy work-life balance.
- **Negotiate Realistic Expectations:** Work with your employer and colleagues to negotiate realistic expectations that align with your priorities. Advocate for a workload that is manageable and reasonable. Discuss deadlines, projects, and responsibilities to ensure that they are realistic and achievable within the time frame provided. Negotiating realistic expectations will help prevent work from overwhelming your personal life and contribute to a healthier balance.
- **Learn to Say No:** It is important to learn to say no to non-essential commitments that may infringe upon your personal time or overwhelm your workload. Prioritize tasks and evaluate whether additional requests align with your goals and priorities. If a request does not align or would significantly impact your work-life balance, politely decline or suggest alternative solutions. Remember that saying no is not a sign of weakness; it is a way to protect your time, energy, and well-being.
- **Create Boundaries:** Avoid checking work emails or taking work-related calls outside of designated working hours. Communicate these boundaries to your colleagues and ensure that they are respected. Additionally, create physical boundaries by designating specific spaces for work and personal activities. This separation helps create a psychological distinction between your professional and personal life.
- **Schedule Personal Activities:** Block out dedicated time for personal activities and self-care in your schedule. Treat these activities as non-negotiable commitments, just like you would with work-related tasks. Allocate time for hobbies, exercise, relaxation, and spending quality time with loved ones. By scheduling personal activities, you ensure that they are given the same importance as work-related responsibilities.
- **Practice Work-Life Integration:** In some cases, it may be more suitable to aim for work-life integration rather than strict separation. Depending on your personal and professional circumstances, finding ways to blend work

and personal life can create a more fluid and balanced approach. For example, you might schedule breaks during the workday to attend personal appointments or engage in personal activities, or you might have the flexibility to work remotely and design your schedule around personal commitments.

Remember that setting priorities and boundaries is a continuous process that requires evaluation and adjustment. Your priorities may evolve over time, and it is important to reassess and realign your boundaries accordingly. Regularly evaluate whether your actions align with your priorities and make necessary adjustments to maintain a healthy work-life balance. By setting clear priorities and boundaries, you empower yourself to make intentional choices, protect your personal time, and ensure that both your professional and personal life receive the attention they deserve. Achieving a good work-life balance is about finding harmony and fulfillment in all areas of your life.

Time Management and Work Efficiency

Effective time management is crucial for maintaining a good work-life balance. Start by organizing your tasks and schedule. Use digital tools, such as calendars or task management apps, to keep track of deadlines and appointments. Break larger tasks into smaller, more manageable ones, and allocate specific time slots to focus on them. To enhance productivity, minimize distractions during work hours. Disconnect from social media, silence notifications, and create a dedicated workspace that fosters concentration.





Practice time-blocking, where you assign specific time periods for specific tasks, ensuring a balanced workload and avoiding excessive multitasking. Remember to take regular breaks throughout the day. Short breaks can recharge your energy, improve focus, and prevent burnout. Use these breaks to stretch, meditate, or engage in activities that help you relax and reset.

Here are some strategies to improve time management and work efficiency:

- › **Prioritize and Plan:** Start by identifying your most important tasks and goals. Prioritize them based on urgency and importance. Break down larger tasks into smaller, more manageable steps. Use tools such as to-do lists, task management apps, or project management software to keep track of your responsibilities and deadlines. Set realistic and achievable goals for each day, week, or month. By planning and organizing your workload, you can stay focused, avoid feeling overwhelmed, and accomplish tasks more efficiently.
- › **Avoid Multitasking:** While multitasking may seem like a way to get more done, it often leads to decreased productivity and increased stress. Instead, focus on one task at a time. Give it your full attention and complete it before moving on to the next. Single-tasking allows you to maintain focus, work more efficiently, and produce higher-quality results.
- › **Time Blocking:** Allocate specific time blocks for different types of tasks or activities. By assigning dedicated time slots for specific work-related activities,

meetings, and personal tasks, you create a structured schedule that allows for a balanced workload. This technique helps prevent tasks from spilling over into personal time and ensures that you have allocated sufficient time for both work and personal life.

- › **Eliminate Time Wasters:** Identify and eliminate activities or habits that consume your time without adding significant value. Examples include excessive social media use, unnecessary meetings, or constant email checking. Set boundaries around these activities and allocate specific time slots for them, rather than allowing them to interrupt your work or personal time.
- › **Delegate and Outsource:** Learn to delegate tasks that can be handled by others, whether it is assigning work to colleagues or outsourcing certain responsibilities. Delegating not only frees up your time but also allows others to develop their skills and contribute to the team. Identify tasks that can be effectively handled by someone else and distribute the workload accordingly.
- › **Take Regular Breaks:** While it may seem counterintuitive, taking regular breaks actually enhances productivity. Allow yourself short breaks throughout the day to rest and recharge. Use these breaks to take a walk or engage in activities that relax and refocus your mind. Stepping away from work for a short period helps prevent mental fatigue, improves concentration, and reduces the risk of burnout.
- › **Continual Improvement:** Regularly evaluate your time management strategies and reflect on what is working and what can be improved. Experiment with different techniques and adjust your approach as needed. Seek feedback from colleagues or mentors who excel in time management. By continually refining your time management skills, you can optimize your efficiency and create more room for personal activities and relaxation.

Remember that effective time management is not about filling every minute with work. It is about allocating time wisely, maintaining focus, and creating a balance between productivity and personal well-being. By managing your time effectively, you can accomplish your work responsibilities efficiently, leave space for personal activities, and achieve a better work-life balance.

Ultimately, by implementing these time management strategies, you can reduce stress, increase productivity, and create more opportunities for meaningful engagement in both your professional and personal life.

Prioritizing Self-Care and Well-Being

Maintaining a good work-life balance requires prioritizing self-care and nurturing your well-being. Engage in activities that promote physical and mental health, such as regular exercise, proper nutrition, and sufficient sleep. Make time for hobbies and interests that bring you joy and relaxation. Create boundaries between work and personal time by establishing a self-care routine. Dedicate specific periods each day for self-care activities, whether it is reading, pursuing a creative hobby, or spending quality time with loved ones. Disconnecting from work during these periods will help you recharge and improve your overall well-being.

Here are some key aspects to consider when prioritizing self-care:

- **Physical Health:** Taking care of your physical well-being is essential for overall balance. Participate in regular exercise to keep your body active and release endorphins, which can boost mood and reduce stress. Incorporate activities you enjoy, such as walking, yoga, or dancing, into your routine. Additionally, ensure you have a balanced diet that includes nutritious foods and stay hydrated throughout the day.
- **Mental and Emotional Health:** Protecting your mental and emotional well-being is equally important. Practice mindfulness and stress management techniques, such as meditation or deep breathing exercises, to cultivate a sense of calm and clarity. Engage in activities that bring you joy and help you unwind, such as reading, listening to music, or practicing a hobby. Prioritize activities that promote relaxation and recharge your mental energy.
- **Rest and Sleep:** Prioritize sufficient rest and quality sleep. Establish a consistent sleep routine and ensure you allocate enough time for restful sleep each night. Create a comfortable sleep environment that promotes relaxation, such as a cool, dark, and quiet bedroom. A well-rested mind and body are better equipped to handle the demands of work and personal life, reducing the risk of burnout.
- **Leisure and Recreation:** Dedicate time to engage in activities that bring you pleasure and relaxation. Pursue hobbies or interests that you are passionate about, whether it is painting, gardening, playing a musical instrument, or engaging in sports. These activities provide an outlet for self-expression, help you disconnect from work-related stressors, and contribute to a sense of fulfillment.



- **Social Connections:** Nurturing relationships with loved ones and maintaining a social support system is crucial for one's well-being. Schedule quality time with family and friends, participate in social events, and foster meaningful connections. Engaging in positive social interactions provides emotional support, boosts mood, and strengthens overall mental health. Remember, prioritizing self-care is not a selfish act; it is a necessary investment in your well-being.

By taking care of yourself, you become better equipped to handle the demands of work and personal life, leading to increased productivity, improved mental health, and a greater sense of balance and fulfillment. Incorporate self-care activities into your daily routine and make them non-negotiable.

Treat self-care as a priority rather than an afterthought. Remember that self-care looks different for everyone, so identify the activities that resonate with you and align with your values and interests. By prioritizing self-care and well-being, you cultivate resilience, maintain a healthier work-life balance, and enhance your overall quality of life.

Building a Supportive Network

Surround yourself with a supportive network of family, friends, and colleagues who understand the importance of work-life balance. Cultivating meaningful relationships is a crucial aspect of maintaining a good work-life balance. This can provide invaluable support, encouragement, and guidance along the way.

Here are some key aspects to consider when building a supportive network:

- › Family and Friends: Strengthening relationships with family and friends who prioritize work-life balance can make a significant difference. These are the people who understand your commitments outside of work and respect your need for personal time. They can provide emotional support, help you decompress, and offer valuable advice based on their own experiences.
- › Colleagues and Peers: Cultivating a supportive network of colleagues and peers who share similar values can be beneficial. Connect with like-minded individuals at work or in professional networks who understand the challenges of maintaining work-life balance. Share strategies, exchange tips, and collaborate on ways to promote a healthier work environment together.
- › Mentorship: Seek out mentors who have successfully achieved work-life balance or have expertise in managing their personal and professional lives. Their guidance can provide valuable insights, practical advice, and accountability. A mentor can help you navigate challenges, identify opportunities, and offer a fresh perspective on balancing work and personal life.
- › Join Communities or Groups: Engaging with communities or groups that focus on work-life balance can provide a sense of belonging and support. These communities could be online forums, social media groups, or local meetups. Interacting with individuals who are facing similar challenges can provide encouragement, shared experiences, and additional resources for maintaining work-life balance.

Remember that building a supportive network is a two-way street. Offer your support and understanding to others who are also striving for work-life balance. Actively participate in discussions, share your experiences, and provide encouragement and advice to create a supportive environment.

By surrounding ourselves with individuals who prioritize work-life balance, we can draw strength, inspiration, and valuable insights to navigate the complexities of balancing our personal and professional lives. Their support can help us stay motivated, make informed decisions, and remind us that we are not alone in our journey toward achieving a healthy work-life balance.

Conclusion

Maintaining a good work-life balance is not an indulgence; it is a necessity for our overall well-being and happiness. The demands of work should not overshadow the importance of personal time, relationships, and self-care. By understanding the significance of work-life balance and implementing practical strategies, we can reclaim control over our lives and create a harmonious existence. Setting priorities and boundaries, practicing effective time management, and prioritizing self-care, are key to achieving a healthy balance.

It requires conscious effort, discipline, and the willingness to communicate our needs and expectations to those around us. Remember that work-life balance looks different for each individual, and it is important to define what it means for you and align your actions accordingly. Embracing a supportive network can also greatly contribute to maintaining a healthy balance. Surround yourself with individuals who value work-life balance and can provide encouragement and understanding. Seek guidance and support when needed, as it is not a journey to undertake alone.

Ultimately, the pursuit of work-life balance is an ongoing process that requires constant evaluation and adjustment. It may not always be perfect, and there will be times when work and personal life overlap. However, by striving for balance and making conscious choices to prioritize our well-being, we can create a fulfilling and meaningful life that encompasses both professional success and personal fulfillment. Remember, you have the power to shape your life in a way that supports your overall happiness and satisfaction.



The Fundamentals of ISO/IEC 27032 – What You Need to Know

 BY ANTHONY ENGLISH

OPINION

Many days in technology began when the Internet, cell phones, and personal computers did not exist; computers were so large at this time that just one would fill an entire room, and putting information into that computer meant typing your program, line by line, on individual punch cards. And all of that was “state of the art”! Back then, the only IT security that we worried about was the joker who might flip your box of neatly ordered punch cards out of your hands and scramble your program source code before you got it dumped into the computer. Things are very different today, however, the two categories of risk we see in the field of technology and data security do have a basis in the earlier technologies that got us here.

Cybersecurity and information security are the two halves of security that we all strive to apply today: cybersecurity deals with what we also refer to as IT security, e.g., securing routers, firewalls, usernames, etc., while information security focuses on security governance, e.g., policies, standards, etc., and the protection of people and data or assets. ISO/IEC 27032 focuses on IT security or cybersecurity, and ISO/IEC 27001 focuses on information security. Thus, ISO/IEC 27032 covers topics related to applied technology and IT security and is, therefore, very useful to frontline IT and security staff. There is often an overlap between information security and cybersecurity, as there should be, and the two concepts are often, as a result, used interchangeably, but separating them can lead to greater clarity when working in security.

