

DIGITAL TRANSFORMATION

ITS IMPORTANCE AND IMPACT
ON ORGANIZATIONS



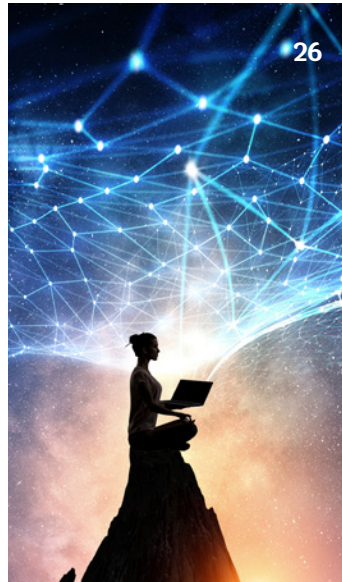
PECB Insights Magazine

delivered to your mailbox



Subscribe & find out more at
www.insights.pecb.com

In This Issue



6 The Standard

Counter-Attacks on Cybersecurity

10 The Expert

Data Ethics in Organizations: Protecting Personal Privacy

16 Technology

AI and Metaverse: Emerging Trends in Cybersecurity

20 Success Story

Bechir Sebai Success Story

26 Innovation

IoT and Edge Computing

32 Work-Life Balance

The Life of an AI Expert

40 Leadership

Business Intelligence, Big Data, and Data Mining

44 Leadership

Integrating IoT and Blockchain to Your Cyber Safety

48 Opinion

Data Privacy in the Age of Digital Transformation

56 Business & Leisure

Exploring the Beauties of Québec, Canada

62 The Expert

The Principles of Building Cloud Security Solutions

68 Books

Digital Transformation Essential Reads

76 Career

Top Five High-Paying Job Positions You Can Pursue with a Cloud Security Certification

78 The Expert

The Influence of Blockchain on Digital Transformation

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

© PECB 2022. All rights reserved.



**// There is no alternative
to digital transformation.
Visionary companies will
carve out new strategic
options for themselves —
those that don't adapt,
will fail. //**

JEFF BEZOS

Executive Chair - Amazon





Counter-Attacks on Cybersecurity

Cyber-attacks are costly, disruptive, and a growing threat to business, governments, and society alike. Happily, an arsenal of standards helps stay ahead of the game.

Cybercrime is on the rise. And as we move deeper into the digital age, the era of the so-called Fourth Industrial Revolution, it is also growing ever more sophisticated and severe, with serious consequences. As cyber criminals become more adroit, cybercrime has touched all our lives in one way or another.

Cyber-attacks can range from hacking into systems and social media, phishing attacks, malicious software including ransomware, identity theft, social engineering, and denial-of-service attacks. This is painful both personally and financially, causing untold damage and destruction, as well as leaving society and citizens vulnerable. According to [McAfee](#), the computer security software company, the cost of these cyber-attacks is on the increase, amounting to around US \$1 trillion in 2020.

A Growing Global Risk

With the COVID-19 pandemic having further embedded our growing dependence on digital systems, it is not surprising that the [Global Risks Report 2022](#) has yet again included the threat to cybersecurity as one of the growing risks facing the world. Cybersecurity failures, it says, have worsened significantly and threaten long-term prosperity.

But how do we stay one step ahead? Building a good cyber-defense system as well as anticipating threats are key elements in the fight against cybercrime, but neither resilience nor governance is possible without credible and sophisticated cyber-risk management plans. “Cybercrime is both a national and international occurrence that is spreading with great speed, affecting businesses, governments, and society as a whole. The scale and complexity of this criminal activity has far-reaching and detrimental consequences and the situation is blurred as cybercriminals operate, using technical infrastructure, across national boundaries,” says cybersecurity expert Dr. Edward Humphreys.

“Cybersecurity failures have worsened significantly.”

As a result, he adds, international collaboration is essential and International Standards are indispensable for global protection. Dr. Humphreys speaks from his many years of business experience. He is also a senior research fellow specializing in cyber-risk, security, and cyber-psychology research and ISMS innovation studies, and the ISO/IEC Convenor of the working group responsible for the management, development, and maintenance of ISO/IEC 27000, a family of standards on information security management systems (ISMS).

Solutions and Controls

International Standards provide solutions, he says, enabling organizations to establish frameworks and systems to assess and manage the situation – to protect information, to secure applications and services, and national infrastructure.

The first step in tackling cybercrime is knowing the risks you face and then deciding the controls that need to be implemented to mitigate these risks. Humphreys points to standards such as the ISO/IEC 27000 family, developed by ISO and the International Electrotechnical Commission (IEC), as the de facto choice for any organization wishing to build robust solutions against cybercrime.

The suite of International Standards specifies a management system that goes into the risk management process of assessing the risks and then determining the controls needed to treat them.

“The first step in tackling cybercrime is knowing the risks you face.”

“There are a range of standards supporting ISO/IEC 27001, such as ISO/IEC 27005 on information security risk management and the ISO/IEC 27003 implementation guidelines,” he says. “And there are many other standards that provide technical support for ISO/IEC 27001, for example to secure networks and embed security features into technology, services and applications.”

Being Prepared

Dr. Humphreys reiterates the need for companies to be prepared and ready to face these attacks. “Cyber-attacks can take place anytime and anywhere, and what is certain is that these attacks are sure to happen but we can never be sure when or where,” he says. “Being ready and prepared is an essential business activity for survival.

It involves a business having in place a process to be able to anticipate and identify, detect and report incidents, and to analyze these incidents to decide how to respond to them.”

This all needs to be done in a quick and timely manner to limit the impact the incident could cause.

“Cyber-attacks can take place anytime and anywhere.”



So how can businesses be better prepared? Once a business detects the presence of a malicious code attack or a denial-of-service attack, the faster it responds with appropriate security measures, the greater the chance of limiting the spread of these attacks as well as limiting the impact and damage. And, as Dr. Humphreys says, there are standards that help businesses to become ready and better prepared to respond, such as the incident management standard ISO/IEC 27035, the standard for business continuity management ISO 22301 and the ICT readiness standard ISO/IEC 27031.



Collective Action

In an already uncertain world, cybercrime can be financially devastating, disruptive to business operations and national infrastructure, as well as affecting citizens and society. For example, an attack on one part of a supply chain may spread and disrupt and damage other parts of the chain. In order to foster more secure and resilient cybersecurity systems, Dr. Humphreys says the management of a supply chain is a good example of where collective action is needed across all parts of the chain to keep it secure.

“Again,” he says, “there are standards that help with supply chain security, such as ISO 28000 and ISO/IEC 27036. Collective action is also needed in various scenarios that involve business relationships and communications with other organizations. There is a group of management standards that will help with building resilience to counter business disruption and ensure survivability and system of governance. These include ISO 22301 (business continuity management systems) and ISO/IEC 27001 (information security management systems) and ISO/IEC 27014 (information security governance).”

With the growth and dependency on connectivity for business, the infrastructure that supports it, and the use of the Internet and mobile devices, there is an even greater need for system security and resilience. Dr. Humphreys acknowledges that standards need to evolve to match the rapid advances in technology. “The third edition of ISO/IEC 27002, for instance, was published in the first quarter of 2022. This high-profile standard deals with information security controls and has been updated to match the advancement in technology, business developments and practices, and new laws and regulations.”

In 2021, he adds, there were many other developments in standardization, including Internet of Things (IoT) security and privacy, big data security and privacy, artificial intelligence security and privacy, and biometric information protection. All these are complemented by recent technical specifications such as ISO/IEC TS 27570, which provides guidance on smart city ecosystem privacy protection, and ISO/IEC TS 27100, which specifies how to create or refine robust cyber systems to protect against cyber-attacks. The complete ISO/IEC 27000 family of standards and these technology-focused specifications are the foundation for building and managing a secure future.

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



Data Ethics in Organizations: Protecting Personal Privacy



BY AHMED QADIR

THE EXPERT

The Pakistan experience says the need for personal data protection legislation is now. Our lives have become more digital. Since COVID-19, the physical has been replaced by the digital. Work-from-home, online schooling, e-Commerce, food and grocery delivery, etc., has left a bigger digital footprint in the form of our personal data. We only have some idea of how much data is collected but generally close to none about how it is managed or used. This is the catch-22 situation. We need these platforms because they are global brands and for the services they give us, but on the other hand, there is a cost to us in terms of our privacy and important data.

In May 2017, [The Economist](#) said that data is a more valuable resource than oil. The shift from price to data is accelerating. Data analytic techniques have become the oil extraction-and-refining plants and data companies have become the new oil giants. Data is the next “essential” facility and money maker, and this is prompting debate on how it should be regulated. Today, big data is a big driver of growth and for some companies, revenue. With a significant shift towards a more digital lifestyle, privacy implications have grown, along with concerns with the ethical discussion of how one’s personal data is used. With concerns that [Google collects 7,000](#) points of information about people, the valid question today is “has Google’s data collection gone too far?”

Much of our everyday activity takes place in the online domain courtesy of the numerous apps running on smartphones accessing the Internet on 4G technology using platforms, such as Google, Facebook, and Amazon. There are also many regional and national platforms in play. Many people are shopping online because of the convenience it offers, even more important as COVID-19 lockdowns were imposed. Online retailers tend to remember your purchase history and base their recommendations on your subsequent purchases on this history. As another, using services such as ride sharing or food delivery also provide convenient and affordable options to people.



All this is done through algorithms that analyse one's digital footprint extensively – every click, every like, every second spent on a website, keywords in communication, demographic data, geographical location, age, gender, political orientation, etc., and mine a wealth of usable information from it. Facebook even considers their “algorithms can enhance our personal relationships.” How can this data be safeguarded? One key challenge is the fact that digital technology spans the globe and many data collectors are not located within national boundaries.

Our digital identities are accessible globally, often without our knowledge or permission.

Privacy from an Ethical Perspective

Data ethics must also realize that privacy is a fundamental human right that underpins freedom of association, thought and expression, and freedom from discrimination. It is not easy to define privacy. Different countries hold different views, as do individuals. Privacy varies from person to person and differs depending on the situation. Broadly speaking, privacy is the right to be let alone, or freedom from interference or intrusion.

It is important, thus, to enact effective legal instruments that define the individual's right to privacy and the threats to it, in the digital age. Data protection helps us in safeguarding our fundamental right to privacy with appropriate legal frameworks that give individuals rights over their data and put in place accountability systems and define the obligations of those who control and process this data. But equally important is to imbue a sense of data ethics in organizations. As acquirers and custodians of data mostly without any deliberate effort, there is a reasonable expectation that organizations will protect our data and help keep us safe online. Without this expectation, online transactions and social media activity could suffer.

There is growing worry over social media companies' non-social and non-economic influence over culture and information, and the implicit threat they pose to the jurisdictions of governments. For instance, Facebook and [270,000 users' data](#) – those who participated in a survey by [Cambridge Analytica](#) and had consented to having their data harvested – led to a breach of the personal information of 87 million users and could possibly have affected the 2016 U.S. elections. Similar concerns have been raised during the U.K.'s process of Brexit.

Tech firms have been voraciously collecting the data of their consumers, offering free services as an enticement. The major platforms – the “[frightful five](#)” or FAANGs – have played a key role in the process. Shoshana Zuboff, in her book, [The Age of Surveillance Capitalism](#), details how Google and Facebook developed their business models to collect and monetize data – “A fundamentally illegitimate choice,” she says.

A 2015 survey by the Annenberg School of Communication, University of Pennsylvania, found that “a majority of Americans are resigned to giving up their data—and that is why many appear to be engaging in trade-offs.



Resignation occurs when a person believes an undesirable outcome is inevitable and feels powerless to stop it. Rather than feeling able to make choices, Americans believe it is futile to manage what companies can learn about them. The study reveals that more than half do not want to lose control over their information but also believe this loss of control has already happened.”

These findings were also reflected in a [Pew Centre](#) research in 2014 that found that “91% of Americans “agree” or “strongly agree” that people have lost control over how personal information is collected and used by all kinds of entities. 80% of social media users said they were concerned about advertisers and businesses accessing the data they share on social media platforms, and 64% said the government should do more to regulate advertisers.” [Another Pew survey](#) in 2017 found that “just 9% of social media users were “very confident” that social media companies would protect their data. About half of users were not at all or not too confident their data was in safe hands.”

Can we expect tech companies to protect our personal information? Not if their business model or a revenue stream depends on collecting and sharing it. Protecting privacy requires a legal framework but will also require a technology adaptation.

The Legal Framework for Privacy Protection

Privacy is a qualified, fundamental human right. The right to privacy is articulated in all major international and regional human rights instruments. Article 12 of the [Universal Declaration of Human Rights](#) proclaims that “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interferences or attacks.”

Article 14 (1) of Pakistan’s Constitution gives individuals the right to privacy: “The dignity of man and, subject to law, the privacy of home, shall be inviolable.” With social media and growing digitalization, the concept of privacy today must also encompass online activities and our growing digital footprints. In 2013, the United Nations General Assembly affirmed that the rights of people offline must also be protected online, calling upon all states to respect and protect the right to privacy in digital communication.

Data protection is a trending topic and many governments have moved decisively to plug the gaps in their national laws. [The British Government](#) introduced a new draft data protection bill in 2017 to replace the 1998 law.