The threats that are faced in the realm of cybersecurity include things like social engineering, hacking, malware, spyware, ransomware, etc., and these topics are addressed in ISO/IEC 27032. Now, you might reply that ISO/IEC 27001 also speaks to these topics and, to an extent, it does, however, ISO/IEC 27032 sees these threats through the lens of preparing for such threats, detecting, and monitoring attacks and responding to any attacks or threats. Historically, IT has sometimes been a background service to the organization, and IT staff were seen as



“that group in the basement” or similar (some TV comedies still use this as a vehicle to deliver laughs!). With this in mind, ISO/IEC 27032 addresses the need for collaboration between IT and others, including internal and external IT clients and any third-party providers to the organization. This last point has been an emphasis on building IT 2.0, where IT is being pulled out of its backroom team mentality to become an integrated part of the organization overall, and information sharing, work coordination, and coordinated incident handling are all covered in ISO/IEC 27032.

All of these elements described above and in ISO/IEC 27032 require some processes that are not typical of where IT evolved from, such as: establishing trust between IT and its clients, establishing processes for collaboration and information exchanging and sharing, and defining technical requirements for systems integration and interoperability across the stakeholder audience. To apply ISO/IEC 27032 correctly, you will obviously need some level of skills in communicating with others and this can sometimes require the ability to communicate technical needs or information in non-technical terms. Not to worry though, ISO/IEC 27032 can help to guide you through all of this – at least at a high level! Cybersecurity then, as defined by ISO/IEC 27032, relies upon application security, network security, and Internet security, and it supports information security and critical information infrastructure protection (CIIP).

Stakeholders and assets are a key focus in ISO/IEC 27032, and the efforts required to utilize controls to address vulnerabilities, threats, and risks that relate to your assets form the baseline of this standard. Industry best practices and innovative technology solutions to address risk and employ organizational security awareness can all be part of a holistic risk management strategy. Because stakeholders can be individuals, e.g., an end user accessing a website, or an organization, e.g., a company trying to protect their website from compromise, the processes for managing threats, vulnerabilities, and risks are varied depending upon to whom, what, and where you are applying them. As we have seen in other recently updated security standards, such as ISO/IEC 27001 and PCI-DSS, the requirements for managing threats have been augmented for both the organization and the individual with increased emphasis on security measures, such as monitoring and alerting for the organization, and requirements for security awareness and involvement all the way to members of the Board. ISO/IEC 27032 addresses these topics from a high level.

Network monitoring and response has its own section in ISO/IEC 27032, which should be a clue to the importance of this security control when it comes to protecting the organization’s network infrastructure and the assets that are accessed via the network. Baselineing your network is a critical step in implementing proper monitoring so that you can monitor for deviations from what are normal operations for your network. In addition, implementing an Intrusion Detection System and an Intrusion Prevention System to help automate the alerting, and possibly automatic blocking of anomalous behavior on your network, are also recommended controls in ISO/IEC 27032. An often-overlooked element of proper protection of your network is having a documented support and escalation process. I have personally assisted with more than a few security incident response events where the client has had to figure out their incident response process in real-time, which is never a good thing when an attacker is already inside your network. Preparing for incidents in advance cannot be over-emphasized as essential for any size of an organization.

The supply chain or third-party relationships are covered in various portions of ISO/IEC 27032, but as we all know, attacks on organizations via third parties that the organization deals with are a new favorite attack vector for hackers. Applying strong third-party security controls, e.g., risk assessments of third parties, security audits of third parties, strong security language in all contracts with third parties, etc., is a common recommendation by security experts globally.

Privacy has also become a cross-domain concern for both privacy and security practitioners, thus, providing a clear security policy on any public website and in any end-user software, usage agreement is important. Apply the privacy principles of use, storage, processing, data management, and data deletion to any privacy policy you create.

ISO/IEC 27032 also speaks to secure development practices, e.g., code review and testing, protection of source code, etc., and the protection of servers, through regular security testing and scans, vulnerability and patch management, QA/Test environments separate from production, secure configurations, etc. These measures can help to protect your organization’s “crown jewels”. For the end user, anti-malware, software updates, phishing protection, personal firewalls, and automated updates are all mentioned in ISO/IEC 27032. I would add a few things here to my security controls list, including; using Mobile Device Management software, web content filtering, and file integrity monitoring.

Social engineering has become a favorite hacker vehicle for delivering ransomware and malware, and for committing fraud. Protection against and end-user training on phishing, vishing, smishing, and physical security threats, e.g., an intruder posing as a telecoms employee while trying to gain access to your offices, are part of ISO/IEC 27032's content although, further details on protecting against these threats are required beyond what is found in ISO/IEC 27032.

Because the world of cybersecurity is constantly evolving, the ISO/IEC 27032 standard must also evolve, and its Annex A helps serve this purpose by providing additional guidance on topics such as Darknet monitoring and utilizing tracebacks, to reconstruct the attack path in a cyber-attack. Before engaging in anything related to the darknet or the dark web, often two terms are thought to mean the same thing, but they do not research how to use these resources safely. For additional reference material, Annex B and Annex C of ISO/IEC 27032 provide some sample additional reference materials and sources.

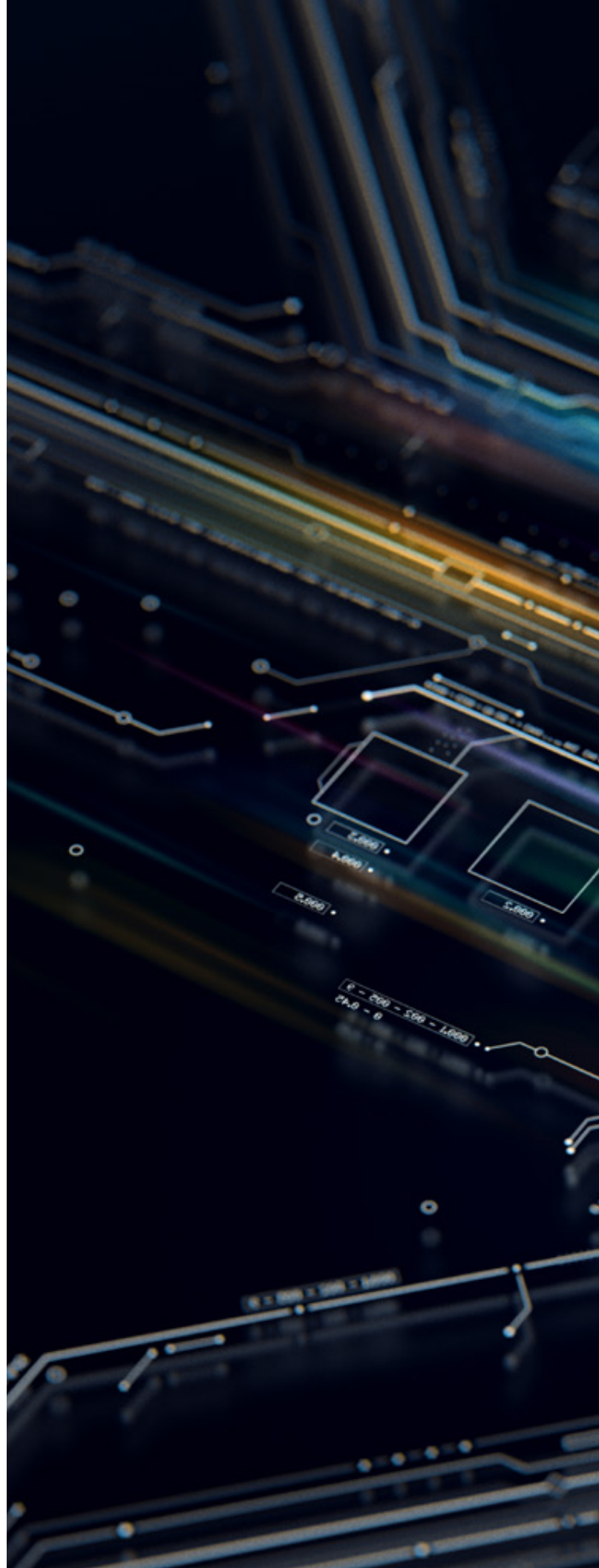
Overall, ISO/IEC 27032 is not written like many other ISO standards; it is more conversational in nature and is meant to provide high-level guidance on how to address cybersecurity in your organization. Combining ISO/IEC 27032 with other ISO resources will provide the best result when you are building your full management system for security and privacy.

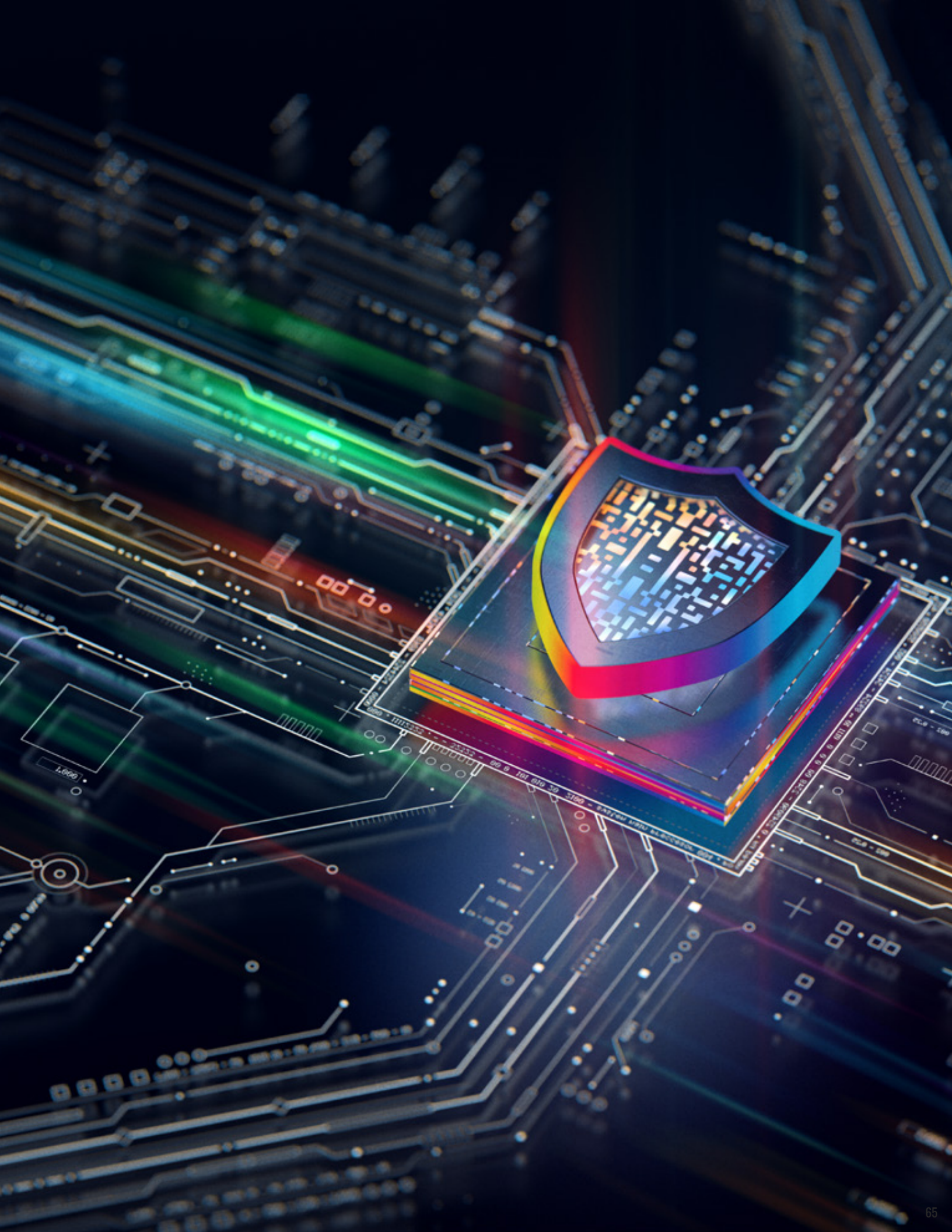


Anthony English
CEO/CISO at Bot Security
Solutions Inc.

Anthony English is a seasoned IT and Security professional with multiple certifications in both disciplines.

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







Data Protection Milestone: GDPR Turned 5

In this digital era, the significance of ensuring security and privacy for your online presence is undeniably evident.

The General Data Protection Regulation (GDPR) is a guideline that enforces stronger data protection for organizations that operate in the European Union (EU) and handle EU citizens' data.

As we celebrate 5 years of GDPR, we invite you to take advantage and make your GDPR compliance easier with PECB's training courses:

- ▶ [GDPR Foundation](#)
- ▶ [GDPR – Certified Data Protection Officer](#)

TANGIER, M

The New Eldorado in t

BUSINESS & LEISURE



MOROCCO

the African Continent!



Tangier sits at the crossroads of trade routes and civilizations – on African soil but just a few miles from Europe’s southern shores. Throughout its history, this exceptional location has attracted merchants, bankers, artists, vacationers, and all manner of adventurers, becoming a cosmopolitan, multilingual place, highly diverse.

Tangier City was able to spur economic growth and create jobs for its rising population, especially given that it is not endowed with oil or natural gas reserves, as opposed to many other regions. Tangier created new jobs three times as fast as Morocco as a whole, with an employment growth rate averaging 2.7% and 0.9% per year, respectively, while also outpacing national GDP growth by about a tenth.

The geographical location of Tangier City is considered a very strategic pathway to Europe, America, and the Middle East. In 2000, Tangier City grabbed the Royals’ attention for transforming the city into a business hub in the Mediterranean region.

The Moroccan central government embarked on a massive investment in infrastructure, including the vast new state-of-the-art Tangier-Med Port, and the modern high-speed train system “Al Boraq” catalyzing the distance between Morocco’s two major economic poles: Tangier-Casablanca has a modern rail system and road links, upgraded airports, as well as a range of market-opening initiatives, such as free trade agreements, open skies airline travel, and relaxed investment and visa regimes. Such measures benefitted the whole country in general, but especially, gateway cities such as Tangier.

The Royal and Moroccan government support is very significant and has a direct impact on fostering existing and future FDIs. Indeed, many government bodies were created for this purpose, mainly Tangier Mediterranean Special Agency (TMSA) and associated governing entities such as Tangier Free Zone (TFZ), Tangier Med Port Authority, and Tangier Automotive City, TAC I and TAC II.

These national enabling interventions were accompanied by highly successful local ones. The city and regional governments embarked on a host of “place-making” initiatives to improve the quality of life for Tangier’s residents and visitors alike, from better water supply and waste management to the preservation of green spaces, restoration of cultural monuments and beaches, and reduced traffic congestion and pollution through more effective geospatial planning. Meanwhile, the city’s old port of Tangier Ville is being redeveloped, helping to attract cruise ships, and allowing the construction of a new Marina.

Tangier’s Renaissance can in part be attributed to its reliance on an innovative public-private delivery model for national and local policies rather than a more conventional government-only approach. Displaying a nimbleness and flexibility more typically associated with private-sector firms, corporatized entities such as the Tangier-Med Special Agency (TMSA) bring together various stakeholders involved in trade, investment attraction, workforce development, and regional decision-making.

Such an approach has contributed to Tangier’s ability to be responsive to the needs of private-sector investors, especially foreign ones, as exemplified by the establishment of cutting-edge facilities to train workers with the skills needed for Tangier’s emerging industries like automotive and aerospace.

Kansai International Management has had its head office in Tangier since its venture design outset back in 2013 and has led the way in international technology, and best practices transfer mainly in Japanese high-tech industries, such as Lean Industry 4.0 and Waste to Energy 2.0. Kansai International Management has accumulated distinctive know-how enabling the transfer of technology and best practices process to turn challenges into business opportunities that drive success.

Kansai International Management Tangier head office has been pioneering in the introduction to the Northern city corporate and business community, mainly in Tangier Free Zone, Tangier Med, and later on Tangier Automotive City I and II PECB certification solutions.



“Since 2015, PECB certification programs have gained tremendous traction in the Moroccan industry with a growing pool of professionals operating in Multinational companies across Tangier Free Zones operating in automotive, aerospace, and agri-business industries, respectively.”

The ever-increasing demand from multinational companies that are leading the Moroccan industry with the highest number of senior professionals desiring to pursue state-of-the-art certifications from the globally leading organization in the certification industry, PECB Group Inc., commonly speaks on the benefits derived from having these career-booster solutions providing peerless know-how and second-to-none expertise.

PECB certifications enable professionals to demonstrate their skill attainment within their business. It also provides a competitive edge when applying for other positions as it not only identifies the person as attaining a recognized level of competence but also importantly identifies that person as one who will extend extra effort for their personal and professional development.

PECB certifications underscore the understanding of the Moroccan skilled workforce about the updated management principles and best practices and provide them extra credibility in the competitive job market.

Kansai International Management strongly believes that PECB peerless certifications are a key factor in senior management job titles and salary progression – definitely a return on the time and cash invested. PECB certifications really capped Moroccan professional career path development and added a pinnacle level of success in the Moroccan industry.

Tangier has successfully capitalized on its inherent advantages, geographic, cultural, linguistic, and industrial, to attract investment and tourists, upgrade new technologies and workforce skills, and help local firms integrate into global supply chains; it has focused on attainable and realistic goals, not merely aspirational ones.

In the scope they have, local leaders have demonstrated strong business acumen and a capacity to act in concert and effectively utilize information feedback loops, ensuring the responsiveness of higher tiers of decision-makers in Morocco.

Finally, the city’s manageable size, about a million inhabitants, makes it easier to get things done, as most key players know each other and interact on an almost daily basis. Without the interplay of such factors, Morocco’s massive investment in infrastructure could have amounted to a little more than just concrete poured onto a once-pristine Mediterranean beach.

By 2020, Tangier Med Special Agency “TMSA” enlisted Japanese Trading House or “Sogo Susha” in Japanese Sumitomo Corporation to sell five industrial parks, spanning 13 square kilometers, near the northern port city



of Tangier, across the Strait of Gibraltar from Spain. The two companies will consider a joint venture to create such parks in the North Moroccan city.

Goods and commodities shipped by sea from Tangier can reach destinations in the EU within a week. Tangier Med port has reached an annual shipping container capacity of more than 10 million, 20-foot equivalent units in 2022, the largest of any African or Mediterranean port and with lower labor costs than in Eastern Europe.

The Royal and both central and local governments are determined to foster the transformation of Tangier into an internationally competitive business and industrial cluster, which is of utmost importance at all levels. Kansai International Management Tangier and Tokyo Office are able to provide FDI support services for Japanese multinational companies willing to invest in the automotive industry in the Tangier region of Morocco.

Kansai International Management can guide Japanese companies through a one-stop shop service, aiming to streamline the installation process, offer 360 degrees services, and support Japanese investors all along their setup process in the Tangier Med industrial platform in compliance with international standards.

Kansai International Management thrives to assist foreign investors in all their procedures, such as; permits, contract agreements, driving licenses, facility management, shared secretariat, lower corporate tax rates, reduced customs duties, and shortened logistics formalities. We can undertake Market Research and Business Intelligence, Environmental Impact Assessment, assistance in benefiting from Moroccan government subsidies, financial assistance for the acquisition of land or construction of manufacturing sites, and many other business support activities for Japanese FDI.

Kansai International Management brand is a parent corporate endorsing the six sub-brands, all registered trademarks in Morocco:

- › Kansai Invest
- › Kansai Capital
- › Kansai Pharma
- › JAPAN Bridge
- › JAPAN Factory
- › JAPAN Wings

With networks across different sectors of the economy, Kansai International Management is able to give guidance to any company looking for sustainable growth.

Top Tourist Destinations and Must-Visit Natural and Historical Sites

1. Cave of Hercules

Situated merely 14 kilometers west of Tangier, the popular tourist attraction draws many tourists. The cave holds geological and mythological importance, as legend has it that Hercules rested here during the “12 Labors of Hercules”. The view here is quite spectacular, considering the cave has two openings, one facing the sea and the other facing land.



2. Cap Spartel

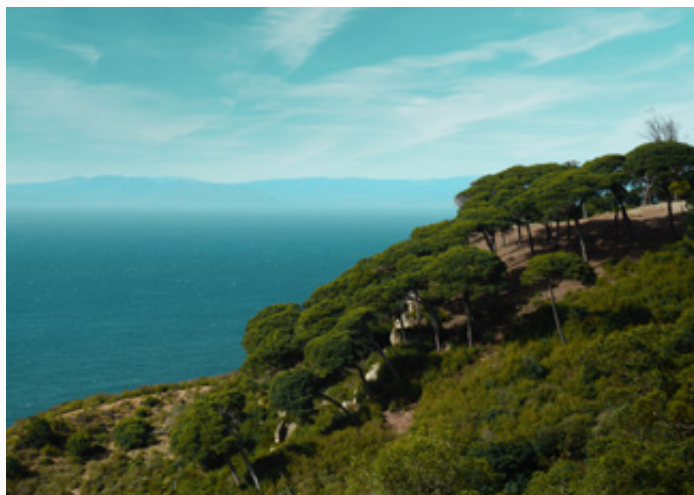
On Morocco's northern Atlantic coast, 12 kilometers west of Tangier, on the far northwest coast of Africa, is Cap Spartel. Sultan Muhammad III constructed Cap Spartel in 1864, and it is situated near the entrance to the Strait of Gibraltar, roughly 1,000 feet above sea level. The lighthouse looks down on the water that joins the Atlantic Ocean with the Mediterranean Sea, the Strait of Gibraltar. And if the weather is good, you will be able to see Spain from this landmark.



3. Perdicaris Park

The Perdicaris Park, also known as the Rmilat Forest and formerly as Villa Aidonia or Place of the Nightingales, is a public park covering 70 hectares in the Rmilat neighborhood of Tangier, Morocco. The lovely park offers many botanical explanations, a lovely sea view, and many Spanish-style villas to explore.

It is worth visiting for a picnic or a walk around the park to enjoy the views that it offers. A museum is also situated within the park for those interested in the historical aspect.



4. Tomb of Ibn Battouta

An important Moroccan figure, Ibn Battuta, who was born in Tangier in 1304 and became the greatest traveler of the period – outpacing Marco Polo, traveled extensively throughout the medieval world as a Muslim Berber Moroccan scholar and adventurer. Ibn Battuta traveled to several non-Muslim countries as well as the majority of the Islamic world during the course of thirty years, including Central Asia, Southeast Asia, India, and China.



5. Villa Harris Park & Museum

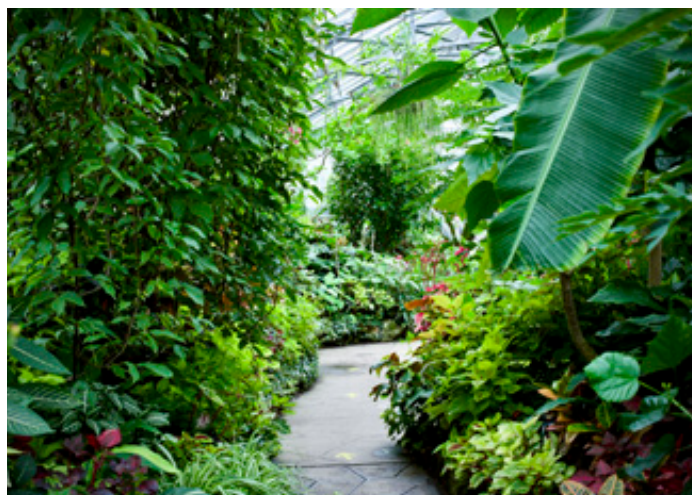
This is a brand-new public park created from Villa Harris's gardens. The landscape is stunning, rotating between big trees, shrubs, grass, and flowers. The deep roots of some of the old trees are where the flowerbeds are. Walter Harris, a renowned London Times correspondent, lived on this property. On the site, his Moorish palace is slowly being renovated. Children's playgrounds and a sizable parking space are available in the gardens. Nowadays, both the museum and the park are contributing to the beauty of the city even more.



6. Donabo Botanical Gardens

A unique place in Tangier. A must for all nature lovers and enthusiasts as it offers a real escape in an extraordinary garden.

This garden oasis is the ideal location to unwind and enjoy the breathtaking views of Morocco's scenery. The garden is situated on Jbel Kebir, which is also known as the big mountain.



7. Tangier American Legation Museum

Morocco was one of the first countries to recognize the newly independent United States of America, therefore, the legation was established here in Tangier.