Key features include the “right to be forgotten” on the internet and “the right to innocence” whereby citizens can request social media sites to remove any content they posted before the age of 18. The bill proposes tougher penalties on companies for data breaches and a requirement by businesses to inform the U.K. Information Commissioner’s office about any breach within 72 hours.

The EU’s General Data Protection Regulation ([GDPR](#)) is the most important change in data privacy regulation in 20 years and considered the world’s most aggressive set of internet privacy rules. GDPR is a common set of rules and practices that apply across Europe, and it is hoped, the world. It grants regulators to fine any company in breach as much as four percent of its total worldwide sales. It promotes three legal and business principles for firms that want to gain or retain user trust: transparency (say what you do), user control (empower your customers), and accountability (do what you say).


GDPR states that first, companies need a person’s consent to collect their data, and second, a person should be required to share only data that is necessary to make their services work. More than 500 million people living in the European Union have two important rights, i.e., the right of erasure and the right of portability.

After GDPR, California passed a digital privacy law – the California Consumer Privacy Act ([CCPA](#)) – that gives consumers more control and insight into the spread of their personal information online.


This is one of the most significant regulations that governs the data-collection practices of technology companies in America. “The new law grants consumers the right to know what information companies are collecting about them, why they are collecting that data, and with whom they are sharing it. It gives consumers the right to tell companies to delete their information, as well as to not sell or share their data. Businesses must still give consumers who opt out the same quality of service.” This is quite a step as most of the existing laws do little to limit what companies can do with consumer information.


The Government of Pakistan has proposed various draft personal data protection legislation since 2018. In this regard, the preparation of a draft Data Protection Bill (PDB) by the government is commendable.

The need for personal data protection has become more urgent since then as e-Commerce, financial, and service activities have increased because of COVID-19 and the general trend of increasing digitalization everywhere.



A man in a light blue shirt is looking at a smartphone. Overlaid on the image is a digital login form with a blue border. The form includes a user icon, a 'Username' field, a password field with a lock icon, a 'Remember Me' checkbox, a 'Forgot Password?' link, a 'LOGIN' button, and a 'REGISTER' button. A face-scanning box is also overlaid on the man's face, and a padlock icon is on the phone screen.





☐ Remember Me [Forgot Password?](#)





There have been serious incidents of data breaches in local organizations in recent years.

In April 2018, [Careem](#), a ride-sharing service in Pakistan (acquired by Uber in January 2020), admitted that “users’ personal data was compromised in a massive data breach.” [Another article](#) said that “The hack affected user data of over 14 million users and 558,880 Captains in the 13 countries and 90 cities that Careem operates in.”

In September 2020, the Karachi Electric Supply Company ([K-Electric](#)) was targeted by a ransomware attack. The ransomware operators demanded payment of US \$3.85 million worth of Bitcoin, rising to US \$7.7 million after a week. K-Electric did not pay and all user data was leaked to the dark web. The legal recourse for those affected: none.

In August, the Federal Board of Revenue ([FBR](#)), the custodian of all taxpayers’ information, was affected by a cybersecurity breach. The agency claims that all personal data was safe but the veracity of this remains doubtful. Ten days after the event, the recovery process was continuing.

A [leading bank in Pakistan](#) suspended international debit card transactions after discovering valuable customer data had been compromised. “Most of the debit cards running to MasterCard networks were subject to fraudulent transactions.”

It is common knowledge that data from government repositories has been accessed without permission and

can be purchased economically. Telecom companies in Pakistan have been known to sell subscribers’ data to third parties, something that is even stated in the privacy policies of some companies. Hence, the talk of a national data regulator is timely.

Unfortunately, Pakistan’s Electronic Data Protection Act, 2005, and the Personal Data Protection Bill, 2018, remain draft pieces of legislation. Concerns about the latter legislation have been highlighted by Privacy International, i.e., exempting state-owned entities from its purview. Pakistan’s lack of data protection laws may make it difficult for international market platforms and other e-Commerce companies to operate locally and to protect its citizens from data breaches. This is an entry barrier as companies may hesitate to operate in a weak regulatory regime. And in general, the feeling of insecurity about one’s personal data can also stifle competition and innovation.

Pakistanis based in Europe will see their online transactions and activity protected under GDPR. These include banking services, e-commerce transactions, and activity on social media. It cannot be one-sided protection and companies in Pakistan will need to adapt to service clients and customers in Europe, and the world. The EU plans to limit market access to the region if countries do not rise to meet Europe’s standards. Data protection laws are becoming part of trade deals. It is time that Pakistan moved decisively to promulgate data protection legislation not just for economic reasons but for personal security and privacy!

Conclusion

It will be a while before regulations in Pakistan for protecting data become effective, leading to the ethical question in the meantime: should data be protected or should less of it be collected? Both protection and collection have their attendant costs and risks. Even the American National Security Agency could not prevent an employee from walking off with a thumb drive full of information and releasing it to the world in 2013.

Can data ethical behavior be encouraged by having the necessary legal frameworks in place? Or can data-dependent companies adopt principles and practices that demonstrate careful stewardship of the information they collect about people? Pakistan provides no legal recourse to anyone who suffers from a loss of personal data, at least, for the time being. It is time to change this by having a GDPR-like legal framework. But equally important is encouraging a sense of ethics. Without fear of legal sanctions, it is difficult to change behavior, and until the National Data Protection Authority is established, there is no other focal agency to advocate for data ethics and personal privacy. Given the global implications of GDPR, Pakistan's draft data protection regulations should be carefully compared and harmonized with those in the GDPR and the CCPA. Data protection, privacy, and ethical guidelines require a global and unified response.



Ahmed Qadir

Public Sector Innovation and Strategy, Open Government, Open Data and Technology, Regulation, Compliance, and Advocacy

Ahmed Qadir began his career in Pakistan in 1996 in the development sector with the United Nations, initially with the *United Nations Population Fund* (UNFPA) for the national program on primary health, and subsequently, with the *United Nations Development Programme* (UNDP) for information and communication technology and electoral reforms. He also worked, albeit briefly, for the World Bank and the Asian Development Bank in Pakistan, before shifting to the public sector in 2005, where he currently is.

His key interests include understanding the nexus between data, privacy, and consumer protection; using data analytics for strategy, strategic management in the public sector, new institutional economics, and organizational transformation. And more importantly, how the threads of his past and current experience mesh together.

AI and Metaverse: Emerging Trends in Cybersecurity

 BY AILSA WILLIAMSON

Imagine being able to rehearse surgical procedures ahead of time or interact with a simulated manufacturing plant in 3D. Imagine being able to walk through a virtual art gallery or attend a concert by your favourite artist from the comfort of your home. These are just some of the potential metaverse applications that we could see in our near future.

The metaverse is positioned to become the next big milestone in the evolution of the internet. In a nutshell, it is a 3D online experience that you can walk through via connected headsets and glasses. The virtual metaverse will be built on the same technology stack that is used to build Web 3.0, including blockchain, cryptocurrencies, and non-fungible tokens. Understanding the metaverse may seem complicated, especially as the technology is still in its infancy, but this has not prevented it from attracting considerable public attention. [Bloomberg](#) analysts have estimated that the total market value of the metaverse could reach US \$800 billion by 2024.

It is unclear whether there will be one metaverse or many, but it will be an immersive next-generation version of the internet, likely rendered by virtual or augmented reality technology. The metaverse has been described as a successor state to the mobile internet, and a platform for leisure, labour, and existence at large. One thing that is clear in this journey to the future is that AI and data science will play a critical role in its success.

How Can AI Enhance the Metaverse?

Whilst it is exciting to see such interest in the potential of the metaverse, organisations taking their first virtual steps into the world must also consider how they can guarantee safety and privacy for their users.

The power of many technologies, including artificial intelligence, will play a key role in safeguarding this deeply immersive new world.



The use of deep learning-based software and natural language processing will aid in driving interactions, whilst artificial intelligence will be implemented to translate images, video, and text. Artificial intelligence will also play a huge part in automating virtual transactions to allow the metaverse to run smoothly for both business and leisure use. The challenge lies in living up to the promises of these immersive virtual spaces whilst keeping critical data safe.

As with any new technology, when deployed to large audiences it will likely face numerous attempted cyber-attacks which may dissuade users from utilizing the platform.



The proliferation of data generated by the metaverse amplifies these risks. Protecting virtual identities and intellectual property rights, therefore, must be prioritized in addition to robust cybersecurity measures for digital and physical attack surfaces.

Data Breaches

As the metaverse expands and more data and devices appear online, the risk of data breaches only grows. Augmented reality devices will hold large amounts of user data, including biometrics, which are a valuable target for cyber-attacks. Strict laws must be developed to protect user data to avoid the information being exploited in the space.

The metaverse universe creates a large attack surface for cyber hackers. Combining traditional hacking methods with artificial intelligence and machine learning could very easily disrupt metaverse interactions if organizations do not employ their own sophisticated cybersecurity protocols.

One major drawback of new technologies is that they do not come equipped with cybersecurity solutions. With the metaverse, in particular, the precise cyber threats are still relatively unknown, and it may take years to identify all of the risks. Metaverse platforms have a duty to protect their user data, but participants should also be extremely careful about the information they are sharing. The task of protecting such a large amount of data should be shared amongst key players building the metaverse, including companies, government bodies, and users, to introduce a system of regulation and governance on data flow.

Privacy and Security Concerns

Identity theft, fraud, and impersonation are clear potential security risks in the metaverse. Cybercriminals will be drawn to the metaverse due to the volume of e-commerce transactions set to occur in the space. Whilst the metaverse is still in the development stage, it has already experienced various types of fraud. It is estimated that over US \$14 billion in cryptocurrency assets were lost to fraudsters in 2021. NFTs will be at the heart of this metaverse economy and phishing schemes will continue to pose a threat leaving sensitive information exposed, and enabling access to cryptocurrency wallets and blockchain scams.

Both defenders and attackers will use artificial intelligence to fight against each other in a world where the best algorithm will win. These algorithms powering the metaverse are constantly learning, which creates a new layer of complexity that will need to be monitored and protected.



We will likely see computer security algorithms being created and developed to take on potential privacy and security threats. Artificial Intelligence and machine learning can be leveraged to continuously monitor user behaviour and find abnormal behaviour patterns. However, this technology will still require some level of human intervention.

Authenticity, Identity Verification, and Protection

Authentication and verification should be at the core of all activity occurring within the metaverse. Theft of user credentials and avatars is likely to be high on the list of attempted cybercrimes in this virtual world. Metaverse users can opt to use their real name or an avatar in the virtual world, but in both scenarios, cyber criminals can attempt to gain access to their credentials and impersonate them. This can be especially dangerous when business interactions, social interactions, or financial transactions are being made, or if sensitive data is at risk of being exposed and held at ransom.

Authentication of user information, location, and third-party data also play a key role in a business's data reliability and accuracy. Vulnerable networks can, not only result in users losing virtual assets, but also risks the loss of reputation for businesses. Therefore, secure authentication tools will be especially important to validate data in the metaverse. Businesses operating in the metaverse should operate strict control over company-wide policies, operations, and implement advanced multi-factor authentication and dynamic data masking to protect against such threats.

Dynamic data masking allows data to be hidden and replaced with other data directory decoys to protect users in the metaverse from cyber-attackers. Whilst multi-factor authentication allows companies to simultaneously check multiple parameters when users attempt to gain access to the metaverse infrastructure. One-time codes, location-based data, and biometric data integrated into the augmented and virtual reality hardware are an example of components that will aid in validating multi-factor authentication logins.



Preparing the workforce in advance to combat cyber-attacks will also help guarantee their security systems are secure, safe, and free of vulnerabilities.

Businesses should clarify the responsibilities of both the organization and its employees, including information on conducting communication in the metaverse and what data will and will not be collected.

Final Thoughts

As the rate of innovation continues to outpace regulation, collaborating with those who have the expertise and tools on cyber threats and artificial intelligence will ease the journey towards creating a metaverse that facilitates immersive global interactions from the comfort of your home.

The metaverse is multidisciplinary and will impact a vast range of industries. Such technologies will carry certain risks but with a cautious and informed approach, players in the metaverse can create incredible, immersive experiences that may shape the future of work and play.

Opportunities and threats are evolving quickly and though many of these are still unknown, businesses must be adaptable and dynamic in their cybersecurity strategies.

Secure lines of defence with added artificial intelligence tools and cross-industry information sharing will be vital in this space to create a safe, secure, and inclusive platform for everyone.

Educating Employees

Emerging technologies come with a huge learning curve and organizations must prepare to make sense of this new virtual world. To ensure that employees are equipped with the ability to identify and act on potential security threats, organizations building and conducting interactions in the metaverse must train their staff as the first line of defense. This includes upskilling the current workforce and consulting with cybersecurity and AI experts on best practises.

Whilst the metaverse is a cutting-edge new technology, it relies on user trust to enable growth, expansion, and ultimately success. Implementing an educational approach to cybersecurity within the organization at the very beginning of the metaverse journey, including training on the artificial intelligence tools that provide extra layers of security, will assist in ensuring safety and the prevention of data exposure and leaks.



Ailsa Williamson

Senior Conference Producer, AI Specialist, Deep Learning, Metaverse, AI Ethics, and Responsible AI

Ailsa is an experienced media professional in content production, marketing, and events with upwards of 50,000 attendees. Ailsa currently holds the role of Senior Conference Producer at Informa where she is driving the launch of a Global Artificial Intelligence event in the Middle East.

As an Artificial Intelligence, Robotics, and Metaverse specialist, Ailsa's expertise in developing and executing event programmes facilitates knowledge sharing, collaboration, and innovation throughout the global technology ecosystem. Ailsa believes that technology's larger impact will be in complementing and augmenting human capabilities, not replacing them.

Bechir Sebai

Success Story

With twenty years of experience in the field of Information Systems Security and Cybersecurity in France and abroad, mainly for major banking and telecommunications accounts, Bechir Sebai has acquired certain expertise that are recognized by his peers.

Taking advantage of his know-how and experience in the field, Bechir has led several structuring projects:

Information Security Management System (ISMS) – ISO/IEC 27001, Privacy Information Management System (PIMS) – ISO/IEC 27701, and Business Continuity Management System (BCMS) – ISO 22301, IT Risk Management, Information Security Audit and Assessment, IT Master Plan Development, Business and Service Continuity, Information Security, Cybersecurity program implementation, and IT technical audit in various sectors.

Certified trainer by PECB and teacher at the Ecole Supérieure de Génie Informatique ESGI, holder of CISA, ISO/IEC 27701 Lead Implementer and Lead Auditor, ISO/IEC 27001 Master, ISO/IEC 27001 Senior Lead Auditor and Lead Implementer, ISO/IEC 27005 Senior Lead Risk Manager, ISO 31000 Senior Risk Manager, ISO 22301 Senior Lead Implementer, ISO/IEC 27032 Lead Cybersecurity Manager, Data Protection Officer (GDPR), ISO 30301 Lead Auditor, ISO 21500 Lead Project Manager, Ebios Risk Manager, ISO/IEC 20000 Lead Implementer, and ISO/IEC 38500 Lead IT Corporate Governance Manager.

He has also been awarded three times in a row (2019, 2020, and 2021) the title of "PECB French Trainer of the Year", for his teaching with feedback and experiences, as his pedagogy was appreciated by the trainees for its various illustrations of concrete, real examples reflecting the reality on the ground.

With his experience and know-how, Bechir started his own business by founding ACG Cybersecurity.

CEO and manager, he leads a multidisciplinary team of over thirty consultants.





Placing the human being at the center of its concerns, the ACG Cybersecurity entity does not cease evolving through a permanent contribution of senior consultants and experts in the field of Cybersecurity, who wish to continuously join the firm in view of the good reputation and the favorable climate which reigns there, to conceive, implement, operate and secure Information Systems according to international norms and standards ISO 2700x, ISO 20000, NIST, ISO 22301, PCI DSS, HDS, ITIL, COBIT, etc.

He can now take pride in having made **ACG Cybersecurity** recognized in a very demanding market in:

- Obtaining the ISMS certification of ISO/IEC 27001 for its business activities,
- Associate member and resident of the Cyber Campus, the totem of cybersecurity in France,
- Obtaining the "ExpertCyber" label from Cybermalveillance.gouv.fr, intended to recognize security professionals who have demonstrated a level of technical expertise in the areas of assistance and support,
- Obtaining the "France Cybersecurity" label for the promotion and awareness of its solutions,
- Signing a privileged partnership with PECB and its University.
- Qualiopi certification for its ACG Academy training center,
- Becoming a SWIFT partner for the implementation and evaluation of its solutions,
- Becoming a training partner with Microsoft, especially on Cloud solutions,
- Being a member of Club Ebios-RM for the development and improvement of its risk management method,
- Being a member of ACN, the Digital Trust Association.

Relying on highly qualified engineers, **ACG Cybersecurity**

has gained the satisfaction and trust of its customers and partners and continues to develop its recognized skills in the evaluation, audit, consulting, support and expertise, and training in information systems security for a sustainable implementation of the French, European, and the international market.

ACG Cybersecurity has a wide and an ambitious catalog of services in its preferred areas:

- Implementation and maintenance of Management Systems (Information Security Management System (ISMS), Privacy Information Management System (PIMS), and Business Continuity Management System (BCMS), including several references and certified clients.
- Continuity and Crisis Management.
- Technical audit and penetration tests.
- Advice and compliance audits (CIS, RGPD, PCI-DSS, HDS, Swift).
- Governance and functional safety.
- Cybersecurity program management (NIST Cybersecurity framework).
- Skills development, training, and awareness.
- Risk management and control of operational risk.
- Incident management and operational security.

Thus, ACG Cybersecurity is positioned as a pure player in cybersecurity. ACG Cybersecurity has developed, thanks to its multidisciplinary team and specific expertise to define and implement cybersecurity strategies.

ACG Cybersecurity has been able to impose itself on a mature market thanks to its strengths:

- Mastery of cybersecurity standards and benchmarks, risk management methodologies,
- Practice of ISO 2700x, NIST, CIS18, RGPD, ITIL, PCI DSS, etc.,
- The technical expertise of the means of security,
- Knowledge of the issues in the sector and the services involved.

Housed since its inception in Campus Cyber at La Défense in Paris, ACG Cybersecurity is an associate and committed member to the cybersecurity ecosystem in France. This place of exchange, collaboration, and innovation, gives the opportunity to develop its services within the excellence of the cybersecurity field, ACG Cybersecurity has been installed, not only there, but also its training center and its ambitious program.

In addition to its expertise in the field of consulting, auditing, and governance, ACG Cybersecurity has created a Training Center to meet the growing needs and shortage of cyber experts on the market.

To do so, ACG Cybersecurity has been certified by Qualiopi since 2022, certification attesting to the quality of the process implemented contributing to the development of skills and whose training actions are eligible for public funding or mutualized and meet the criteria of the single national quality reference.

ACG Cybersecurity, since its creation, has developed a strategic and privileged partnership with PECB, in addition to the marketing of its services, as an approved organization, its trainers, all certified field specialists, animate and promote its contents and modules, as well as its approach to the development of cybersecurity skills.

A rich training catalog is, thus, set up to meet a proven training need, including PECB certification training (ISO/IEC 27001 Lead Implementer and Lead Auditor, ISO/IEC 27005 Risk Manager, ISO 31000 Lead Risk Manager, ISO/IEC 27032 Lead Cybersecurity Manager, ISO/IEC 27701 Lead Implementer and Lead Auditor, ISO 22301 Lead Implementer and Lead Auditor, CDPO, Cloud Security Manager, Ebios Risk Manager, ISO 38500 Lead IT Corporate Governance Manager, as well as the development of other training courses specific to ACG Cybersecurity, in particular in the areas of pentesting, crisis management, information systems security governance, CISO training, etc.

In 2022, as an academic partner of PECB University in France, ACG Cybersecurity aims to achieve high potential in the field of the acquisition of advanced skills and the delivery of quality diplomas recognized by a certification body and higher education.

ACG Cybersecurity will offer, for the beginning of the school year in February 2023 at Campus Cyber La Défense, three Executive MBA courses, which will be led by certified cybersecurity specialists to obtain:

› Executive MBA in Cybersecurity

The program prepares candidates to manage information security challenges from a technical and strategic perspective with an emphasis on the business side. Candidates in the program develop their technical skills in computer systems and acquire knowledge of business management. They acquire the skills necessary to draw conclusions between information security and business risks.

› Executive MBA in Business Continuity Management

The program provides you with a thorough understanding of the disruptions, emergencies, or threats that an organization faces. You will acquire the skills to respond to, and successfully manage, emergency situations so that the organization's operations and business continuity are not disrupted. The courses in this program prepare you in the areas of disaster recovery, business response, risk analysis, and information management.

› Executive MBA in Governance, Risk, and Compliance

The program introduces you to the principles of risk management and its areas of application. You will become proficient at analyzing all of an organization's operations, whether minor or complex, and identifying areas most susceptible to fraud and risk.

In addition to its consulting, auditing, governance, and training activities, ACG Cybersecurity also has the status of Young Innovative Company by engaging in research and innovation.

Its team of engineers and researchers is working on innovative solutions that will prevent cyber-attacks in the near future and allow other companies to protect themselves and have the necessary tools to face cybersecurity threats. This solution is currently being developed and tested and will be deployed shortly. Through its approach, ACG Cybersecurity enjoys a solid reputation that reflects a professional image that is continuously recommended by the cybersecurity industry. This notoriety is acquired thanks to its customers and partners who have given it their trust, which ACG Cybersecurity is fully aware of, and is thankful to them for doing everything possible to remain earnest of it at all times.

For more information or to request support, please contact us at contact@acgcybersecurity.fr or visit our website <https://acgcybersecurity.fr/>

Note: Certification Audits are conducted only for clients who do not receive consultancy services.



Bechir Sebai

Founder and CEO of ACG Cybersecurity

Bechir has over 15 years of experience in strategic and operational consulting in security and cybersecurity for large private and public groups in France and other European countries. ACG Cybersecurity can

be contacted through: contact@acgcybersecurity.fr





PECB is proud to announce its selection as a 2022 IT & Technical Training Watch List Company!

The title is awarded by Training Industry, based on criteria such as; quality of programs and services, industry visibility, innovation, and impact on the IT market, customer representation, and business performance and growth.

PECB is grateful to our partners and customers for their trust, support, and loyalty. We strive to always stay up-to-date and keep providing high-quality training courses.

FIND OUT MORE





IoT and Edge Computing



BY NIKHIL AGARWAL

The phrases "Internet of Things" and "Edge Computing" seem to pop up in almost every search result I get today. For the most part, they are used interchangeably since they share the same infrastructure. However, upon closer inspection, it becomes clear that they are radically different.

Edge computing complements a number of other cutting-edge innovations, like hybrid cloud and 5G networks. The Internet of Things (IoT) is another area where this technology shines. The edge and the Internet of Things are more than simply a match made in heaven. Inevitably, they will rely more and more on one another.

While the goals of the Internet of Things and the Edge are identical, the paths to getting there are completely different. To see how they vary from one another, we need to examine each technology separately.

IoT in Simple Words

The Internet of Things (IoT) is made up of intelligent devices that are linked to a network. These devices transmit and receive significant volumes of data to and from other devices which results in the production of a vast quantity of data that has to be processed and evaluated.

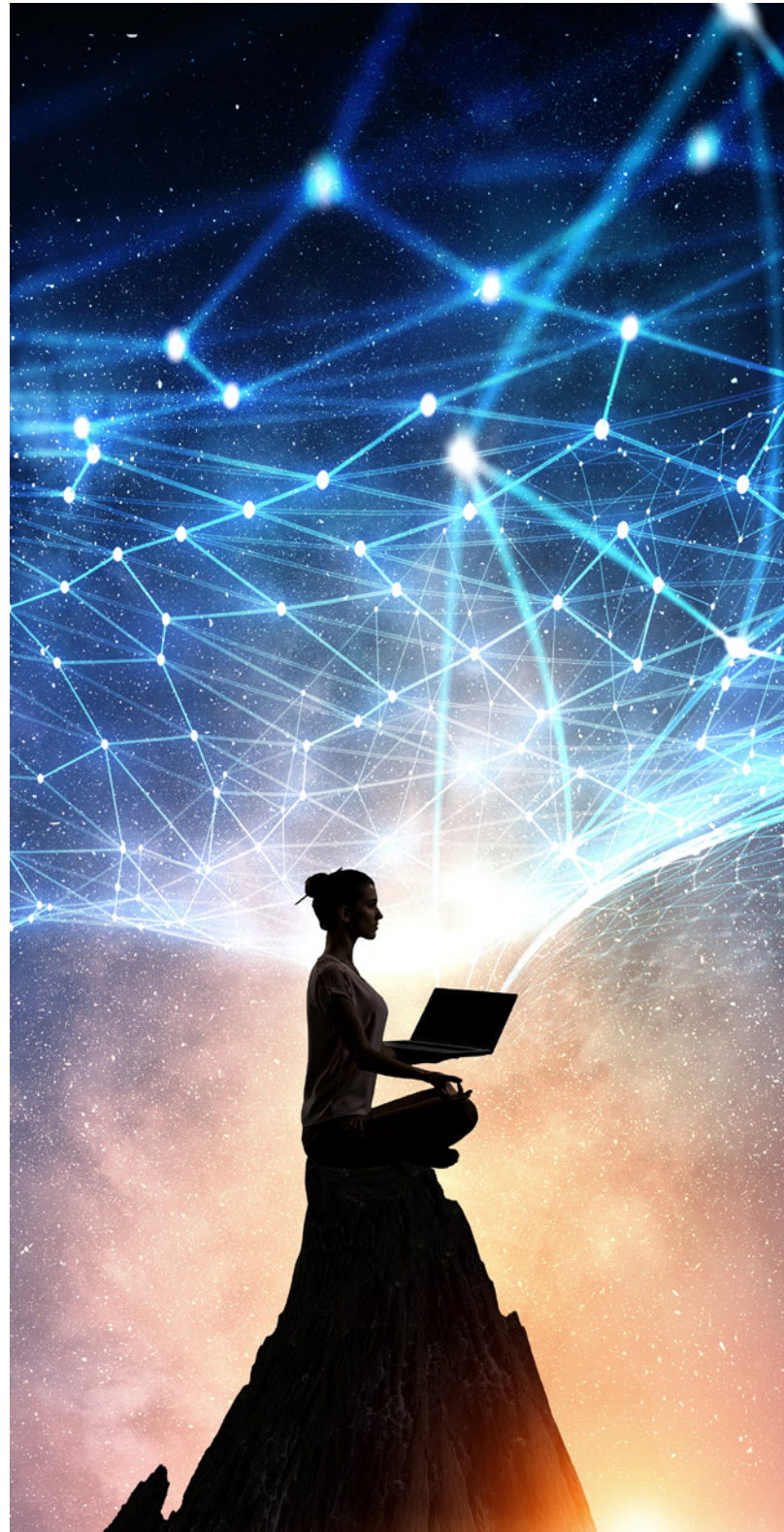
Edge Computing in Simple Words

IoT data may be captured and processed at the edge by using edge computing, which is a technique for computing on-site where data is received or utilized. This eliminates the need to transport data back to a data center or the cloud.