The museum stands as the only US historic museum outside of the US. With beautiful architecture, characterized by its arches, window grills, several courtyards, research libraries, and private museums, it most certainly is worth a visit.



in

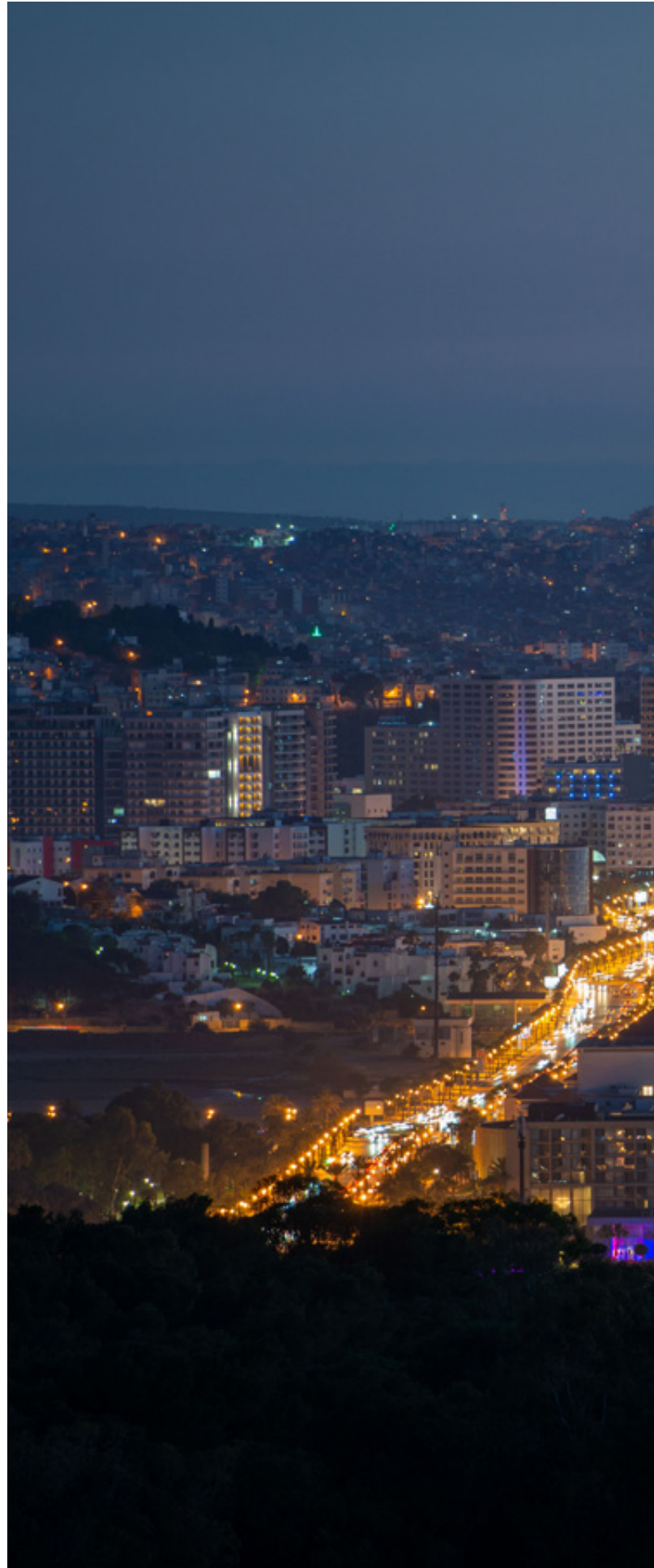
Mohammed CHANAOU

Owner, Founder, and Managing Director at Kansai International Management Co.,Ltd

Mohammed Chanaoui is the Managing Director of North and West Africa at World Leader in Lean 4.0 Industry Inc.,

and Owner, Founder, and Managing Director of Kansai International Management Co., Ltd. Mohammed holds a Bachelor and Master of Science in Industrial Management from Kansai Gaidai University, Japan.

Mohammed has succeeded in an astounding career where he developed a key strategic, managerial, and technical set of skills through many extensive years as senior Project Manager within APMG International and Blackstone Inc., as Project Managing Director for a Waste to Energy Project, Plant Quality Manager for Treves Automotive, Plant Program Manager for Exco Automotive, both operating in Tangier Free Zone and as Project Manager Assistant within Toyota Motor Corporation Global Headquarters in Toyota Aichi Japan.





Establishing an Evolving Work Environment Through Security Measures



BY MICHAËL RAISON

In today's fast-paced digital world, cyber threats and privacy breaches are a growing reality. The increasing number of cyber-attacks in recent years has put businesses under immense pressure to take adequate measures to ensure their security. To establish a secure and evolving work environment, it is essential to cover all the cybersecurity pillars for a 360° approach. Companies must strengthen their cyber resilience posture day after day, step by step, to stay ahead of evolving threats.

Organization types vary. At Approach, when we cover the defense and aerospace industrial base, we are playing the cybersecurity Olympic games every day, placing the bar very high. In literature, most cybersecurity specialists and influencers define their final goal based on higher results because they know that the further we protect the systems, the further the hackers will strengthen their attacks.

In practice, this strategy is not realistic for everybody today, and the objective looks too high for the majority. Less technological organizations or smaller ones might have a lower dependency on cybersecurity, even if all organizations want to protect their critical assets and their intellectual property, also known as the crown jewels. Even in the defense sector, some companies are not there yet. Many companies need to start with a step-by-step approach. As cybersecurity specialists, we need to adapt.

Also, companies evolve at a fast pace. Over the course of cybersecurity audits and implementations, it is common to find that companies have different departments evolving at a specific speed. In this context, the management of conflicts appears, and we need to place cybersecurity versus business growth cursor with additional care. Precedence between several cybersecurity priorities, standards, and practices becomes part of the daily negotiation.

To stay competitive, organizations need to give free rein to design and offer a competitive "time to market."



This attitude often presents conflicts with the hyper-structuring requirements for cybersecurity. Therefore, it is crucial to establish continuity in a company's cybersecurity strategy and DNA, and make the cybersecurity structure and basic hygiene effortless for the departments.

Without a doubt, the cyber risk analysis is not one-shot. The proper management of information and necessary controls must continue over time. It is, therefore, imperative to implement security measures that enable businesses to establish an evolving work environment that can adapt to changing cyber threats and safeguard against potential breaches.

Establishing the Right Roadmap and Strategy

The strategic methodology for establishing an evolving work environment through security measures requires a roadmap based on frameworks and standards that match your organization's needs. EU companies usually apply EU standards first, such as ISO/IEC 27001. US companies follow their own way, i.e., the National Institute of Standards and Technology (NIST) frameworks.

The defense sector has its own requirements, such as Cybersecurity Maturity Model Certification (CMMC). Whatever the applied standard, conducting cybersecurity assessments and audits will help the creation of a risk-based strategy that identifies potential threats and vulnerabilities. Assessment tools can enable efficient and continuous assessments over time, allowing organizations to track their progress and adjust their cybersecurity posture as needed. You need the right experts with the right tools to ensure this within your organization.

Companies should also consider testing and stimulating some real-world scenarios and exercises within the company to define realistic objectives, such as metrics, Key Performance Indicators – KPIs, etc., that evolve with the company. Certification can also demonstrate the cybersecurity posture to the market, which is either a business enabler or a showstopper today. You also need the right experts with the right tools for demonstrating this.

A CISO (Chief Information Security Officer) must be in place to carry the company's tailored “anticipate and prevent” mechanisms, with sharp advice, pragmatism, and preciseness. For sensitive and critical activities (Network and Information Security – NIS 2.0, Defence, etc.), you need a well-experienced CISO with a broad market set of references in your sector. The CISO needs a team. For many organizations, money is the sinews of war,

and the question of cyber cost leans two ways: teams will request a cybersecurity budget, and shareholders will ask for a Return on Investments (ROI) that covers this budget. The CISO is the right role to identify the right security posture and ROI, along with management.

This can be very penalizing for nascent stars whose ROI is difficult to demonstrate. However, starting on the wrong foot and taking the wrong shortcuts would lead to banning innovation if it is data-related or cyber-dependent. Yet cybersecurity is an opportunity for innovation. A company that manages to overcome cyber difficulty, including the innovation department, has an advantage over others. Therefore, organizations should see cybersecurity as an opportunity to innovate and differentiate themselves from their competitors.

More than this, we see more companies driving their change management with the help of cybersecurity messages that nobody can refute.

Adapting To the Right Situation Together, At the Company Speed

The journey towards establishing an evolving work environment through security measures requires adapting to the right situation and pace together with the company's speed. It is not a one-time effort but a continuous process that involves protecting applications, infrastructure, systems, identity and access management, networks, and cloud systems. It is crucial to detect and respond to potential threats with the right security operations team that has the right size, skills, tools, and with 24/7 coverage. Preparing for recovery after a compromise is also essential and should be part of daily activities when implementing a strong business continuity plan.

To begin their cybersecurity journey, organizations must ask critical questions, such as whether the cybersecurity need is global or localized to a specific activity. They must also consider whether it is useful to have a “secure project factory” and whether a single project can take on the global cyber effort. Furthermore, they must determine the minimum and the maximum cyber effort that is essential and bearable and establish who will do the work. These questions are vital to ensure that the cybersecurity approach is practical, pragmatic, and effective.

Each change in the company, i.e., new project, product or service, new structure, merger and acquisition, new applicable law, etc., reflects a cyber journey as well.

For larger organizations, these questions can be centralized at the group level and replicated for a set of entities. However, certain freedom must be adjustable at each level according to the local need. Additionally, most organizations rely on strong partners or subcontractors. The cybersecurity requirements flow down, and assessment and control are, therefore, necessary. It is not unusual to call for external and neutral specialists in this case; those specialists will use known frameworks and tools to proceed with the partner cybersecurity roadmap without affecting the business relationship.

Today, the cybersecurity path and speed are highly influenced by regulations and strong contractual requirements. Consequently, organizations must stay informed and updated on these changes, ensuring that they are compliant and continuously improving their cybersecurity posture. Establishing an evolving work environment through security measures is an ongoing process that requires a holistic and risk-based approach, continuous improvement, and adaptation to changes in the industry.

Adapting Just In Time Because Of a High Risk or an Incident

As a decision-maker, it is crucial to understand that cybersecurity is not a one-time event but an ongoing process. A proactive approach to cybersecurity is always recommended, but in case of a high-risk situation or an incident, an organization should be prepared to adapt its cybersecurity measures quickly to mitigate the risk.

The first step is to identify the potential threat or incident and assess its impact on the organization's assets, data, and reputation. Once the situation is understood, it is essential to act quickly and implement immediate measures to contain the situation. This can include isolating affected systems, disabling network access, and restricting access to sensitive information.

Next, it is important to notify the appropriate experts to assist with the investigation and recovery process. This can include IT professionals, forensic specialists, and legal counsel. They will help identify the root cause of the incident, recover data, and provide guidance on how to prevent similar incidents in the future.

A key aspect of adapting cybersecurity just in time is continuous monitoring and testing of the organization's security measures. Regular vulnerability scans and penetration testing can identify weaknesses that can be exploited by attackers. Implementing robust incident response plans and conducting regular training for employees can also help mitigate the impact of a cybersecurity incident.

Cybersecurity Posture Changes along Time and Space

When it comes to cybersecurity and resilience, there are different types of entities outlined in the NIS 2.0 Directive, such as Vital, Essential, Important, and those that are not within the scope of the directive. Even within your own organization, some departments or activities may fall into these categories or may not be important for cybersecurity at all. The level of risk appetite in your organization may also change depending on various factors like investments, board consciousness, and threats.

For example, your financial department may be more important to protect than your marketing department, or the reverse, depending on your company.

It is important to note that your organization's risk appetite may also change over time.

You need to adapt your security posture to the evolving need. Most activities will not be able to support the strongest requirements, like in the Defense and AeroSpace industry.



Usually, a one-size-fits-all cybersecurity approach will not work or be efficient. Some departments or users may require a higher level of security than others. Your organization may need to be very careful when segregating the company and its different operational aspects. The main goal is to prevent contamination and ensure business continuity in the event of a major incident or attack.

To do this, you should adopt a fine-grain cybersecurity strategy that prioritizes your investments where they are most needed. Your organization should have a strict separation of duties and silos to avoid contamination and permit business continuity in case of an attack or major incident. A fine-grain cybersecurity strategy is the best way to invest your resources where they are needed the most. You can even create an evolving strategy based on factors like alert levels, trusted networks, and company layers.

A company must be prepared to adapt its cybersecurity measures quickly in response to a high-risk situation or an incident. This requires a proactive approach to cybersecurity, continuous monitoring, testing of security measures, and quick action to contain the situation and notify the appropriate experts. With these steps in place, a company can better protect its assets, data, and reputation. These elements are the reasons why we are present and strong in the market.

In conclusion, by taking a tailored approach with the help of experienced cybersecurity specialists, you will ensure the best return on investments for the cybersecurity measures you implement in the evolving work environment.