Let us talk about the Internet of Things and Edge Computing with three real-world applications in the market today.

IoT Real-World Applications

1. Automated Home Systems
One of the most important uses of the Internet of Things is home automation.



The IoT ecosystem allows for the connection of common household items, such as thermostats, fans, and lighting, granting the ability to remotely activate or deactivate the devices. That connection and control is made possible through IoT. In a case scenario where I want to make sure my house is nice and toasty and the lights are on when I get home from work. I can use the IoT app to turn on the heat and lights before I get back in my vehicle and go home. When I finally get there, my home will be nice and toasty. I cut down on my energy bill in the process.

2. Robotics and Automation System

The Internet of Things is used in factories to automate a wide variety of procedures. Industrial IoT (IIoT) is mainly used to manage equipment and collect vital performance data. The Internet of Things (IoT) is also used by smart factories to automate manufacturing pipeline processes. There is no need for human involvement in any of these processes either.

3. Management of the Supply Chain

Devices connected to the internet allow supply chain managers to monitor the whereabouts of goods in real-time. Managers make use of sophisticated routing algorithms based on the data they collect to speed up shipping times. The Internet of Things is also helpful for obtaining information after an event has occurred. Thus, that helps the administration to make well-informed choices.

Real-World Application of Edge Computing

› Self-Driving Cars

In order to function properly, autonomous cars must constantly gather information about their surroundings. All of this crucial information is analyzed via edge computing. Then, it processes information in real-time to make judgments that aid the car's navigation.

› The Agricultural Sector

Information regarding crop development, available sunlight, soil quality, pesticide influence, and other factors may be gathered and analyzed with the use of edge computing. To better their operations in the here and now, farmers may utilize this information. They may change when they harvest, how often they irrigate, how often it rains, etc., based on the weather forecast.

› Production and Factory Work

Edge computing is used by many industries to collect real-time information about their production processes. They use this data to effectively locate production issues.

As a result, the quality of the finished product is enhanced.

- › In what ways, beyond processing and analytics, may IoT make use of edge computing?

Latency

Many IoT apps are sophisticated, monitoring systems that gather, analyze, and act on data. This is done hourly, daily, or as prompted by a device contact. Edge computing helps IoT get real-time information. By putting computation near IoT devices, data gathering and analytics are closer (i.e. often within the same country or region, perhaps even on the premises, rather than in a large centralized data center). The shorter round-trip to and from the data center reduces network latency. Edge computing optimizes IoT apps requiring real-time activities (e.g. cooling systems turned on as soon as a sensitive piece of machinery starts to overheat).

Bandwidth

Many IoT devices transmit tiny data packets to a data management platform that does analytics. Currently, data is sent to a centralized, typically private, cloud infrastructure. Future growth in connected devices may overburden operators' backhaul networks. Even though individual data packets are just a few bytes, when streamed in real-time from multiple devices in a relatively limited geographic region, e.g. a manufacturing facility or metro center, the cumulative impact might be considerable. Edge computing may analyze and filter IoT data closer to the devices, optimizing bandwidth by sending only data required for long-term storage or analysis to a central management platform.

Security

How to handle security as more devices are linked is a key IoT challenge. Malware may utilize IoT devices to launch DDoS assaults. Edge computing is not more secure than a private cloud, but it is more proximate. Edge computing may let organizations store data in regions with differing data protection rules than where the data is created. If edge servers are on-premise, firms can be confident data never leaves their local boundary and restrict access to the servers holding the information.

With edge computing, data processing occurs as near to an IoT device as feasible. As a result, there may be benefits for business IT in the areas of latency, performance, cost, and security.

Conclusion

IoT operates without edge computing in many useful scenarios. Edge computing might become essential as more devices are networked and use cases with stricter latency, bandwidth, and security requirements are explored.

Unknowns and obstacles will decide edge computing's future position in IoT. These include protecting the physical security of edge infrastructure, which stores data outside of designated data centers. Many systems strive to tackle interoperability difficulties and ease device administration and control.

IoT and edge computing save people and companies time and effort. IoT and edge computing may be used in the same infrastructure to accomplish distinct goals.

IoT and edge have separate purposes while seeming similar. Some firms mix them to accomplish aims. IoT devices capture data and edge devices analyze it at the source to provide companies with instant, comprehensive insights.



Nikhil Agarwal

Technologist, Cybersecurity
Advisor and Penetration Tester

Nikhil is a Senior Solution Architect with [Fortanix Inc.](#) and the architect of enterprise-scale confidential artificial intelligence and computing projects.

He is also an inventive, avant-garde

information security leader and evangelist.

Among the top 25 consulting leaders, ranked by [Analytica](#) 18th in Cybersecurity, 10th in Emerging Technologies, and 3rd in Cloud Security in 2021.

Nikhil has evaluated and designed security-focused tools and services for Cloud, Containers, and CICD pipelines, leading teams to implement them. These tools and services cover application and platform security, orchestrate security controls, and integrate with security operations, identity, and access management (IAM). Nikhil is well-versed in all facets of cybersecurity, from the more established methods like penetration testing and DevOps to the more cutting-edge Next-Generation methods like red teaming, shadow IT, cyber threat intelligence (CTI), darknet monitoring, and forensics.

Nikhil has extensive experience working in EMEA and APAC across a wide range of client industries, and he is well-recognized as a technological specialist who is eager to share what he has learned with others.

Social Website – www.reachtonikhil.com





PECB's Newest Training Courses Have Launched

PECB is happy to inform you that we have launched two new training courses:

- Lead Crisis Manager
- Digital Transformation Officer

For more information please visit www.pecb.com.

The Life of an AI Expert



BY LÁSZLÓ GRAD-GYENGE

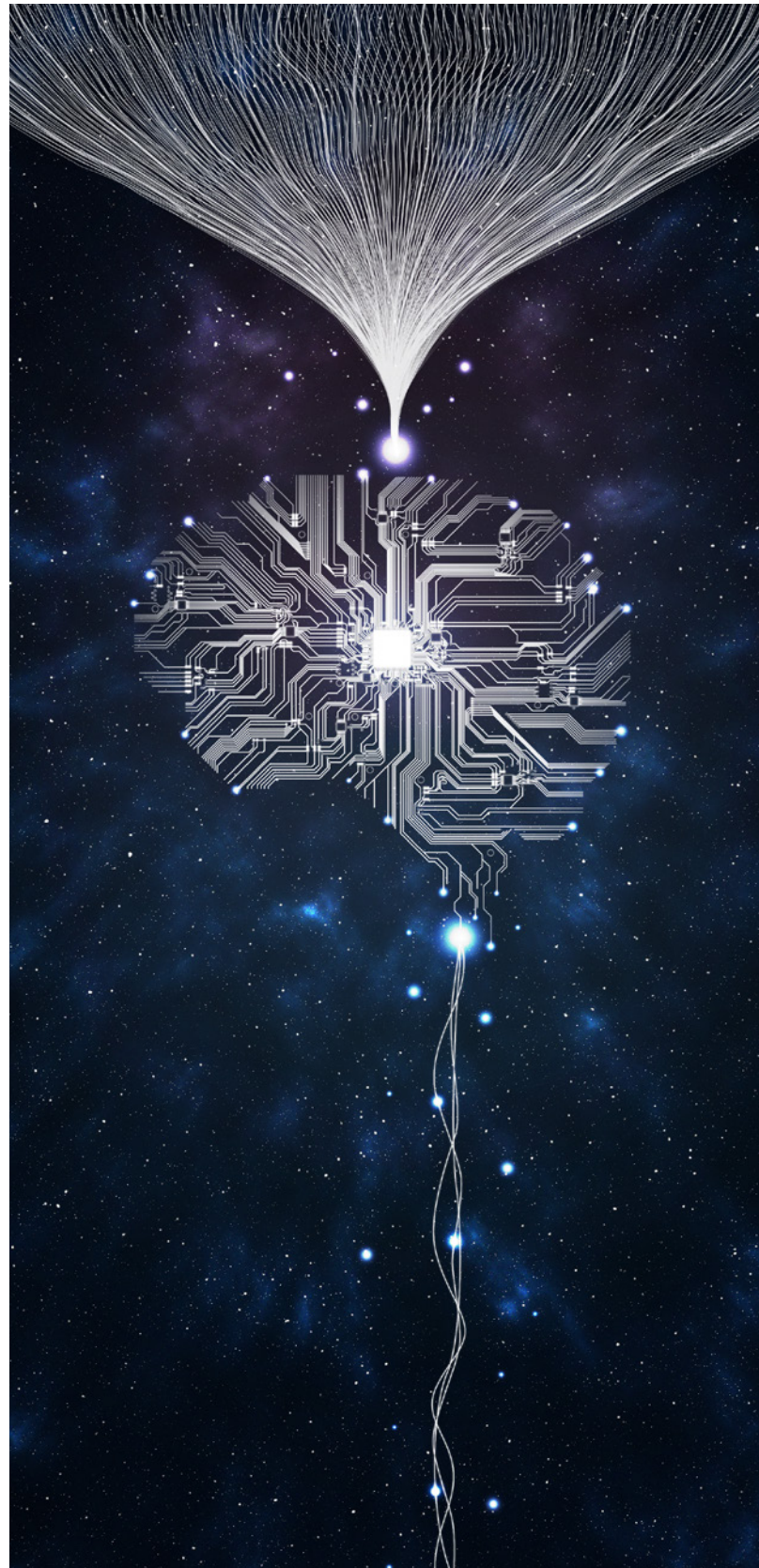
Defining the AI expert, one might start with the definition of the base vectors, the prototypes of such professionals. Some candidate prototypes can be: the AI expert who works as an employee in a well-paid position at a tech giant, a famous professor at a top university being a well-known expert in the field of machine learning, or the leader of a company that specializes in a particular field of AI. As most of us, I am neither of the above, but I am somewhat a combination of the prototypes above. Therefore, I hope, through this article, I can offer some insights and present an example on the lifestyle of an AI expert.

To summarize the life of an AI expert in one word: analysis. In two words: constant analysis. The thirst for knowledge is a key motivating factor for me. To explain it with an analogy, understanding the physical, chemical, biological, ethological, sociological, artificial, and organic structures I meet with, is similar to what the Grand Unified Theory (GUT) means for a physicist. The main aim of GUT is to unify the fundamental interactions between particles into a single model.

In my case, the difference can be found in the scale. While GUT focuses on a model at a single scale, at the level of particles, I try to be multimodal and multiscale. As we change the scale from physics through chemistry, biology, human ethology, to sociology, the magnitude or aspect changes. Chemistry is based on the rules of physics, but we need special techniques to describe chemical processes.

Biology is based more or less on chemistry, but we use special techniques to describe the genotype and the phenotype of living beings. We arrived at the level of individuals. Ethology provides the techniques to study and analyze the behavior of these complex and self-organizing structures built up from atoms. Some of the high-level living beings are not operating individually and organize themselves into smaller or bigger groups, like an ant colony, a shoal of fish, a pack of wolves, a cow herd, a village of people, or an office of people.

Physics is the first gate to pass. The world that we live in is based on more or less simple rules of physics. To be more exact, on the scale that we live on, most of the physical phenomena can be described with linear or quadratic relations and relatively simple distributions.



However, physics becomes much more complex when we change the scale to the atomic or to the galaxy magnitude. How is it related to AI? There are already published results about estimating fluid dynamics with artificial neural networks. These days I work on the estimation of the properties of scattered light in the field of Raman spectroscopy to identify certain materials. The first thing to do here is to understand the underlying physical process in order to define an algorithm that catches the essence of the physical process.

Another project I work on these days can be found in the field of petrochemistry. For context, it is not biochemistry but it was a few hundred million years ago. These days, it is more organic chemistry according to that huge meteorite. The task in this case is to optimize the production process. I work closely with experts in this field. We work with a relatively complex model of the production line and later hopefully on the real-time process. The goal in this case is to optimize the models according to an objective function, which can be cost minimization, profit maximization, quality improvement, etc.

Communication is an essential tool for us that can be helpful when organizing individuals into groups or society. Its most adequate and long-lasting form is the written text. I had the chance to work on a software product that relies on the latest results of computational linguistics and semantic modeling. The goal of semantic modeling is to develop algorithms that model the meaning of written text of natural language. To explain it with an example, let us take a look at the following two questions.

When is the restaurant open? What are the opening hours of the restaurant? The questions are formulated differently but have the same meaning. This is what the algorithms should catch. This task is solved with the help of semantic encoders. Semantic encoders assign a semantic vector to a text (question, answer, sentence, paragraph, etc.) in a way the vector holds the meaning of the text. It means that two different texts with similar meanings should be mapped to similar semantic vectors. We apply such algorithms to implement a semantic search engine that helps companies with information as an asset to manage their company documents.