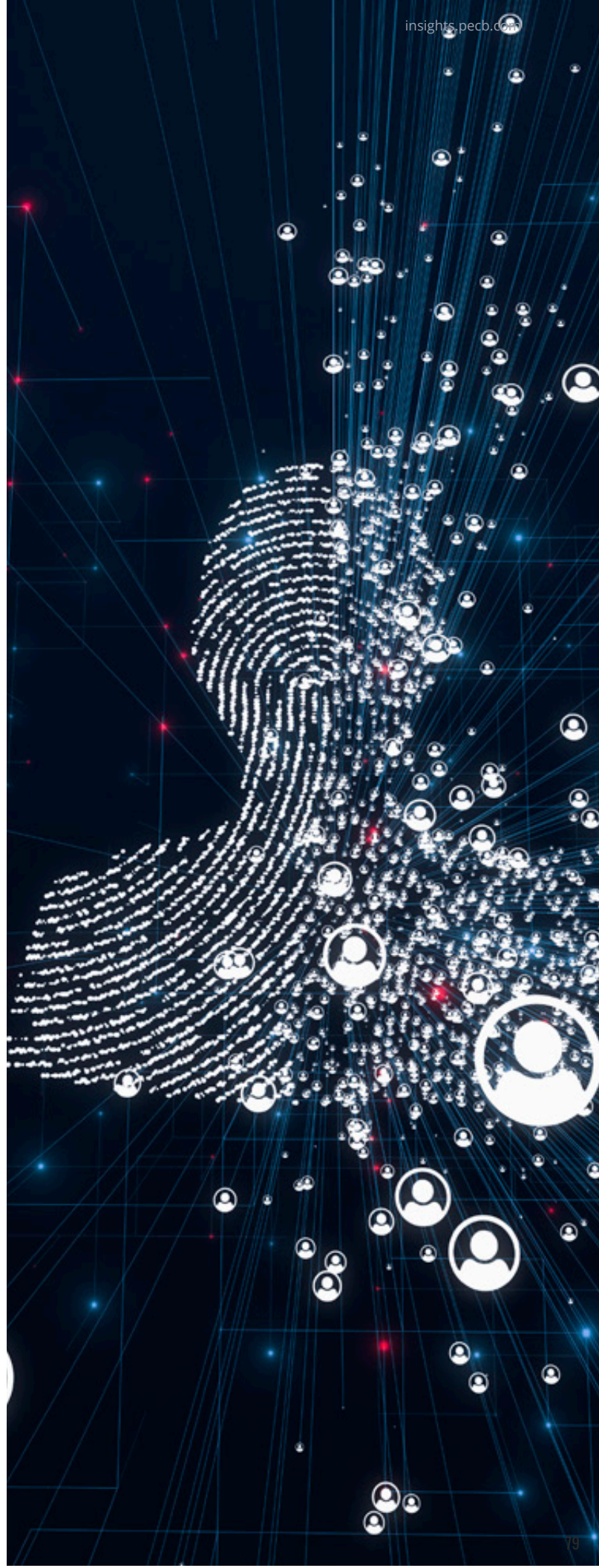


Michaël Raison
Consultant for Approach

Michaël Raison is a trained and certified specialist with over 20 years of experience in management roles, as lead auditor, and coaching for cybersecurity.

Currently Head of Compliance and Risk and CISO for Sabca group, and advisor for many companies in the defense and aerospace sector in Belgium, at board level, including trade compliance, physical security, business ethics, and sustainability.

As a board member of the Cyber Made in Belgium for the Defense initiative, he is currently building and reinforcing the defense and aerospace industrial base, including the aspects of NIS, CMMC, and Industry cybersecurity.



Q&A from the Webinar

“ISO/IEC 27001, CYBERSECURITY, AND RISK MANAGEMENT – HOW TO AVOID DATA BREACHES”

Cybersecurity risk management is very important when it comes to maintaining the assets of an organization. Simon Lacey and Nick Frost, two renowned experts, came together to provide a comprehensive exploration of the subject matter during August 2022 in the PECB Webinar.

If you missed the live session or have burning questions that remained unanswered during the webinar, this is your chance to gain invaluable knowledge and clarification.

Question: In the case of a risk assessment project in a process where the involved parties could not get to an agreement on how to categorize risk, who should be the one to decide on the risk?

Answer: If it is a case of categorization, i.e. how to describe the risk, then you should refer to the SME, so if it is a cyber risk, then it should be the CISO. However, if it is an operational risk, then possibly the head of operational risk or the CRO. If the categorization is to do with the actual rating or description that is given to the risk, then again it should be the SME for the risk area (e.g., cyber, finance, operational, legal, etc.), and they need to provide the applicable evidence as to why the risk is of a certain rating.

Question: How to successfully execute risk identification according to ISO/IEC 27001 requirements?

Answer: The standard ISO/IEC 27001 states that a risk assessment is to be conducted to identify risk and the controls to reduce likelihood or consequence. However, it does not specify the specific process of a risk assessment – although it refers to guidance, such as ISO/IEC 27036 and ISO/IEC 27005, which are the main ISO documents for information risk assessment. There are many solid approaches to identifying risk using a structured process based on sound risk logic. In my experience, my recommendation for using a risk methodology in the context of ISO/IEC 27001, would be to follow a rigorous approach to ensure that the identification has been based on objective thinking.



Question: In terms of transparency, at what point should you start telling your clients about a data breach?

Answer: There will be legal and regulatory requirements for informing independent bodies that uphold privacy rights, such as the UK’s ICO, so this would be one of the groups to inform first. Many of these bodies can also guide you on how to approach clients as well. But what is important is to ensure you have a plan to investigate how the breach occurred (so you can remediate any vulnerabilities) and understand the extent of the breach (number of records, details, and individuals that may be compromised so you can alert them). In addition, your clients may have clauses in contracts that require you to notify them in a defined period of the discovery of a breach.

Question: Based on your experience, could you provide some insight into the prevalence and adoption of cyber insurance in the context of cybersecurity and risk management, particularly concerning preventing data breaches?

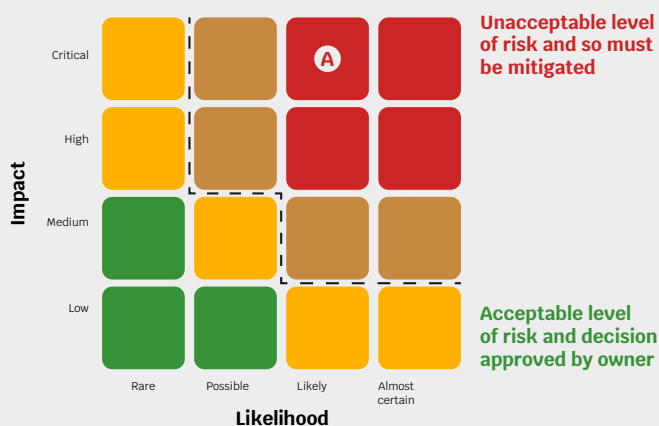
Answer: Five years ago, cyber insurance was considered a key requirement for managing risk. My observations are that organizations are now more aware of what is in and out of the scope of acquiring cyber insurance. A key feature of cyber insurance is that it can provide immediate access to security specialists (forensic cyber professionals) post-incident, but it is unlikely that cyber insurance will act as a preventative measure.

Question: Does a CISO reporting to a 'peer' chief indicate a lack of priority for cybersecurity? Placing the CISO at an appropriate level within the organization is crucial for effective leadership and accountability in this critical area.

Answer: In very general terms, I would say that it is an example of maturity if the CISO is reporting to senior business management or C-level business representatives. We are all aware that cyber risk is a business risk, but this should be reflected through reporting lines, so the CISO has direct access to leadership. In many organizations we work with cyber risk is the top risk, so you would expect the leadership to want to get access to the CISO or equivalent. It is also important for the CISO to be supported if the reporting lines change so that both parties speak a common language of risk.

Question: What are the recommended steps for conducting a risk assessment of a large organization with hundreds of systems, and how can the process be optimized for efficiency and effectiveness?

Answer: It would be prudent to take a triage approach that would act as a pseudo filter to help distinguish between critical and non-critical systems in a situation such as this. Any system that is identified as critical should then undergo a cyber risk assessment.



Heatmap and risk ratings

- Critical level of risk
- High level of risk
- Moderate level of risk
- Negligible level of risk
- Delineating risk appetite



Other features of a cyber risk assessment to consider that help streamline an approach would be to develop a set of re-populated data sets (threat templates, impact reference tables) that reflect certain characteristics of a system, i.e., an internet-facing device that contains credit card details will require a specific set of prepopulated threat templates, specific control library, etc.

Question: Could you please elaborate on the organization's high-risk appetite and how it can be documented and approved through the appropriate structure?

Answer: A common way to reflect an organization with a high-risk appetite would be to use a heat map such as below. The first image shows an organization with a lower level of risk appetite (redder) than the second image (less red).

An organization's risk appetite may reflect a range of factors such as regulatory pressures (likely to have a lower risk appetite), a new venture (likely to have a higher risk appetite), operating in parts of the world that are exposed to more risks such as civil unrest, environmental disasters (and so would have a higher risk appetite).

Question: What is the rationale behind an organization adopting ISO/IEC 27001 for cybersecurity and risk management, and is ISO 9001, which is risk-based, sufficient to cover all aspects of risk management?

Answer: There are many reasons for why an organization would adopt ISO/IEC 20071 – these include requirements of key clients, opening new markets and business sectors, and providing assurance to the existing client base. However, there are other reasons as well, including formalizing existing business practices and enhancing resilience. The easiest way to understand the rationale clearly, is to map interested parties and their requirements of the business and information security.

The standard for information risk management is ISO/IEC 27005, which defines the steps to identify and evaluate risk. ISO 9001 is for quality assurance, although shares many similarities with ISO/IEC 27001 and it is possible to implement both at the same time, despite their different scopes.

Question: Does accepting data breaches reduce reputation risk, or is the greater risk the inability to demonstrate a reasonable state of cybersecurity, which could lead to legal, financial, and reputational consequences for organizations?

Answer: Accepting data breaches and a failure to demonstrate reasonable cybersecurity practices could both lead to reputational consequences.

If a data breach occurs, then it is likely that those individuals that have been affected will notify the information commissioner's office (or equivalent), complain on social media, notify the mainstream media, and soon, which would not take long for negative attention to focus on the organization in question.

Question: What are the best practices for identifying a business's threat landscape and creating a risk register? The process can be daunting, with the challenge of knowing where to start. Could you guide an effective and efficient approach to this process?

Answer: It would be best to start with a recognized cyber risk standard.



Any such standards will have a threat list, threat taxonomy, and a process to enable you to assess your threat landscape. But be aware that terms such as threat, vulnerability, impact, and risk need to be well understood to objectively assess risks to the organization.

Question: How can the cybersecurity industry address the issue of victims of cybercrime suffering financial loss and reputational damage with little legal recourse? By creating a more balanced playing field, there is greater potential for collaboration in identifying and prosecuting cybercriminals.

Answer: The cybersecurity community is helping victims of cybercrime as many organizations release threat data into the public domain, and recommend practices to protect yourself and your family from cybercrime. However, I do believe more can be done as we are seeing the cost of cybercrime continue to soar, for example:

1. Independent bodies that can collate and analyze sources of threat intelligence to warn citizens of the latest scams
2. Addressing barriers when law enforcement agencies are collaborating across multiple jurisdictions to track individuals that are responsible for such crimes
3. Free access to technologies that can be used on home laptops – several governments now provide some simple but effective tools that can help address vulnerabilities that could lead to cybercrime

Question: What steps can organizations take to proactively secure more funding for cybersecurity initiatives, rather than relying on a reactive approach after a cyber-attack?

Answer: Establishing an understanding of cyber risks for your organization is key to providing a robust business-focused argument as to what level of investment is a need and where it needs to target, and as you have mentioned establishing a proactive approach.

Conducting a program of cyber risk assessments over time will generate a rich source of data, that when analyzed, will identify key risk trends (i.e., the most common risk that has the biggest 'potential' impact on an organization, most common threat types, etc.).

These trends must be reported to senior management, so they understand the potential consequences to the organization.



Question: Which approach is better for risk management: scenario-based or asset-based? What factors should organizations consider when choosing an approach?

Answer: A hybrid approach would be best. When you are conducting an asset-based risk assessment, you should be using scenarios to enrich discussion when assessing the components of risk nevertheless, i.e. presenting scenarios such as the possible sequence of impacts following a data breach and scenarios when determining the sequence of threats that could occur from a targeted attack.

Question: What are the key areas that organizations in under-resourced regions like the Caribbean should focus on to enhance their cybersecurity posture, and how can they prioritize these areas in the absence of sufficient resources?

Answer: It would be best to focus heavily on scenario-based activities. If there are limited resources and funding to help prevent such cyber-attacks from occurring, then you have to fall back on “what do we do when attacks occur”.

It is something all organizations must do anyway, but for those similar to yourselves that are under-resourced, it is important that the focus is on how to respond to an attack and bring back the systems, and processes back in a minimal amount of time.

Question: When considering assets that matter for risk management, how can organizations factor in availability as a critical component? For example, if a system experiences prolonged unavailability, how does this impact the overall risk posture?

Answer: Assessing availability and the impact should be part of a business impact assessment.

The business impact assessment will consider the types of impact (reputational, operational) and respected levels (critical, high) based on a breach of confidentiality, integrity, and availability. When assessing availability, you need to consider the impact based on the length of the outage.



Nick Frost

Co-founder and Lead Consultant at CRMG.

in

Nick’s career in cyber security spans nearly 20 years. Most recently Nick has held leadership roles at PwC as Group Head of Information Risk and at the Information Security Forum (ISF) as Principal Consultant. In particular, Nick was Group Head of Information Risk for PwC designing and implementing best practice solutions that made good business sense, prioritized key risks to the organization, and helped minimize disruption to ongoing operations.

Whilst at the ISF Nick led their information risk projects and delivered many of the consultancy engagements to help organizations implement lead thinking in information risk management. Nick’s combined experience as a cyber risk researcher and practitioner designing and implementing risk-based solutions places him as a leading cyber risk expert. Prior to cybersecurity and after graduating from UCNW and Oxford Brookes Nick was a geophysicist in the Oil and Gas Industry.



Simon Lacey

Principal Information Security Consultant

in

Simon is a resourceful, creative Information and Cybersecurity professional with a proven track record of instigating change, disrupting the status quo, influencing stakeholders, and developing a ‘big picture’ vision across business populations. Multiple industry experience; excels in building stakeholder engagement and consensus, and supporting organizations to make sustainable change.

Simon also has considerable experience in risk management, education and awareness, strategy development and consulting with senior management, and is a confident and engaging public speaker. Simon has previously worked within the NHS, Bank of England, and BUPA, before setting out as an independent consultant forming Oliver Lacey Limited, supporting clients in multiple business sectors.

When not working, Simon loves to run – currently training for the Berlin Marathon, a Director of Aylesbury United Football Club, records vlogs, and is an experienced standup comic.

UPCOMING WEBINARS ▶





PECB INSIGHTS 2023 CONFERENCE

JOIN US ON 4-5 OCTOBER, 2023

**It is Closer Than
it Looks!**

Get ready for an unforgettable experience because the PECB Insights Conference 2023 is just around the corner! Join us on 4-5 October, 2023, in the vibrant city of Paris for two action-packed days of learning, networking, and making meaningful connections.

This year's conference will feature 12 panel sessions focused on Information Technology, Security, and Privacy, with 6 sessions conducted in English and 6 in French. Check out the complete agenda by clicking [here](#).

In addition, we are happy to present the launching of the two following Pre-Conference Training Courses:

- ▶ **Chief Information Security Officer**
- ▶ **NIS Directive 2.0**

These will be held in a hybrid format, where the first two days will be held online on 18-19 September, followed by two days in-person in Paris on 2-3 October.

Standard Ticket	\$499 \$399	Includes only panel sessions on 4-5 October
Pre-Conference Ticket	\$1399 \$1,299	Includes only one hybrid training course
Premium Ticket	\$1499 \$1,399	Includes both a training course and panel session access

We are confident that the PECB Insights Conference 2023 will be an excellent opportunity for you to advance in your career and stay up to date with the latest developments in IT, security, and privacy. Register now and do not miss out on this chance to learn from industry leaders and share your thoughts with peers.

Join us in Paris and experience the excitement for yourself!

REGISTER HERE ▶

Enroll Now in the **CHIEF INFORMATION SECURITY OFFICER** Hybrid Training Course

Take your cybersecurity career to new heights with our Chief Information Security Officer (CISO) Pre-Conference Hybrid Training course.

- 📅 18-19 September, Online
- 2-3 October, In-Person
- 📍 Renaissance Paris La Defense Hotel
60, Jardin de Valmy 92918 Puteaux, France

Designed for professionals seeking comprehensive knowledge and practical skills in information security management, this intensive program equips you with the expertise to protect organizations from evolving cyber threats.

Meet the Trainer



GRAEME PARKER

Managing Director at Parker Solutions Group
UK and Ireland Managing Director at PECB
United Kingdom

Graeme Parker is a seasoned Cybersecurity and Risk Management professional, with extensive experience in both technical and business aspects of these fields. Having worked with high-profile private and public sector organizations, he has developed a deep understanding of the industry's demands and how to navigate its challenges.

[Read More](#)

Ready to learn, network, and grow?

PURCHASE TICKETS ▶

Enroll Now in the **NIS DIRECTIVE 2.0** Hybrid Training Course

Join our NIS2 Directive Hybrid Training course and strengthen your understanding of the European Union's Network and Information Systems Directive (NIS2).

📅 18-19 September, Online
2-3 October, In-Person
📍 Renaissance Paris La Defense Hotel
60, Jardin de Valmy 92918 Puteaux, France

Designed for professionals working in critical infrastructure sectors, this program provides comprehensive insights into the regulatory requirements and best practices for achieving cyber resilience.

Meet the Trainer



PETER GEELEN

Executive Director & Managing Consultant at CyberMinute
Owner & Managing Consultant at Quest for Security
Belgium

Peter Geelen is a seasoned security professional and the owner and managing consultant of Quest for Security. With over 20 years of experience, he has a proven track record of delivering high-quality services in identity and access management, privacy, information, and data protection, as well as cybersecurity, corporate security policies, security hardening, and cloud security.

[Read More](#)

Ready to learn, connect, and develop?

PURCHASE TICKETS ▶



Gain a Deeper Understanding of Cybersecurity and Data Privacy Through These Books

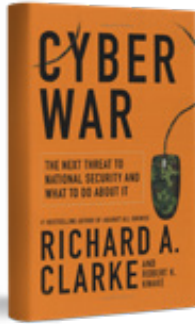
In today's digital age, cybersecurity and privacy have become increasingly important issues. With more and more of our personal and professional lives taking place online, protecting our sensitive information from cyber threats has never been more critical. The field of cybersecurity is constantly evolving, with new threats emerging all the time. To help you stay informed about this important topic, we have put together a list of books that provide insights into the world of cybersecurity and privacy.

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World by Bruce Schneier



In "Data and Goliath," author Bruce Schneier explores the privacy implications of the massive amounts of data collected by governments and corporations. He argues that this data collection has led to a loss of privacy and a shift in power from individuals to those who control the data. Data and Goliath is a well-researched overview of the technological changes and factors which affect our security and privacy. According to the author, technological advancements in cell phones, GPS, the Internet, and computers have created a world in which personal information has become ubiquitous and the potential of it being marketed to and sold by nascent data brokers is greater. This mass collection of data has become a concern, especially in recent years, to most individuals and organizations. The book provides a critical examination of how our personal data is collected, used, and abused by those in positions of power.

Cyber War: The Next Threat to National Security and What to Do About It
by Richard A. Clarke and Robert K. Knake



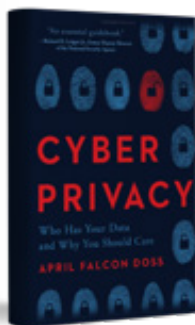
As nations rely more and more on computer technology, the risks posed by cyber-attacks grow progressively more serious and important to a country's economy and security. The book is an easy read for computer scientists, students, professionals in the field of security, or those interested in better understating cyber warfare. "Cyber War" discusses the potential for cyber warfare and the steps that governments and organizations can take to defend against it. This is an essential read for cyber warriors who need to understand the historical context around the evolution of defending any nation in cyberspace, offering valuable insight into the cyber scenarios of modern days. The authors, Richard A. Clarke and Robert K. Knake, both have extensive experience in cybersecurity and national security and provide insights into the threats facing our digital infrastructure. The authors cover important topics that concern security challenges, policies, and prior case studies of cyber warfare, to name a few. The book also provides recommendations for policymakers and individuals on how to protect themselves and their organizations from cyber-attacks.

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers by Andy Greenberg



"Sandworm" provides an in-depth look at the activities of a Russian hacking group known as Sandworm and their attempts to infiltrate critical infrastructure. Author Andy Greenberg, a senior writer for Wired Magazine, provides readers with a detailed account of the group's activities, including their role in the 2017 NotPetya malware attack. We are led to this group of Russian cyber military super-hackers by Andy Greenberg's eccentric writing in the book Sandworm. In order to comprehend the group's goals and potential targets, Greenberg describes the cyber military team's exploits throughout their brief history, as well as the malware experts that are following every lead. We witness the puzzle come together in understanding what and who Sandworm actually is through Greenberg's story. The book also discusses the geopolitical implications of cyber-attacks and the challenges faced by law enforcement in holding cybercriminals accountable. The author talks about the people he visited and spoke with, giving us an understanding of who they are and how they handled the cyberwarfare in their own nations. He conducted a great deal of research, taking the reader with him every step of the way.

Cyber Privacy: Who Has Your Data and Why You Should Care
by April Falcon Doss



An informative and clearly written book tackling the collection of data, by the government and the private sector, to answer your questions on who has your data, why you should care, and what you can do about it. This is an expertly researched guide on the ways your online presence puts you at risk and the ways you can take measures to protect your privacy, online presence, and identity. The author takes the time to provide a walk-through of data privacy origins and the potential impact of our penchant to over-share and its impact on our security. The author develops and complements questions related to personal data use, and not only, raising the question and concern about people's interest in their rights online. It is a comprehensive examination of the way corporations, governments, and social media acquire and use your digital data, and it is a current read, in that it examines issues such as COVID-19 contact tracing, facial recognition technology, and intelligence surveillance of foreign terrorists. This book is equally valuable for the layperson and the expert.



PECB UNIVERSITY
EXISTIMATIO PER VERITATEM



PECB University Congratulates the Recently Graduated MBA Students

The classes of 2020 and 2021 at PECB University have graduated from their MBA programs!

This is a result of their hard work and dedication towards their goals. It is an evidence of their academic and professional education through numerous courses and effective development, implementation, and management.

We wish the students the best in their professional and academic path onwards.

Join the PECB University family. Visit the PECB University [website](#) to get better informed, or contact the PECB University counselor at university.studentaffairs@pecb.com.

Top Five High-Paying Job Positions You Can Pursue with a GDPR CDPO Certification

According to a report by [Finbold](#), there was a total of 984.47 million Euros in GDPR fines only in the third quarter of 2021.

This is a clear indicator of the importance of complying with the GDPR. A GDPR certification helps organizations that handle information of individuals covered by the GDPR in any form. It is an essential form of demonstrating commitment to data privacy and increasing customer confidence, in addition to the obvious necessity for legal compliance.

PECB offers GDPR — Certified Data Protection Officer training course and certification delivered by experienced and expert trainers who will help you to understand the GDPR and how it applies to your organization.

The salaries presented below represent an average that derives from information provided by PayScale, Glassdoor, Zippia, SalaryCom, and ZipRecruiter.

1. Chief Data Officer

Based on the information provided by PayScale, Glassdoor, and ZipRecruiter, the average salary of a Chief Data Officer is **U.S. \$168,058 per year**.

2. Senior Security Consultant

Based on the information provided by PayScale, Glassdoor, and Zippia, the average salary of a Senior Security Consultant is **U.S. \$110,550 per year**.

3. Privacy Manager

Based on the information provided by ZipRecruiter, Glassdoor, and Payscale, the average salary of a Privacy Manager is **U.S. \$106,045 per year**.



4. Data Management Consultant

Based on the information provided by PayScale, Glassdoor, and ZipRecruiter, the average salary of a Data Management Consultant is **U.S. \$99,960 per year**.

5. Data Protection Manager

Based on the information provided by ZipRecruiter, Glassdoor, and SalaryCom, the average salary of a Data Protection Manager is **U.S. \$97,510 per year**.

PECB Certified Data Protection Officer training course provides the knowledge and methods needed to help organizations ensure compliance with the GDPR.

Becoming a Certified Data Protection Officer will enable you to acquire the necessary expertise to understand the risks that could have a negative impact on your organization and implement the required strategic responses based on the GDPR best practices, requirements, and principles.

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

START NOW! ▶



Building Resilience Against Cyber Threats



BY MOHAMMED ABDUL FATAWU

As the world becomes more digitized and complex, cyber threats have become more sophisticated, posing a significant risk to businesses across all industries. Cyber resilience is the ability of an organization to prepare for, respond to, and recover from a cyber-attack, minimizing the impact on its operations, reputation, and financial stability. In this article, I will explore the role of ISO/IEC 27001 and ISO 22301 in building cyber resilience and how they can help you develop a comprehensive cybersecurity strategy that can stand the test of time and assist improve the cybersecurity resilience posture of your organization.

Introduction to Cyber Resilience

Cyber resilience refers to an organization's ability to withstand and recover from cyber-attacks. With the increasing frequency and complexity of cyber threats, it is essential for businesses to have a proactive approach to cybersecurity. Cyber resilience is not just about preventing attacks; it is also about ensuring that your business can continue to operate in the event of an attack.

A cyber-attack can have a significant impact on a business, affecting its reputation, customer trust, and financial stability. Therefore, it is crucial to develop a comprehensive cybersecurity strategy that covers all aspects of cyber resilience, from prevention to recovery.

Understanding the Role of ISO/IEC 27001 in Your Business Strategy

ISO/IEC 27001 is a globally recognized standard for information security management. It provides a framework for organizations to manage and protect their information and security assets from a range of threats, including cyber-attacks. Implementing ISO/IEC 27001 can help businesses to identify and manage information security risks, ensuring that they have a robust and effective information security management system in place.



ISO/IEC 27001 covers all aspects of information security management, from policies and procedures to risk assessment and treatment. It is a risk-based approach that allows organizations to tailor their information security management system to their specific needs.

By implementing ISO/IEC 27001, businesses can demonstrate to their stakeholders that they take information security seriously, giving them a competitive advantage in today's digital landscape.

How ISO 22301 Can Help in Building Cyber Resilience

ISO 22301 is a standard for business continuity management. It provides a framework for organizations to prepare for, respond to, and recover from disruptive incidents, including cyber-attacks. By implementing ISO 22301, businesses can ensure that they have a comprehensive business continuity management system in place, thereby, minimizing the impact of disruptive incidents on their operations.