A less business-focused but more society-oriented software I worked on is the MediaBubble project. The project was funded by Google DNI. The main goal of MediaBubble is to help people extend their filter bubble. It is based on the phenomenon that most people – let us call them online news readers – acquire their daily set of information from a single news source.

The problem is that such readers can be easily influenced as they have no chance to deeper analyze the information, and no chance to fact-check. Our software worked on the Hungarian online media. We developed web scrapers that collected the news from the major news portals. Then semantic encoders and clustering techniques have been applied in order to conduct real-time topic detection. With the help of this information, we were able to present the reader articles outside their filter bubble. This way, the readers had the chance to extend their bubble and be less influenced.

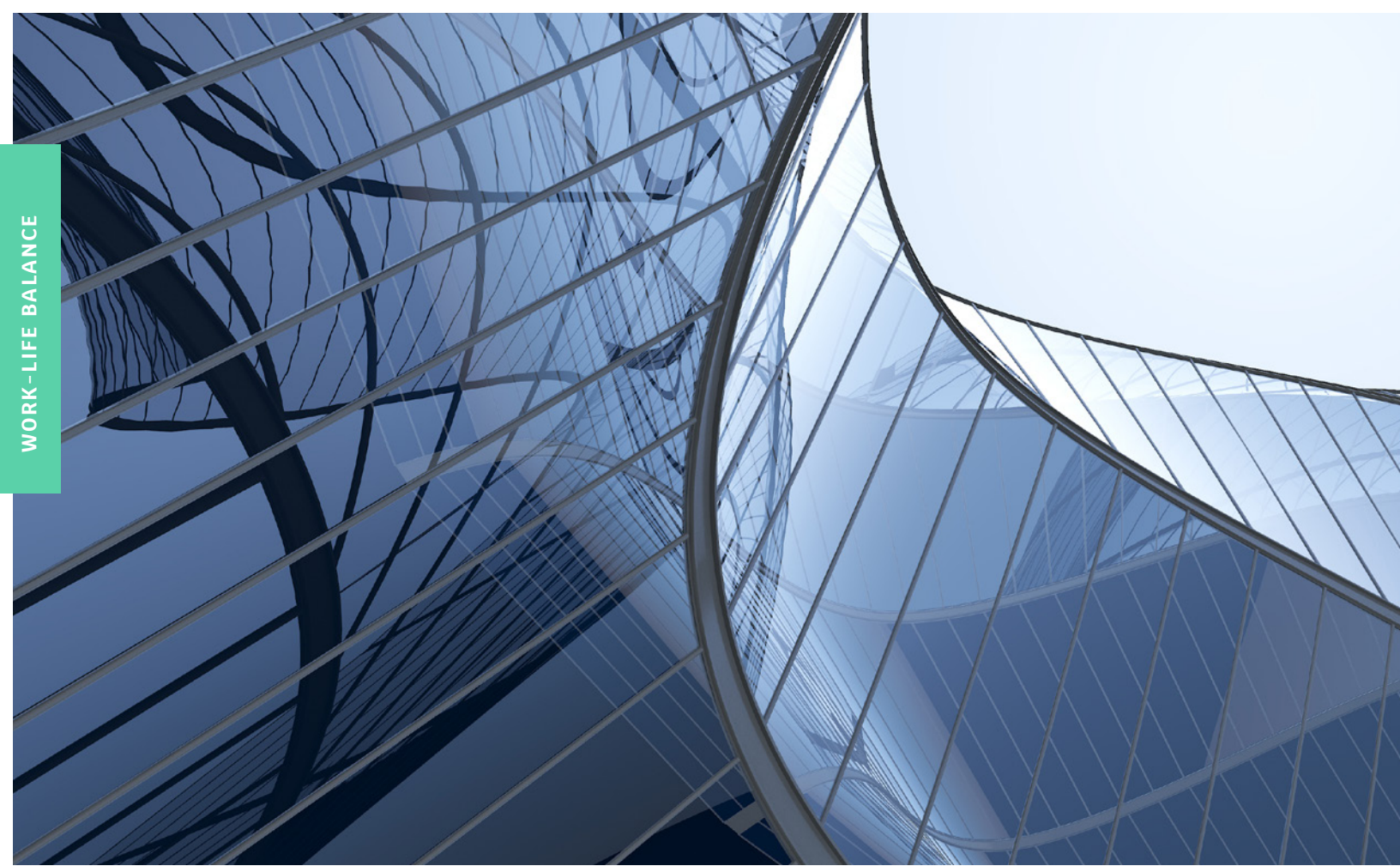
The main drawback of written text is that it misses an important communication channel, the meta-communication. Fortunately, there are already existing techniques to analyze human meta-communication from multiple aspects. My company is involved in a project titled AIMLP. The project goal is to estimate leadership competencies based on video, audio, and EEG signals. The video signals are processed with emotion and gesture detection algorithms. I guess that facial expression detection algorithms are well known for everyone from the bounding boxes on faces indicating happiness, sadness, fear, disgust, neutral, etc.

Gesture detection is a plus from our side, as unlike facial expressions, gestures are more instinctive and cannot be controlled consciously. We consulted with experts in this field and identified the essential gestures that can be relevant in this use-case. Such gestures are hands in the pocket, touching the nose, hands being kept near the body, straight posture, bent posture, etc. Having the list of relevant gestures identified, we developed a video processing software that detects the mentioned gestures.

A commercial EEG device has also been involved in the project in order to detect focus, stress, or neutral mind states. The audio processing is done by the partner company [Sestek](#), as we work on this project in a consortium in the frame of a grant. The consortium lead is the Singaporean company [8nalytics](#), as they have expertise in the field of behavioral science. If you are interested in our technology, you may take [a look at the project](#).

The rest of my observations and conclusions in the field of ethology and sociology are credited to survival in an office environment. According to one of my professors, in such an environment, individuals follow a twofold strategy of cooperating and competing at the same time. It means some good guesses can be helpful to improve a career.

One may also think about the presence of the two forms of behavior regarding Evolutionary Stable Strategy (ESS).



ESS is a term in the field of biological modeling and evolutionary game theory.

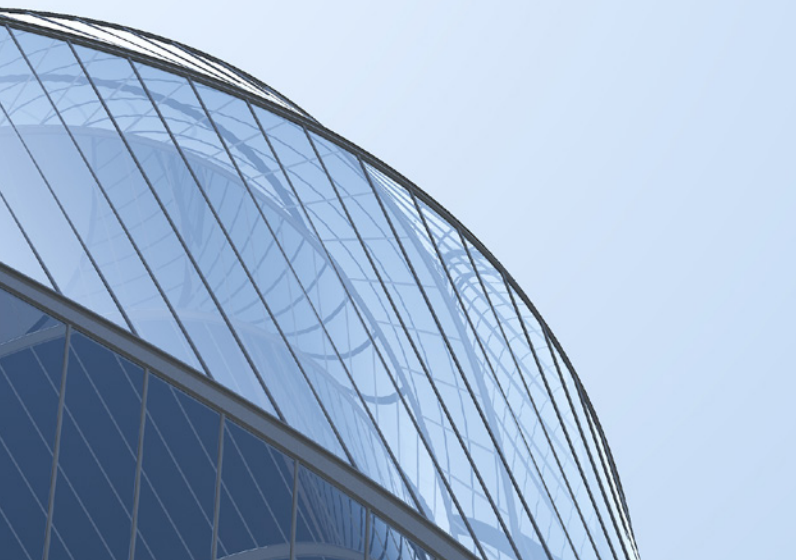
As an example, imagine a bird population. There are two types of behavior when two males meet in the mating period. Option one is to pose, option two is to fight. If all the birds take option one, then the population will be weak in the long term, as nothing ensures that the strongest survive. If all the birds take option two, then no males will be left for reproduction. The truth is somewhere in the middle, as evolution may aim more for adaptability. There will be posers and there will be fighters.

The question lies in the ratio. What is the ideal ratio for a population to be the most effective? As with every concept, ESS can also be generalized for more options and can be applied to the human race in, e.g., an office environment. We just finished the proof of concept of an Industry 4.0 project. The goal in this case is to monitor the production line with a smart camera for process monitoring.

We embedded state-of-the-art computer vision algorithms in the system that conducts object detection. Such algorithms are capable of identifying a class of objects that have been shown the algorithm before. The actual classes are forged material, molded material, spring, and gumi ring.

The outcome of the machine learning algorithm is then used to record the point of time when a particular part has been mounted to the product, as we talk about an assembly line. This way we can understand the change in time and are also able to detect if a part has been skipped. A typical problem in our case is when a gumi ring is omitted from the product, which can lead to a serious drop in the pressure.

As the product is actually a train brake, it can be problematic, as the brake force significantly decreases in this case. Fortunately, the brake system is designed in a way that the other brake devices can compensate for the breakdown. And at last, some words about the project of my heart, the electronic nose. The idea of our electronic nose is to develop a device that is able to identify smells and odors. The original plan was to develop a breathalyzer to identify COVID-19 infection. Although the prototype of our device was ready, we did not manage to find a medical partner to conduct the trials, because the system was overloaded. As we had the device, we started to measure smells of objects or fluids that we found in the lab. The first trial was to identify if there is sugar in the coffee or not, which task we managed to solve. Then we did experiments in the food industry to identify spoiled meat, milk, etc. We also work with the police to find drugs and explosives.



You may know the classical slogan: data is the new oil. To train a machine learning algorithm, you need data. You need a lot of data and relevant data. The essential property of machine learning algorithms is that these algorithms provide good quality estimations in a familiar environment, on the domain where the training data resides. This property can be explained by the difference between interpolation and extrapolation. Interpolation always has the chance to provide better quality estimations than extrapolation. AI experts work in a similar way. You train them, and feed them with information. The more domains are covered by the training data, the better estimations and predictions can be provided by them. This mechanism is similar to image augmentation, where the images shown to a neural network are enriched artificially, which technique leads to an improvement in the final quality.

You may conclude that I work maybe too much. Yes. It is true. The reason is that I love my job. On the other hand, I have some experiences outside the matrix. I love my family. I try to spend as much time as possible with my wife and daughter. I am pretty much into art, and sometimes do art. Sometimes I do art with my daughter. These days more [photography](#). Decades before painting and clay sculptures. Sometimes music, guitar or saxophone. I managed to finish writing my book, which is a series of interconnected short novels. The illustrations are to be done. A few weeks ago I bought a Kiel Boat (Hungarian notation). The plan is to reduce workload and do more sport.

We may finish with a citation from Einstein: “Imagination is more important than knowledge.” I agree. Imagination is crucial in the life of a researcher. I would add one thing: “The stable ground”. I think that one can be creative in a field if the essential knowledge is also available, is rich enough, and is represented properly.

You may take a look at my [homepage](#) for more information on our results in this topic. As you may have guessed, I am not an employee with a 9 to 5 type of job. I am an entrepreneur. I manage my own company. It means that while being an AI expert I also have to manage my team and build the business. High-quality software is to be delivered. We have responsibilities, bugs, and warranty periods. This is where I learned how to build complex software systems, run a business, manage employees, manage projects, and manage clients.

Artificial intelligence can be found in the intersection of mathematics and computer science. It means that if you want to be good at it, you have to be both a mathematician and a computer scientist. Mathematics is needed to know what to implement. Computer science is needed to be able to implement it. This is what my degree is based on.

But I did not stop learning. I think that lifelong learning is important. This is the reason why I decided to have a half status at the University. Here I work with students. They learn from me, and I learn from them. Fair deal.

The disadvantage of my approach to a hybrid life is the stress factor. Its advantage is that I have the opportunity to see the world from several different aspects. When doing the balance, I find it worth it.



László Grad-Gyenge
Artificial Intelligence Expert,
Researcher, and Lecturer

László is the owner and managing director of CREO, a software development company. The company mainly does business software for multiple platforms as web development and app development. Creo has a special interest in the MedTech sector.

In his daily work, László focuses on applied AI projects. He works in various domains, such as recommender systems, natural language processing, digital signal processing, computer vision, and autonomous vehicles. His goal is to apply his AI algorithms in the software products developed by his company.

PECB INSIGHTS 2022 CONFERENCE

The PECB Insights Conference 2022

The two-day conference event featured a number of different panel sessions and roundtable discussions on topics related to Information Technology and Security and Privacy.

Agenda

The Need for Ethical Hacking: Why Organizations Need to Employ White Hat Hackers

Facebook's Meta-Verse and Its Impact on Privacy

No Cookies for Me: How Successful Will ePrivacy Be at Reinforcing Digital Trust and Security?

GDPR vs. US Data Privacy Legislations: Which is Proving More Successful and Why

Blockchain and Tokenization: How Secure and Reliable Is It?

Opting Out of Data Tracking: Apple's Take on Privacy and Should Other Manufacturers Follow

Top Cybersecurity Risk Predictions for 2023 and Beyond

Cloud Security and Insecure APIs: How Crucial is Good API Management?