ISO 22301 covers all aspects of business continuity management, from risk assessment and mitigation to incident response and recovery. It is a holistic approach that enables organizations to identify and prioritize critical business processes, ensuring that they can continue to operate in the event of an incident. By implementing ISO 22301, businesses can demonstrate to their stakeholders that they have a robust and effective business continuity management system in place, enhancing their reputation and customer trust.

The Importance of a Cybersecurity Roadmap for Resilience

A cybersecurity roadmap is an essential tool for building cyber resilience. It is a strategic plan that outlines the steps that a business needs to take in order to achieve its cybersecurity objectives. A cybersecurity roadmap should cover all aspects of cybersecurity, from risk identification and assessment to incident response and recovery.

A cybersecurity roadmap should be tailored to the specific needs of the business, taking into account its unique risks, vulnerabilities, and threat landscape. It should also be regularly reviewed and updated to ensure that it remains relevant and effective in the face of evolving threats.

Incident Response Process for Cyber Threats

An incident response process is a critical component of

cyber resilience. It is a plan that outlines the steps that a business needs to take in the event of a cyber-attack. An incident response process should cover all aspects of the incident, from detection to containment, eradication, and recovery.

An incident response process should be regularly tested and updated to ensure that it remains effective in the face of evolving threats. It should also be communicated to all relevant stakeholders, including employees, customers, and suppliers, to ensure a coordinated response to the incident.

Cybersecurity Report - What It Is and Why It Is Important

A cybersecurity report is a document that outlines the cybersecurity posture of a business. It provides an overview of the organization's information security management system, including its policies, procedures, and controls. A cybersecurity report should also include an assessment of the organization's cybersecurity risks and vulnerabilities, as well as recommendations for improvement.

A cybersecurity report is essential for building cyber resilience. It enables businesses to identify areas of weakness in their cybersecurity strategy and take steps to address them. It also provides stakeholders with a clear understanding of the organization's cybersecurity posture, enhancing their trust and confidence in the business.



Business Resilience Framework for Cyber Threats

A business resilience framework is a comprehensive approach to managing risks and ensuring that a business can continue to operate in the face of disruptions, including cyber threats. A business resilience framework should cover all aspects of business continuity, from risk assessment to incident response and recovery.

A business resilience framework should be tailored to the specific needs of the business, taking into account its unique risks, vulnerabilities, and threat landscape. It should also be regularly reviewed and updated to ensure that it remains effective in the face of evolving threats.

Resilience Assessment - Measuring Your Cybersecurity Resilience

A resilience assessment is a process that enables businesses to measure their cybersecurity resilience. It involves assessing the organization's cybersecurity posture against industry standards and best practices, identifying areas of strength and weakness, and developing a plan for improvement. A resilience assessment should cover all aspects of cybersecurity, from policies and procedures to technical controls and incident response.

A resilience assessment is essential for building cyber resilience. It enables businesses to identify areas of weakness in their cybersecurity strategy and take steps to address them.

Conclusion - The Importance of Cyber Resilience in Today's Digital Landscape

In today's digital landscape, cyber resilience is more important than ever. Cyber threats are becoming more sophisticated and frequent, posing a significant risk to businesses across all industries. Building cyber resilience requires a proactive approach to cybersecurity, including the implementation of globally recognized standards, such as ISO/IEC 27001 and ISO 22301.

A comprehensive cybersecurity strategy should cover all aspects of cyber resilience, from prevention to recovery. It should also be regularly reviewed and updated to ensure that it remains effective in the face of evolving threats. By building cyber resilience, businesses can protect their operations, reputation, and financial stability, enhancing their competitive advantage in today's digital landscape.



in

Mohammed Abdul-Fatawu

Business Continuity Planning
Partner-Operations at
GCB Bank PLC.

Mohammed Abdul-Fatawu is a Certified PECB ISO Trainer for ISO 22301 Lead Implementer and Lead Auditor. ISO 21502, ISO 31000, ISO 37001, ISO 37301, etc. Mohammed has over 14 years of Banking experience spanning over Retail, Operations, Corporate, and Risk Management.

GDPR Turns Five

 BY ALEX CARROLL

Five years ago, on May 25th, 2018, the GDPR became enforceable. To mark this anniversary, Alex Carroll, a privacy consultant at TechGDPR, reflects on the changes that took place in the European privacy landscape over that period, considers the opportunities it has created for organizations and provides some insights into what organizations should look out for in the next five years.

Changes to Date

1. Reactions to Novelty

The fundamental principles of data protection found in Article 5 of the GDPR were not created with the Regulation but had enjoyed successful international and European iterations in the forty-plus years that preceded it; yet it appears many organizations woke up to the principles of data minimization, purpose limitation or privacy by design on May 25th, 2018.

Since then, the regulatory landscape has changed somewhat and a high number of data protection cases were presented and ruled on in court. **The European Data Protection Board (EDPB)** has provided prolific guidance readable by experts and non-experts alike; while individual **Supervisory Authorities (SAs)** have been busy advising companies, members of the public and DPOs, investigating processing practices and ordering companies to comply, occasionally issuing fines to those who ignored the recommendations.

Many companies have taken the challenge very seriously, but others still believe they can fly under the supervisory radar. This is not particularly intentional; they likely think the Regulation does not apply to them. Often, new clients formulate needs based on misconceptions as to the scope of the Regulation or based on the misguided belief they do not process **PII**. While they might not process PII, they are still likely to process **personal data**, the very asset the framework regulates and it is arguably only a matter of time before they are called out by disgruntled employees or dissatisfied service users. The general public has become increasingly savvy about their rights and how to



exercise them, and many companies are not listening to the tell-tale signals from customer support, sales, and procurement teams and eventually find out the hard way.

Then in July 2020, a not-so-unexpected ground-shaking development, the so-called **Schrems II ruling** of the Court of Justice of the European Union (CJEU) invalidated the **EU-U.S. Privacy Shield** framework, relied upon by 5000+ US companies, many of which acting as suppliers of services to EU companies. This was a predictable repetition of the Schrems I case, which, five years prior, had invalidated the **Safe Harbour**. The ruling also placed much more stringent requirements on companies relying on the next available international transfer mechanism, **Standard Contractual Clauses (SCCs)**, making their use insufficient without an accompanying **Transfer Impact Assessment (TIA)**.

2. Increased Awareness

› Reactions from the B2C Sector

There has been an increase in awareness of the general public for privacy rights, sometimes backed by communication campaigns by large platforms like Apple and Google who, under impulse from court decisions, strategized privacy as a market differentiator, offered more transparency or user control -e.g. the reject-all-cookies button on Youtube- and imposed, in their marketplaces, more stringent conditions for app publishers or removed them altogether.

› Reactions of the B2B Sector

But for most companies, the impetus has come from a mix of ethical and commercial factors, chiefly pushback from B2B clients with increasingly demanding procurement checklists. Before Schrems II, it was common to talk to vendors who had little understanding of the Regulations and virtually no preparedness. The Schrems II decision was the necessary awakening for a lot of companies to get DPAs in place and address transfers. Nowadays, few processors in the US, for example, show resistance or lack of knowledge as to what is expected in EU client **contracts** by virtue of **statute**.

3. Predictable Changes

Much like the Schrems II case, **Brexit** also did not come from leftfield. It turned the UK into a **non-EU-country** and quickly got adequate country status from the EU Commission. The UK GDPR is similar to its mainland counterpart, and while the British supervisory authority indicates EDPB guidance on Transfer Impact Assessments is still valid, some companies have chosen to perform them

the UK way in anticipation of further deviation from EU data protection by the UK. The UK's **adequacy status** will be reviewed by June 2025, and by then, such anticipation may have proven worthwhile.

4. Increased Enforcement and Fines

There has been a significant increase in enforcement actions and fines across the EU. The biggest to date was handed to Meta on May 12th at € 1.2 billion for sending Facebook data back to the US, despite implementing new SCCs and additional supplementary measures found *not* to address the risks to the fundamental rights and freedoms of data subjects.

To name a few others, Google was fined €50 million for violating **transparency** and **lawfulness** obligations, and the Spanish bank BBVA, €5 million for similar violations, while TikTok was fined €5 million for making it harder to refuse **cookies** than accept them. Instagram was fined €405 million for privacy settings inadequate for **child use**. Amazon was fined €746 million for, though unconfirmed, targeted **advertising**; this is worth singling out as perhaps being the closest to a large class action, which the GDPR provides for.

5. Coordinated Task Forces

The EDPB responded to complaints filed by Schrems' [NOYB](#), and under its consistency mechanism, set up a cookie banner task force to assess dark patterns in cookie implementation and exchange views on legal analysis and possible infringements. Another NOYB



complaint, following the Schrems II case, found many transfers to be still based on the invalidated Privacy Shield. Anonymization of the IP address **only after** the data is sent out of the EU was unsurprisingly found insufficient and of accountability was found lacking in joint-controllership scenarios or when relying on data controllers that do not provide sufficient guarantees.

6. An Opulence of Tools to Choose From

› Press Releases from Supervisory Authorities and Case Law

Following the Schrems II decision, a flurry of press releases were published by authorities across the EU, warning about the implementation of vendors like Google Analytics, Google Fonts, and Mailchimp and advising on feature settings or the deprecation of such tools. As case law provides a constant feed of insights into applications of the law. A highly recommended newsletter subscription on the topic is that of NOYB itself, which provides the EU round view of lower-profile **rulings**.

› The Resourceful DPO

DPOs who are successful at establishing communication channels within their companies are faced with daily questions from their colleagues, vendors, and partners alike. To help them, many answers have made their way into the 30+ guidance documents provided by the EDPB. Arguably, the ones that have been most relied on include updated guidance on the concepts of controller and processor, updated recommendations on measures that supplement transfer tools, guidelines on the territorial scope of the GDPR, guidance on the interplay between that **scope and transfer requirements**.

› Support from the Fields of Cybersecurity and Compliance

The EU Agency for Cybersecurity (ENISA), known for its **cybersecurity certification schemes**, released its **Pseudonymisation Techniques and Best Practices** in 2019. Yet it should be noted that national initiatives are equally welcomed and constitute complementary material in the DPO's toolbox. One such contribution in Germany is the **Practical Guide to the Anonymisation of Personal Data** from the Stiftung Datenschutz, the data protection foundation, which helps consider the relationship between the practical side of the technique and German national legal requirements. Specific to the GDPR's Article 25 requirement to design data processes that are the least privacy-invasive, the ISO's consumer protection technical committee published the ISO 31700-1:2023 **Privacy by design for consumer goods and services**, establishing high-level requirements to protect privacy throughout the lifecycle of a consumer product.

Opportunities for the Privacy Profession

It may sound bold but it can be argued that regulators do not intend for companies to be 100% compliant, but rather expect them to act responsibly. There is no such thing as total compliance, and relevant certification frameworks have only just started to emerge, like ISO/IEC 27701 and more recently, Europrivacy. Much like implementing an ISMS, the focus should be on the **journey (the process improvement)** rather than the **destination (the certification)**. A sizeable difference, however, between complying with security standards, which are still largely normative, and conforming to the law is that in the former, the CISO serves **company interests**, while in the latter, the DPO serves **data subject interests**.



1. Fixing Compliance with the Data Protection Office

Many organizations have chosen to appoint a **Data Protection Officer (DPO)** in an attempt to "man the problem", and in so doing, have defaulted to being hands-off, assuming one person alone would bring the organization into compliance with little-to-no disruption to operational models.

A suitable analogy there would be the appointing of an ISO/IEC 27001 lead implementer, expecting them to get the organization certified within a year while failing to communicate top-down on security objectives and failing to assign responsibilities, promote **multidisciplinary contributions** or adequately **resource** the effort. Additionally, the misconception around the tasks and **the independence** of the DPO leads to invalid internal DPO appointments. **Conflicts of interest** happen when DPOs are expected to report to CFOs or CTOs or when the DPO also happens to be head of security, CISO or CEO. A DPO must be seen as an independent representative of the data protection authority, holding office within the organization and reporting to the highest form of management, i.e. CEO or board of directors.

2. The DPO of 2023

While the role of the DPO is still unclear for many organizations, DPOs themselves have had five years to better understand their challenges and sharpen their ability to establish and manage comprehensive privacy programs, while monitoring the fast-changing regulatory landscape and adjusting the compliance roadmap accordingly. For DPOs with little-to-no support nor robust project management skills and tools, the last five years will easily have triggered a burnout or two.

3. The DPO of Tomorrow

With the Cybersecurity Act, the DPO, already the best-placed contact person for all things data, compliance, and due diligence, is likely to play a stronger advisory role in data governance but also security-related fields like encryption, pseudonymization, the degree of anonymity, the review of access rights and the performing of control **audits**. This will lead to more **tailored training** opportunities for the wider organization that help it fathom the relationship between **information security** and **data protection** and leverage both as factors of competitiveness.

4. Raising the Awareness of Stakeholder Groups

Central to the DPO's advisory role is their ability to raise awareness. This is a starting point in any program and any discussion. Yet data protection training mostly focuses on operational staff, while top candidates for training remain **C-level executives**. As powerful proponents for the inclusion of privacy into company-wide OKRs, their understanding of what the DPO can and cannot do helps better resource, designate owners and sign off on efficient privacy programs. This in true conformance with clause 5.1 of ISO/IEC 27001 and its expectation for demonstrated leadership and commitment.

Sales teams receive procurement inquiries pertaining to privacy, such as questions about use, storage and international data transfers. As basic due diligence, **procurement teams** need to understand what questions to ask and how to spot a vendor full of marketing hot air. **Process and data owners** are responsible for updating records of processing activities, the cornerstone of GDPR compliance, from which obligations around transparency and lawfulness are established. Importantly, **design and product teams** are the champions of privacy by

design, a core principle of the Regulation. Finally, **staff** at large need to be aware of what sensitive data is and how to handle it. They need to recognize incidents or breaches and report them by means of well-established processes, because when a breach happens on a Friday night, the data controller only has 72h to report it to its registered authority.

5. Implementing Basic Principles

Training turns practitioners from maverick innovators (e.g. sharing, reusing, but also losing, corrupting, or misusing data) to responsible data handlers based on simple principles anyone can understand (such as **transparency, lawfulness, security, and accountability**). Yet most companies have trouble implementing data minimization or defining and implementing data **retention schedules**. This is true of marketing, where the more data, the merrier. Data minimization is also problematic with AI where models are trained on quantitative volumes to identify qualitative patterns. Machine learning triggers violations of transparency as data is not traceable collected with the transparency expected of data controllers. Put simply, model trainers are essentially non-compliant data controllers, unable to fulfill obligations they are unaware apply to them. Additional violations include those of **purpose specificity** and **purpose limitation**, where data is collected and consolidated, oftentimes prior to there being a specifically defined, communicated, or legitimized purpose for either of these two activities.

What to Expect in the Next Five Years

1. Cookie Cleanup

In 2023, cookies are only slightly less of a pain than they used to be. This has nothing to do with the Regulation and everything to do with companies exploiting dark patterns.

Some rely on third-party solutions for their banners or on Consent Management Platforms (CMPs). One such CMP, IAB Europe, which appealed its €250,000 fine from the Belgium supervisory authority, did not initially recognize its data controller role and let implementers of its consent transparency framework set **audience tracking** and **profiling cookies** by default, leading them to believe this practice was valid.

It is perhaps worth myth-busting here that no vendor solutions, be it a CMP, cookie banner solution or other intermediary- provides compliance to data protection law, as such. If solutions are not scrutinized, additional clarifications not requested, or limitations of liability are not challenged, chances are clients assume compliant risk from the outset, with a very **false sense** of having done what was needed.

› Legitimate Interest Cookies

The same can be said for the dark practice of not setting cookies by default (great) while relying on the **legitimate interest** as an alternative to user **consent** and making it hard for visitors to **object** to that interest (very bad). The intersection of the **ePrivacy Directive and the GDPR** dictates that consent is the only legal base that can be implemented for **non-essential cookies**. Be on the lookout for enforcement cases.

› The End of the Cookie Nightmare?

In the past, a lot of uncertainty resulted from national implementations of the ePrivacy Directive, and their interactions with national implementation of data protection acts. On the one hand, the **Directive** stipulates that read and write operations on user terminals require consent unless the cookies are absolutely necessary to deliver the content, whereas the GDPR provides modalities on what constitutes **valid consent**.

Note the so-called cookie Directive was last updated in 2009 when smartphones and online services were far less ubiquitous. The privacy community has great expectations for the e-Privacy **Regulation** due in 2024, to potentially provide clarity on communication metadata, and more enforceable rules on cookies and spamming.

Whilst on client browsers, the age of the cookie is far from over, it is recommended to monitor the emergence of a flurry of more user-friendly and privacy-preserving audience measurement and advertising techniques.

2. Further Regulation of Cybersecurity

› The NIS2 Directive

[NIS2](#) will become enforceable in October 2024. It lays down obligations for EU Member states to adopt strategies and establish competent authorities. It applies to public or private SMEs of a specific type that provide their services or carry out their activities within the Union. Much like the GDPR, it emphasizes **accountability** and **reporting** and the **immediate breach notification**. Companies should already be on the lookout for member state transpositions of the requirements into national law.

› The Cybersecurity Act

In the past, the adoption of national cybersecurity certifications has led to divergence and has prevented mutual recognition. The [CSA](#) aims to enhance cybersecurity protection in the EU by streamlining **certifications**. It also provides a **permanent mandate** the European Union Agency for Cybersecurity (ENISA). Companies that manufacture or provide ICT products, services, and processes will need to review their current cybersecurity practices, processes, and standards to ensure they comply with the new certification requirements. Whether they are candidates for compulsory certification should be clarified by member states by the end of the year.

› AI

The EDPB recently established a task force to promote consistent and effective enforcement of data protection laws with respect to artificial intelligence and natural language processing technologies, and to ensure the correct and consistent application of the GDPR by national DPAs. This follows from an injunction taken by the Italian DPA against OpenAI, while more authorities are expected to follow suit, such as the German Datenschutzkonferenz, the French CNIL, and the Privacy Commissioner of Canada.





The UK has launched a consultation on new AI regulations that would similarly require companies to comply with **transparency** and **accountability** requirements when using AI systems.

3. Six More EU Data Regulations to Look Out For

› Digital Markets Act (DMA) and Digital Services Act (DSA)

In late 2022, the DMA and DSA came into force. It aims to create a safer digital space protecting the fundamental rights of users and aims to establish a level playing field for businesses, ultimately fostering innovation, growth, and competitiveness in the single market and globally. In April, the EU Commission adopted the first decisions, designating 17 **very large online platforms** that reach at least 45 million monthly active users (Alibaba, AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando) and two **very large online search engines**, Google and Bing. Because these gatekeepers centralize vast quantities of user information, the DMA and DSA exacerbate GDPR requirements for transparency and accountability while promoting **user empowerment**, stronger **protection of minors**, more diligent content moderation and **less disinformation**. The UK government is also developing its [Online Safety Bill](#) to address online harms, including the spread of **misinformation**, **hate speech**, and other **harmful content**. The proposed legislation will require online platforms to take more responsibility for the content posted on their sites and to protect users from harm.

› The Data Act

The [Data Act](#) being discussed at the EU Parliament will harmonize rules on **fair access** to and use of data for businesses to easily switch their data and other digital assets between competing providers of cloud and other data processing services. The creation of a common European **interoperability framework**, data spaces for strategic sectors of the economy, and domains of public interest should encourage a market for data enabling sharing and use across sectors. Non-personal data should also be shared, i.e. monetized.

› The Artificial Intelligence Act (AI Act)

Similar to the scope of the GDPR, the act will apply to providers and implementers of AI systems located within the EU as well as those located in a third country, where the output produced by the system is used in the EU. It aims at guaranteeing safety and the respect of existing law

by considering the **fairness, security, and robustness** of AI algorithms by heightening **transparency requirements**. Like the GDPR, the Artificial Intelligence Act takes a **risk-based approach** but is more practical and places AI systems into four risk categories from low to unacceptable with, for example, requirements for high-risk systems to include: a risk management system, data governance, technical documentation, transparency, human oversight, accuracy, robustness, and cybersecurity. Worth noting is that maximum fines will be 50% higher than those of the GDPR. The law will also prohibit AI-based **social scoring** done by public authorities, the likes of what the Chinese government allows. Current debate indicates the intention to extend this ban to private actors as well.

› The AI Convention

The AI Convention of the Council of Europe is being drafted to serve as a convention on artificial intelligence, human rights, democracy, and the rule of law. The AI Convention will be the first **legally binding international instrument** on AI and will be open to non-EU states.

› European Data Governance Act (DGA)

The [DGA](#) will apply from 24 September 2023. It provides a cross-sectorial framework to make the planned data market a reality. More data should become available by regulating the re-use of publicly held, protected data, and promoting **data sharing** by regulating new **data brokers** that act as marketplaces while also encouraging the sharing of data for altruistic purposes. The DGA establishes a European Data Innovation Board, extends to data intermediation service providers and most importantly, applies to both **personal** and **non-personal** data. As data is intended to flow freely, innovation will flourish as market entry costs are lowered for smaller companies.

4. Looking Ahead

› EU-US Data Transfer Framework, Schrems III in Waiting?

A hot topic that organizations should monitor closely is that of a much-needed future-proof adequacy decision. The Safe Harbour and Privacy Shield were invalidated in 2015 and 2020, respectively by the EU Court of Justice in the so-called Schrems I and II cases. The privacy community is on standby as litigation is already expected to ensue if an adequacy decision comes through. For instance, it is widely recognized that no agreement can effectively limit US intelligence agency from accessing EU-citizen data stored in, or accessible from, the US and simultaneously provide data subjects with adequate redress mechanisms.

› Enforcement Actions are Expected on DPO Appointments

The EDPB has just launched a coordinated enforcement action on DPOs to better assess their designation, knowledge, and experience. But this is perhaps not so much about the DPOs as it is about the organizations employing them.

Expect enforcement to focus on the possible conflict of interest of the internally appointed DPO, whether they **are able to report** directly to the highest management, how well they are **resourced**, or made to remain **independent** and effectively perform their tasks. As a CEO, ensure you sit down with your DPO and align your respective understanding of GDPR articles 37 to 39.



Alex Carroll

Consulting Manager at
TechGDPR DPC GmbH

Alex Carroll is consulting manager at TechGDPR DPC GmbH, a small privacy consultancy that offers project-based and hourly consulting in data protection, training, DPO as-a-service,

EU representation and ISO27001 implementation support. He leads a small team of highly motivated and experienced privacy and tech consultants, manages key accounts, and develops upskilling strategies for his team to stay atop a fast-evolving field. He was part of the drafting committee that led to the 2020 publication of the DIN Spec 4997 Privacy by Blockchain Design.

More recently, he was invited to speak and moderate at the 2022 PECB Insights conference in Brussels on the topics of cookies and blockchain security. He and his team are about to release regular videos on TechGDPR's youtube channel related to privacy compliance management from a distinctly European perspective. He has developed the self-paced GDPR-for-product-owners-and-software-developers training course and a standard GDPR compliance audit methodology and will soon offer an internationally recognised 3rd-party-certified training on EU data protection.

His background in adult education and elearning design led him to dive into quality management frameworks. It was while determining how the GDPR informed the context-of-the-organisation clause under ISO 9001 that he was led down the rabbit hole of data protection, struck by the parallels between normative and statutory compliance and comparable stakeholder management strategies.

ENRICH YOUR EXPERTISE IN YOUR CHOSEN FIELD

Develop further with PECB's new and updated training courses!
Contact us at marketing@pecb.com or visit our [website](#) for more.

New and updated training courses:

Training Course	Language	Status	
ISO/IEC 27005 Risk Manager	English	Updated	→
ISO/IEC 27002 Introduction	English	Updated	→
ISO/IEC 27001 Introduction	English	Updated	→
ISO/IEC 27005 Foundation	English	Updated	→
ISO 45001 Foundation	English	Updated	→
ISO 28000 Lead Auditor	English	Updated	→
ISO 28000 Lead Implementer	English	Updated	→
ISO 28000 Transition	English	New!	→
ISO/IEC 27001:2022 Transition	Spanish	New!	→
ISO 21502 Lead Project Manager	French	New!	→

WEBINAR **LIVE**

BE ON THE LOOKOUT FOR JUNE'S WEBINAR

Data privacy and security have become critical concerns in our increasingly digital world. The GDPR, introduced in 2018, sets out strict guidelines for the protection of personal data of individuals within the European Union (EU) and the European Economic Area (EEA). Non-compliance with GDPR can result in hefty fines and damage to an organization's reputation.

To mitigate these risks and establish effective data protection practices, many organizations are turning to ISO/IEC 27701:2019, an extension to the ISO/IEC 27001 standard. Learn more through this webinar.

TOPIC: GDPR and Data Protection: Ensure Compliance and Minimize the Risk of Penalties with ISO/IEC 27701

June 27, 2023, at 3:00 PM CEST



LISA GOLDSMITH
GDPR Expert, Strategist,
Consultant, Trainer, and Speaker








MIKE BOUTWELL
Founding Partner -
Infosec Program Partners



REGISTER HERE

SPECIAL T

TITANIUM

PLATINUM

GOLD PA

Note that PECB Partners are listed as per the credits

HANKS TO

PARTNERS



PARTNERS



PARTNERS



acquired from January 1, 2022 to December 31, 2022.

**ESTABLISH
THE NECESSARY
PRIVACY MEASURES
WITH GDPR**