Meet our speakers



ROB VAN KRANENBURG
Chief Innovation Officer at asvin.io
BELGIUM



ADRIAN DAVIES
Principal Consultant and Cyber Risk
Management Group at CRMG
UNITED KINGDOM



CHRISTOPHE MAZZOLA
vCISO at Mobilexpense Senior Cybersecurity
Consultant at Approach
BELGIUM



MICHAËL RAISON
Senior advisor, Auditor & Coordinator at
Approach Belgium
BELGIUM



JORGE ALEJANDRO CARRILLO UGALDE
President at (ISC)²
CZECH REPUBLIC



SILVANA TOMIC ROTIM
CEO & Consultant at ZIH
CROATIA



NNASOM JUNIOR NELSON
Data Protection and Cybersecurity Manager at
Excilone
FRANCE



BENJAMIN KORNHAUSER
Founder at VDS & Cie Information security
training, awareness and auditing
FRANCE



PIERRE MARI
Founder of BlockX
FRANCE



FATOS ISMALI
Senior Data & AI Solutions Architect at Microsoft
UNITED KINGDOM



AHMED AFIFI
Cyber Security Manager at the National Bank
of Egypt
EGYPT



CHRISTOPHER MAGNAN
Program Manager at Superlative Technologies
UNITED STATES



ANASTASIIA OSTAPENKO
CEO of Simple Security & Compliance
UKRAINE



DR. ROMAN KREPKI
Senior Manager - Cybersecurity and Risk at
Mazars GmbH & Co. KG
GERMANY



OLIVIER GUILLO
CEO of Smart Global Governance
FRANCE



ALI LARIBI
Founder and Cybersecurity senior consultant at Fortress Plus
FRANCE



ALEXIS HIRSCHHORN
COO - Head of Advisory Services at Abilene Advisors S.A.
SWITZERLAND



RALF SCHADOWSKI
Head of Data protection at ADDAG GmbH
GERMANY



ABDEMALEK NAJIH
Founder and CEO of AN Advice Sàrl IT Security Compliance and Threat Intel Officer at IQ-EQ
LUXEMBOURG



CHRISTIAN DE BOECK
Managing Consultant at Synergit
BELGIUM



GUENAËLLE BLANCHET
IoT, Data (Consultant and Trainer)
Founder of New Business IoT and SCANSOR
FRANCE



DR. OBADARE PETER ADEWALE
Co-Founder & Chief Visionary Officer Digital Encode
NIGERIA



ALAIN HERRMANN
State Data Protection Commissioner
LUXEMBOURG



KAROLIEN VAN BEL
Managing Partner at OLINKO
BELGIUM



MARK OLIVER NEUFURTH
Product Marketing Expert at IONOS SE
GERMANY



NATHALIE POUPAERT
Local Privacy Officer North Europe at Sanofi
BELGIUM



HAMID JEMRHILI
Independent Auditor, Consultant and Accredited Trainer by: PECB, ECCouncil, APMG, ISACA, PeopleCert
MOROCCO



OVIDIU IONESCU
Chief Executive Officer of Punto Iberica SRL
SPAIN, ROMANIA



RINSKE GEERLINGS
Managing Director at Business As Usual
AUSTRALIA



ALGIS KIBIRKSTIS
Principal Security Consultant at EthISecure Services
CANADA



JESSICA DENEET
Privacy Consultant at CRANIUM
BELGIUM

Business Intelligence, Big Data, and Data Mining



BY JOSEPH IYOFOR

LEADERSHIP

Business Intelligence, Big data, and Data Mining are all buzz trending words, in multiple industries, different forums, and C-level strategy discussions. All the talks and discussions about these three intersecting subjects matter for several reasons:

1. The next stage of human evolution is digital.
2. AI/ML is a transformative general purpose technology that is affecting and will continue to play a huge role in the way we live and work as humans.
3. Transformative technology comes like a wave, one thing leads to another and it does cause massive disruption in multiple industries, creating new sets of demand and supply in its wake.
4. The huge volume of data that is generated each year, which doubles every 2 and a half years, has to be processed for value creation.

What really are Business Intelligence, Big Data, and Data Mining? Do they really have anything in common? Do they even really intersect at some point in value creation? Let us, firstly, understand what this subject matter is, and then we will see how they relate, have clarity, and intuitively separate the hype from the reality of what can be accomplished with one versus the other.

Business Intelligence is a technologically driven process of analyzing data, and technical information and presenting it in a user-friendly view, such as reports, charts, dashboards, and graphs for actionable business decision-making. It informs decisions and combines a variety of tools and technologies to achieve this. So it is a process, not a silver bullet that automatically gives an organization meaningful insight to its data collection. Data is the new oil, if your organization is to stay ahead of the competition with innovative solutions and services, it must have the right tools and technology, and more importantly the right people to put it all together by asking the right questions to derive meaningful insight from their data collection.



This is what business intelligence is all about. Big data is larger, more complex data that is generated and transmitted in real-time from a variety of sources. It could be structured, semi-structured, and unstructured data.

Examples include social media chats and conversations, healthcare devices and the information it sends, household IoT devices, equipment sensors, etc. Not every data that is huge is classified as big data.

Its attributes or what marks it as big data include;

- › **Volume** – A large quantity of data that is generated and sometimes stored for further processing
- › **Variety** – The type and nature of data that keeps evolving
- › **Variability** – The distance of data points from one another from the distribution center
- › **Velocity** – The speed of data generation or processing is heavy, fast, and large
- › **Veracity** – The quality of the data being analyzed

Big data application is for batch processing or real-time processing, which to be used depends on what you are trying to achieve or the question you are seeking an answer to. Data mining – data mining is the process of sorting through large data sets or blocks of information to identify patterns, trends, or relationships that help in solving business problems through data analysis. Its endpoint is to enable an organization to predict future trends and make better-informed business decisions. It is also known as Knowledge Discovery in Data (KDD).

Data mining is at the heart of the Digital Revolution that is ongoing, it has created the cloud computing industry with its many specializations and cutting-edge technology that has evolved from the Hadoop architecture, Apache Spark, and now Databricks. All of this is needed because conventional databases, such as MySQL, Postgres, MongoDB, etc., cannot handle big data. To sum it all up, Business Intelligence answers the business questions of: “what has happened?,” or “what will happen in the future?” Big data and its machine learning algorithm toolkits tell an organization holistically, it is largely probabilistic while Business Intelligence is somewhat deterministic. Data mining is the advanced toolkit for Business Intelligence and Big Data Analysis.

For those in leadership positions in this industry, it is highly important to make sure that you are well-informed with all the latest trends and news in order to ensure that your organization is up to standard with all best practices.

It is the leaders' responsibility to make sure that the team is also well-informed by being transparent. Utilizing technologies that process, store, and facilitate data analysis is essential to setting up an effective big data environment. The utilized infrastructures are deployed more than once and different infrastructures to cover all various aspects of data for an organization. Understanding how to use and manage big data in your organization can be a massive advantage in the market.

Business Intelligence provides your organization with the needed knowledge on the impact of current practices within your organization, employee satisfaction, and all internal data you may need to push your strategies in the right direction, such as company satisfaction, media reach, employee performance, and much more. For leaders that employ that knowledge, of the analysis of past and current data, in their organization's strategies and future plans in the correct way, the impact is sure to be noticeable.

As data mining is predominantly used to identify smaller and specific pieces of data, organizations are evidently seeing the benefits of sorting through large data in order to pinpoint relevant information. This is done in an effort to make the management's and leaders' decisions more precise and beneficial to the organization.



Joseph Iyofor

Transitioning to Analytics/
Data Science Product
Management

Joseph Iyofor, who is transitioning to Analytics and Machine Learning Product Management, has an MBA from the prestigious Edinburgh

Business School, has over 8 years of experience delivering best practices in Risk Management, Internal Control, ISO Management Systems, and Business Analytics. He has several professional certifications in different fields, which include: ISO 31000, GRCP, CICP, CRCMP, CRBA, etc.

As a consultant, he has trained several officials and personnel of Renaissance Capital, Liberia Revenue Authority, First Bank, to name a few, on ISO 31000 best practices and implementation, business performance improvement, internal control mapping, cost reduction in project management, GRC implementation, etc.

He has advanced problem-solving skills and is a believer in creating value with best practices. He loves to read and explore.

ISO/IEC 27001:2022 and ISO/IEC 27005:2022 Are Now Published

ISO/IEC 27001:2022 provides requirements for organizations seeking to establish, implement, maintain, and continually improve an information security management system.

ISO/IEC 27005:2022 provides guidelines for the establishment of a systematic approach to Information Security risk management. This international standard supports ISO/IEC 27001 concepts and is designed to assist an efficient implementation of information security based on a risk management approach.

ISO/IEC 27001:2022 and ISO/IEC 27005:2022 are available for purchase online (PDF only) on the [PECB Store](#).

FIND OUT MORE



ISO/IEC 27001:2022

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

This document
implementing, i
information sec
the organization

ISO/IEC 27005:2022

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

This document provides guidance to assist organizations to:

- fulfil the requirements of ISO/IEC 27001 concerning actions to address information security risks.

Integrating IoT and Blockchain to Your Cyber Safety



BY GOVINDA MENGJI

IoT and Blockchain have become buzzwords in the current technological era. Every new technology solves some problems and generates new challenges. Cybersecurity is one major challenge that is hindering the fearless usage of technology. The solution lies in how effectively these technologies are integrated and implemented. Hence, this article is an overview of the integration of IoT and Blockchain to ensure cyber safety. It also discusses the essential security measures and lists the IoT security challenges.

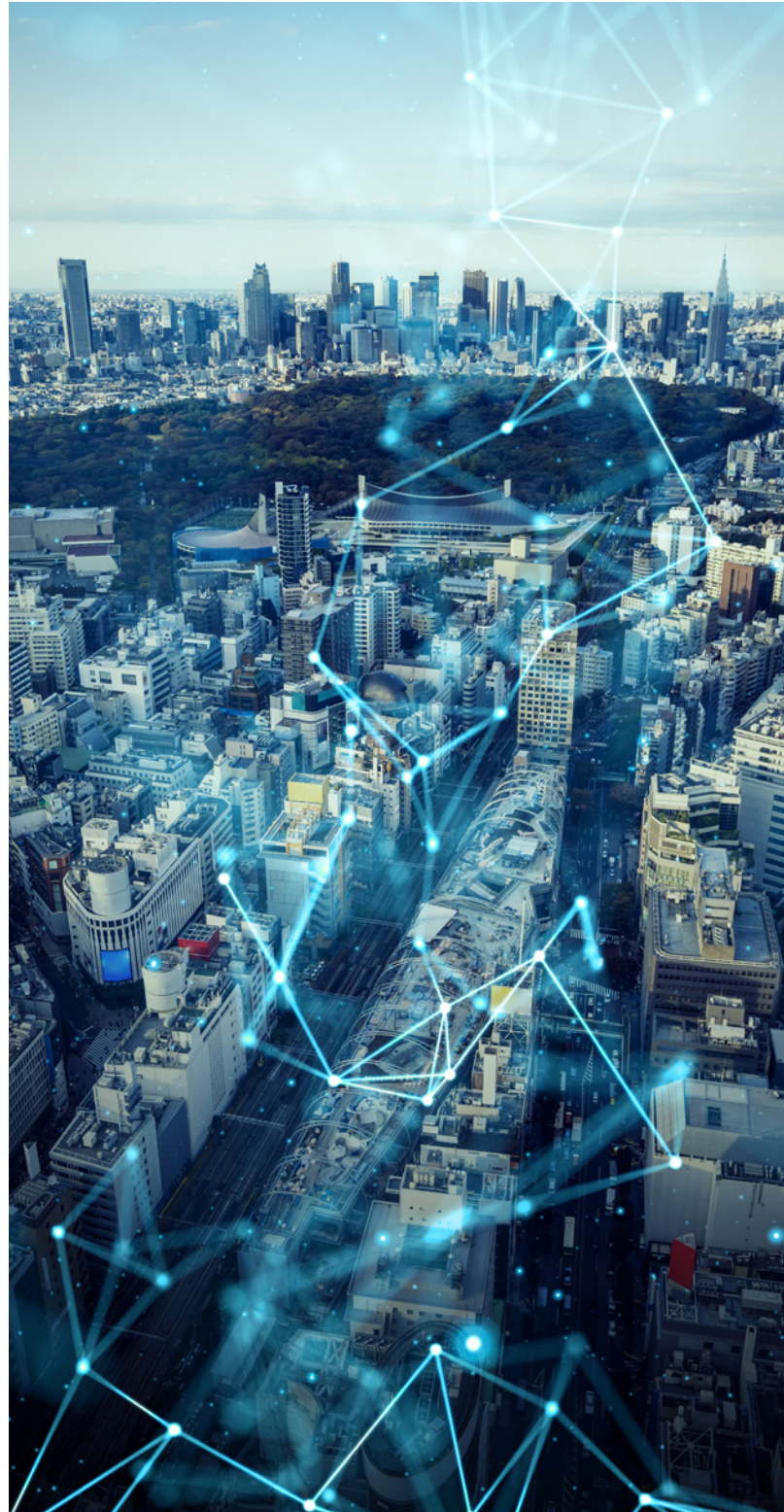
IoT Overview

The network of physical electronic devices, or machines, are implanted with sensors and software for the purpose of communicating and exchanging data with other devices and systems through the internet, each of these devices has an IP address, is referred to as the Internet of Things (IoT). Today IoT plays a major role in transforming our lives. As technologies are enhancing, hackers and cybercriminals are developing new, high-tech ways to breach secure and private data. However, with significant advancement in the IoT range, the issues related to data and information security needs to be addressed.

IoT has enormous advantages but they often lack security. User data must be kept private and safe. Better security must be created, maintained, and made the norm for IoT and linked devices to keep the data secure. In addition, IoT makes it possible to share data and information via Blockchain.

Highlighting some of the major IoT security challenges:

- › Visibility and Transference
- › Data Privacy, Confidentiality, and Integrity
- › Authentication, Authorization, and Accounting
- › Secure Communications
- › Data Encryption
- › Middleware Security





Blockchain Overview

Blockchain is an indispensable technology that is hitting headlines due to the popularity of cryptocurrencies, such as Bitcoin and Ethereum. Is Blockchain only concerned with cryptocurrencies? The answer is an emphatic no. Blockchain technology has moved beyond cryptocurrencies to another level.

Blockchain is a distributed, decentralized, immutable ledger that can be used to record transactions and track assets with Blockchain, the intermediary in digital transactions is eliminated. In a Blockchain, each block in the chain represents a record and the chain links all of the blocks together.

Key Security Features of Blockchain:

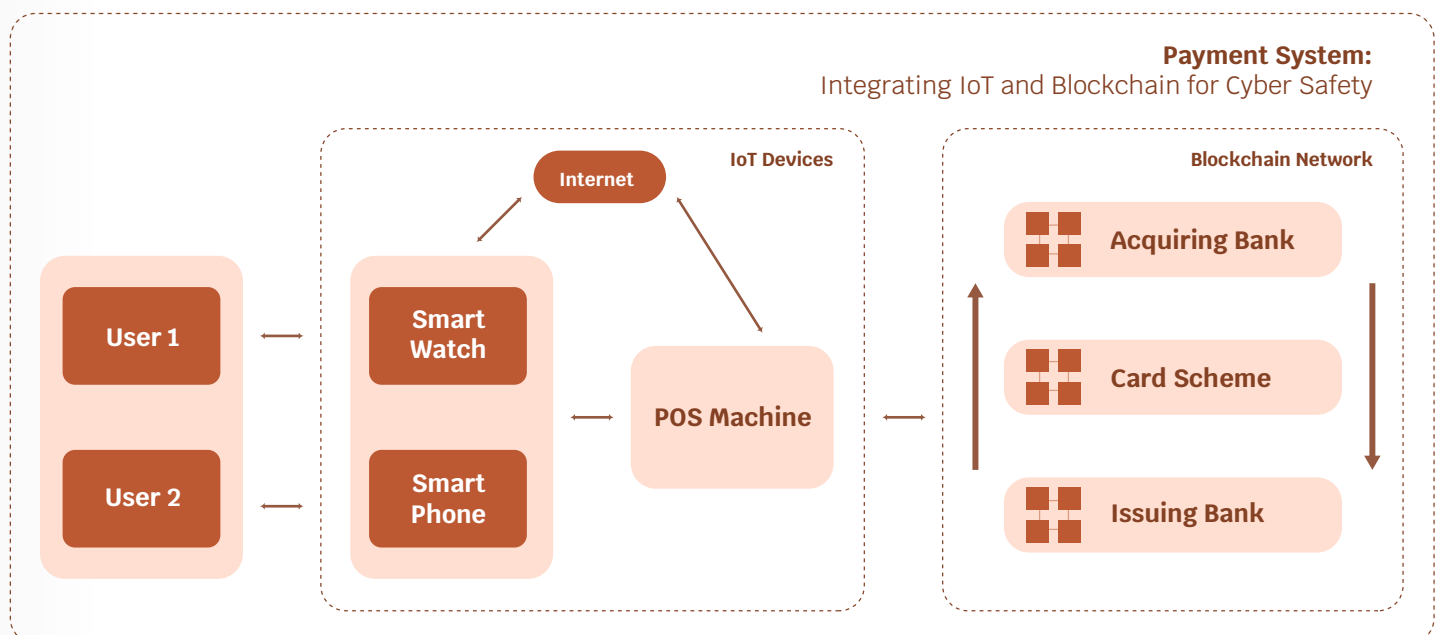
- **Cryptographic Security:** Hash functions are one-way functions where it is simple to go ahead (from input to output) but computationally impossible to move backward (output to input).
- **Identity Management:** Blockchain identity management systems address current identity issues such as: inaccessibility, data insecurity, and fraudulent identities.

- **Multisignature:** Blockchain uses digital signatures to ensure the authenticity and integrity of transactions; Multisignature requires multiple private keys to generate a valid digital signature, allowing multiple parties to approve a transaction. Furthermore, in blockchain technology, it is infeasible to break public key cryptography even by brute force guessing.
- **Data Privacy:** As data in blockchain is immutable and blockchain network can be configured in Private/Public or Permissioned/Open Blockchains
- **Secure Communication:** Blockchain can ensure that an attacker cannot monitor and change the communications occurring between nodes.

IoT and Blockchain are both fantastic innovations on their own, but when they are combined and implemented, they get astounding outcomes that are beneficial for cyber safety.

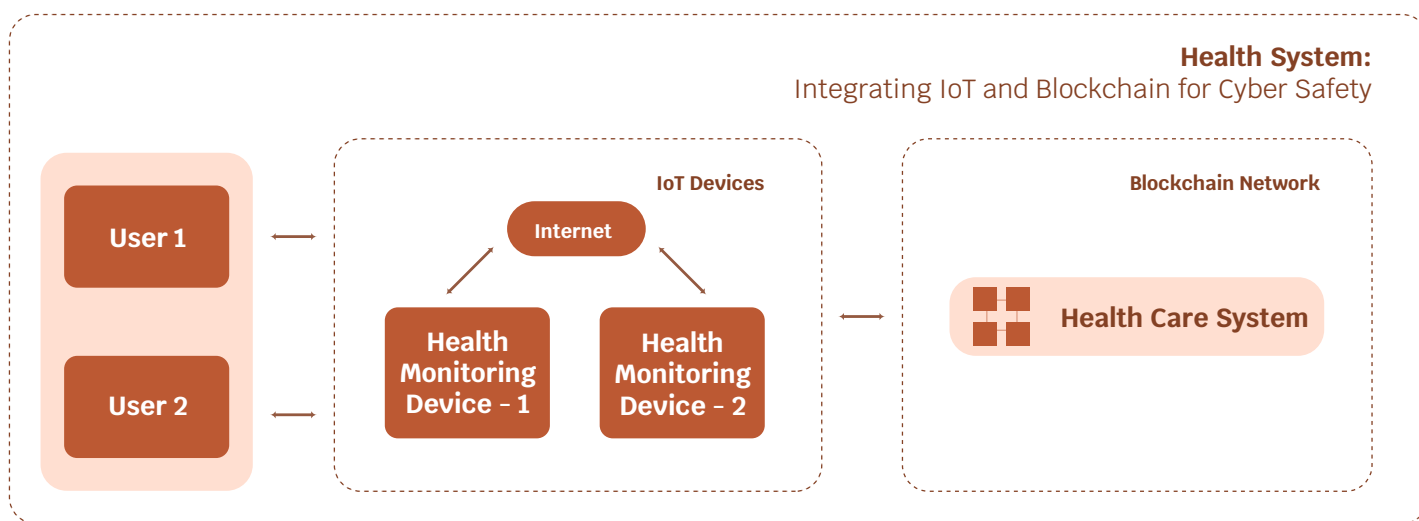
Below are the use cases for integrating IoT and Blockchain to ensure Cyber Safety.

Use case A: IoT Payment System: Integrating IoT and Blockchain for Cyber Safety:





Use case B: Health System: Integrating IoT and Blockchain for Cyber Safety:



Currently, IoT technology is used with conventional databases. The above high-level block diagrams (Use case: A and Use case: B) the Payment and Health Care systems can be replaced by Blockchain technology.

However, the process and flow remain the same.

By adopting Blockchain technology, it is possible to address the following IoT cybersecurity concerns:

- Blockchain is based on peer-to-peer network in which all nodes have the same copy of records which solve the Data Integrity issues.
- Blockchain can be implemented in Private/Public or Permissioned/Open Blockchain. It ensures access control and prevents unauthorized access to Data Privacy.

Furthermore, Blockchain can keep track of data gathered by sensors and prevent fraudsters from duplicating it with other harmful types of data.

- ECDSA (Elliptic Curve Digital Signature Algorithm) solves the limitation of IPv6 address
- Blockchain network can track every transaction and record, which addresses the problems with trusted accountability.
- Blockchain network will be connected to multiple nodes, it will be resilient, and fault-tolerant, this solves the problem of single points of failure.
- Blockchain hashing function generates a unique ID, that can be assigned to each IoT device. Furthermore, each transaction and record will be tracked in the blockchain network which will solve the problem of identifying the trusted origin of data.

- › Blockchain operates on reading writing operations only, data in blockchain is immutable, which will address the data compromise and data manipulation issues.
- › Blockchain technology is third-party and risk-free, as it can perform operations without the intermediary.
- › Smart contract programs help to develop access rights and customize the policies based on the requirements.

Conclusion

The future of the financial sectors and other industries is becoming increasingly digital, which makes the process more convenient for end consumers. Internet of Things (IoT) and Blockchain technology are part of this rapid transition towards the bank of the future, both end users and financial sectors as well as other industries need to adapt to these trends for cyber safety.

Thus, with the development of high-speed networks and sophisticated network devices, IoT is unquestionably an emerging technology. IoT currently faces security limitations and concerns, some of which can be addressed by incorporating Blockchain technology.

The challenges of technology and cybersecurity are two sides of the same coin. The importance of cyber safety increases as technology evolves.



Govinda Mengji
Senior Specialist,
Blockchain, Cloud,
IT-DR at Deloitte

Govinda is a senior specialist at Deloitte – Cyber and Technology, Risk Advisory. Govinda has a degree in computer science and

is a senior specialist cybersecurity consultant. He has implementation experience in technologies, such as cloud and virtualization. He has experience working with multiple industries, such as aviation, health insurance, stock exchange, oil and gas, and banking sectors across the GCC Region.

Govinda is blockchain and cloud certified and supports organizations with technology transformation, cloud strategies, technology implementation, cloud security, cybersecurity resilience, and IT Disaster Recovery (DR).

Disclaimer: The views and opinions expressed in this article reflect those of the author and not of his organization, company, or colleagues.



Data Privacy in the Age of Digital Transformation



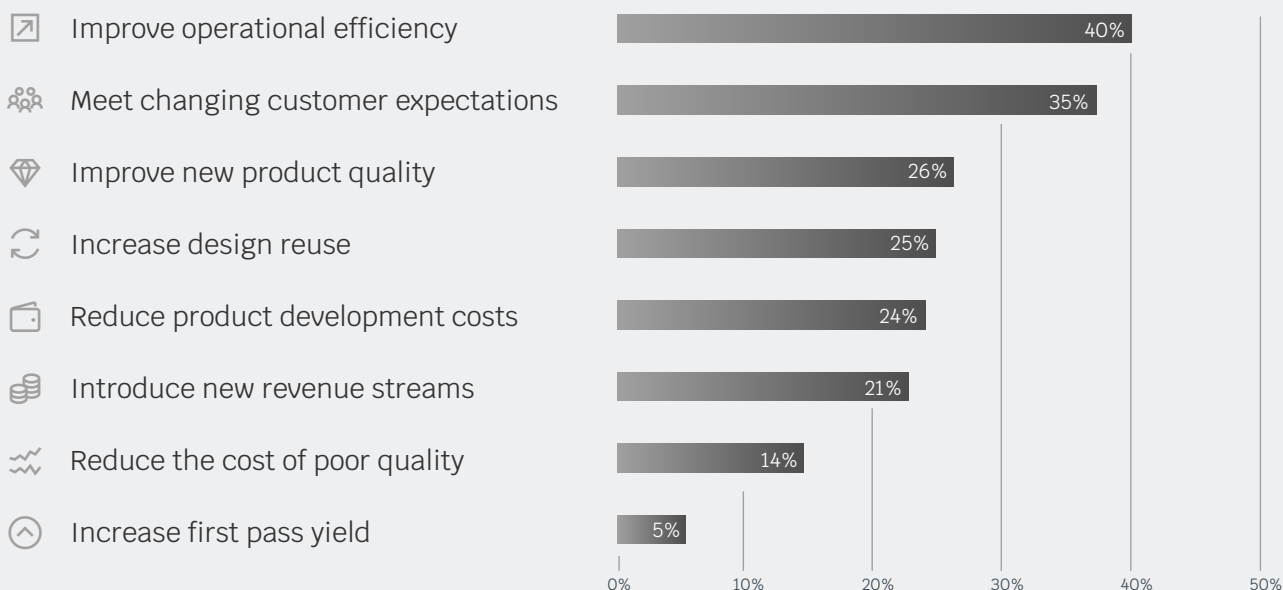
BY HAFIZ SHEIKH ADNAN AHMED

Most of us have been hearing the term "digital transformation" pretty much everywhere for a few years now. It all started by migrating business processes to automation, e-services were introduced, and with the advent and usage of mobile phones, we saw mobile apps for almost every line of business. Entire industries were transformed and moved a great deal of their activity online, embracing technologies such as cloud storage, IoT, and more. Digital transformation (DX) used to be just good to have. But since COVID-19 disrupted business operations worldwide, many organizations now see DX as a necessary step in preserving their business. The [Global Digital Transformation Market](#) is expected to grow from US \$469.8 billion in 2020 to US \$1,009.8 billion by 2025, at a Compound Annual Growth Rate (CAGR) of 16.5% during the forecast period.

According to [Finances Online](#), the top benefits of adopting a digital model include improved operational efficiency, changing customer expectations, and improving new product quality.



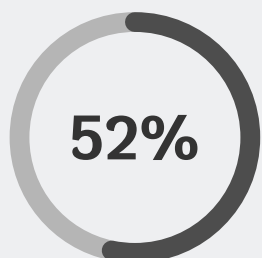
Top benefits of adopting a digital model



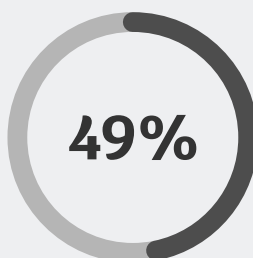
It is also noteworthy to understand what “digital business” does mean to organizations. It enables worker productivity through tools, such as AI-assisted processes,

the ability to better manage business performance through data availability, and meet customer experience expectations.

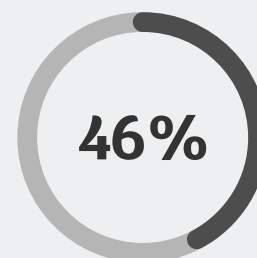
What does “digital business” mean to organizations?



Enable worker productivity tools such as AI-assisted processes



Ability to better manage business performance through data availability



Meet customer experience expectations




With the advent of digital transformation over the last two decades has coined a new statement “data is the new oil”, and that holds true from the fact that individuals, organizations, states, and countries across the globe are realizing the importance of data and data privacy. The bad guys are as intelligent as the good guys, and they know what they are after. With the massive migration in the last couple of years to remote work due to COVID-19, making better use of the cloud has exposed more data to risk, and it is still unsure whether everybody is aware of that increased risk and how to protect it.

After the enforcement of the EU [General Data Protection Regulation \(GDPR\)](#) in 2018, which I consider the referring point of all modern data privacy laws and regulations, states and countries around the globe are either adopting existing data privacy laws or creating their own. According to a [2021 report](#) by Morrison Foerster, 133 jurisdictions around the world have enacted omnibus data privacy laws. Throughout the last several months, many countries have announced and enforced data privacy regulations. For example, China enacted the [Personal Information Protection Law \(PIPL\)](#), Saudi Arabia approved a [Personal Data Protection Law](#) that came into effect in March 2022, and the United Arab Emirates (UAE) has published the [UAE Data Protection Law](#) that introduces major changes to data protection in the UAE.

So, now we are standing at an interesting crossroads. We want things to be done in the blink of an eye, our lives are “digitalized”, and are connected to devices all around. Our lives are overtaken by robotics, chatbots, virtual assistants, virtual reality, Artificial Intelligence, Machine Learning, etc. Data ownership is flawed, on paper it appears to be controlled by the one who that data belongs to, but the reality is different – data owners themselves are not aware of how their data is being shared and used. Through algorithms based on data, many organizations target ads based on your search history, in order to cater to consumers’ interests and inevitably be of benefit to their business.

While digital transformation is creating major opportunities for organizations, it is also introducing a new dimension to the traditional view of risk. With industry 4.0, business leaders are making strategic choices on the investment, technology, resource levels, and skills needed to operate a digital business, all of which will have an impact on the short-term profitability and long-term viability of the organizations. These strategic choices inevitably involve an element of risk. At the same time, organizations must cope with external threats. For example, as an organization undergoes digital transformation and more of its assets become digital, the threats of cybercrime and risks around data privacy are growing.



Let us take the example of Artificial Intelligence (AI). Artificial intelligence (AI) has developed rapidly in recent years. Today, AI and its applications are a part of everyday life, from social media newsfeeds to mediating traffic flow in cities, to autonomous cars, to connected consumer devices, such as smart assistants, spam filters, voice recognition systems, and search engines.

AI has the potential to revolutionize society, however, there is a real risk that the use of new tools by states or organizations could have a negative impact on human rights. The following are some of the major data [privacy risk areas and problems](#) related to AI:

- › **Reidentification and De-Anonymization** — AI applications can be used to identify and track individuals across different devices in their homes, at work, and in public spaces. For example, facial recognition, a means by which individuals can be tracked and identified, has the potential to transform expectations of anonymity in public spaces.
- › **Discrimination, unfairness, inaccuracies, and bias** — AI-driven identification, profiling, and automated decision-making can lead to discriminatory or biased outcomes. People can be misclassified, misidentified, or judged negatively, and such errors or biases may disproportionately affect certain demographics.
- › **Opacity and secrecy of profiling** — Some applications of AI can be obscure to individuals, regulators, or even the designers of the system themselves, making it difficult to challenge or scrutinize outcomes. While there are technical solutions to help improve some systems' interpretability or ability to audit, a key challenge remains whenever this is not possible, and the outcome can significantly impact people's lives.
- › **Data exploitation** — People are often unable to fully understand what kind of — and how much — data their devices, networks, and platforms generate, process, or share. As consumers continue to introduce smart and connected devices into their homes, workplaces, public spaces, and even bodies, the need to enforce limits on data exploitation has become increasingly pressing.
- › **Prediction** — AI can utilize sophisticated machine-learning algorithms to infer or predict sensitive information from non-sensitive forms of data. For instance, someone's keyboard typing patterns can be analyzed to deduce their emotional state, which includes emotions such as nervousness, confidence, sadness, or anxiety. Even more alarming, a person's political views, ethnic identity, sexual orientation,

and even overall health status can also be determined based on activity logs, location data, and similar metrics.

Let us now talk about IoT or the Internet of Things. The Internet of Things (IoT) is a broad term that generally refers to physical devices connected to the internet that collect, share, or use data. This includes personal wearable devices, such as watches and glasses, home appliances such as televisions and toasters, features of buildings such as lifts and lights, supply chain and industrial machineries such as forklifts and sprinklers, and urban infrastructures such as traffic lights and rubbish bins. IoT devices and the data they collect can provide convenience, efficiency, and insights into essentially every aspect of our world. For the public sector, the IoT is currently providing many benefits and has the potential to generate even greater public value in the future.

Consumers, governments, and businesses everywhere have been increasingly using IoT devices, and it is widely expected that the use of IoT will continue to expand rapidly. However, rushing into IoT without proper consideration of privacy can lead to harmful and unexpected consequences. As IoT grows, the amount of data it generates will naturally increase alongside it. These large collections of data can, in many cases, constitute personal, health, and sensitive information, raising many privacy challenges. Some of the challenges around data protection include, for example:

- **De-Identification of IoT data** – The data collected by large IoT ecosystems like smart cities can be valuable for a range of purposes, such as research or informing policy decisions. A common way to maximize the value of this data is to make it publicly available online. However, it is generally impermissible for datasets that include personal information to be publicly available. The simplest way to ensure personal information is not included in a dataset is to allow individuals to remain anonymous by never collecting information that can identify them. However, data collected by the IoT is often very difficult to de-identify due to its highly granular nature.
- **Transparency** – The passive nature of many IoT devices can make it difficult for individuals to be informed that their personal information is being collected. Devices in public spaces can collect information automatically, sometimes relying on individuals to opt-out if they do not want their information collected.
- **Accountability** – The number of organizations that can be involved in an IoT ecosystem can make it difficult to identify who is, or should be, accountable for what. The nature of IoT devices can make it impossible for an

organization to have control over every aspect of it. For example, organizations often have little or no control over security and privacy risks with communication technologies, such as satellite or 5G, as these are usually provided by third-party telecommunication companies. This can also be the case for cloud services, which can allow users to have anywhere from no control to high control over the security and privacy settings of the services they are using.

- **Interoperability** – The rapid expansion of IoT in recent years has led to the development of many kinds of devices, Application Programming Interfaces (APIs) infrastructure, data formats, standards, and frameworks. This has caused significant interoperability issues, in that devices, software, and data from one vendor often do not work with devices, software, and data from other vendors.

Data Privacy Solutions for Digital Transformation

Privacy laws have never been as important as they are today, now that data travels the world through borderless networks. Exciting times are ahead for privacy legislation as several notable privacy laws will be enforced. Cross-border transfers are likely to be one of the notable compliance issues tackled by legislative bodies and data protection authorities to ensure the regularization and normalization of data transfers between countries.

Governments around the world are reacting to the increased demand for data protection through different legislations. There is a proliferation of data protection laws during the last few years, which introduced new compliance requirements for organizations. In case of new regulations, it is vital to achieve balance between protection and free movement of sensitive data. Global compliance involves safeguarding sensitive data like payment and personal information.

The EU General Data Protection Regulation (GDPR) is a landmark privacy law and a milestone for the digital age. It has introduced new rights for individuals, such as the Right to be Forgotten and the Right to Portability, as well as made breach notification mandatory.

Something organizations should take into consideration is hiring Privacy Architects and protection officers to assess their objectives and the privacy legislation that they will have to comply with. Organizations need to ensure that DPOs (Data Protection Officers) should be experts, in both privacy and technology, a rare yet essential combination of expertise. This is not just a matter of data privacy but compliance as well.

While investing in the right security solutions will enhance the business' posture against new technology-related risks, organizations need assistance in tackling this challenge from a compliance point of view.

Organizations need to work towards implementing transparent and secure mechanisms. With the right security solutions, companies can achieve the freedom and flexibility they need to succeed in a digital economy with confidence. Organizations need to define data governance strategy and privacy/protection should be at the heart of this strategy. It should include regular training, awareness, and workshops on digital technologies and how to protect personal data while using those digital technologies. Besides external threats like phishing attacks, organizations should keep in mind to guard their sensitive data against insider threats as well. The latter requires a focus on understanding and securing the data itself. Organizations also need to employ data security governance principles by focusing on sensitive data protection and privacy, conducting, deleting unnecessary data, and consolidating data silos, whether they are on-premise or in the cloud, to ensure project alignment with business objectives.

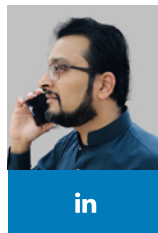
The Final Verdict

Despite its potential pitfalls, digital transformation remains an extremely exciting venture for businesses of all shapes and sizes. The prospect of leveraging cutting-edge technology to accelerate their business processes, and thereby, making themselves more competitive is certainly attractive. However, data privacy should always be the foundation of any digital transformation project, as without it, the whole house will start to fall.

At the end of the day, companies that incorporate transparent privacy policies into the building blocks of their companies are the ones that will see increased brand loyalty moving forward.

They are the ones who are actively pursuing ways to incorporate blockchain into processes and who are actively working to not just meet but exceed the guidelines of the General Data Protection Regulation.

They are the ones who actively empower their customers to offer them information, knowing it will be used to enhance their user experience — no more, no less. But in the next three to five years, I anticipate privacy will become a game-changer for the organizations that do it right. It will bolster trust and ultimately sales. And customers will, thankfully, be all the wiser for it.



Hafiz Sheikh Adnan Ahmed

IT Governance, Risk, and Compliance, Business Continuity, Information and Cybersecurity, and Data Protection Expert, Certified PECB Trainer

Hafiz Sheikh Adnan Ahmed's journey started back in 2005 as a Quality Assurance Engineer and over the years he shaped his career in the areas of Information and Communication Technology (ICT) governance, Information and Cybersecurity, Business Continuity and Organizational Resilience, Data Privacy and protection, Risk Management, enterprise excellence and innovation, and digital and strategic transformation. He is an analytical thinker, writer, certified trainer, global mentor, and advisor with proven leadership and organizational skills in empowering high-performing technology teams. He is a certified Data Protection Officer and has won Chief Information Security Officer (CISO) of the Year award in 2021 and 2022, by GCC Security Symposium Middle East and Cyber Sentinels Middle East, respectively.

Hafiz is a public speaker and conducts regular training, workshops, and webinars on the latest trends and technologies in the fields of digital transformation, information and cybersecurity, and data privacy. He is an ISO Lead Auditor and ISO Management Systems Auditor for ISO 9001, ISO 20000, ISO/IEC 22301, ISO/IEC 27001, and ISO/IEC 27701 Management Systems. He volunteers at the global level of ISACA® in different working groups and forums. He is the Co-Founder and CIO of Azaan Cybertech Consulting, and his role is to drive and align business strategies of the company's esteemed clients towards information and cybersecurity centric and to oversee the people, processes, and technologies within the organizations to ensure they deliver outcomes that support the goals of the business. To know more about Azaan Cybertech Consulting, log on to: <https://azaan.net.au>

Hafiz can be contacted through email at: hafiz.ahmed@azaanbiservices.com



International Computer Security Day

Cybersecurity affects all aspects of our lives, from our day-to-day activities to our organizations. The importance of cybersecurity is emphasized yearly on November 30, National Computer Security Day. Recent breaches have highlighted the need to keep peoples' and organizations' online presence safe, and in an effort to do so, many organizations have started to implement stronger security measures, follow guidelines, and implement security standards.

Standards such as [ISO/IEC 27001](#) and [ISO/IEC 27002](#) provide specific guidance and requirements for Information Security, which help ensure your security and continually improve security management in an organization.



Exploring the Beauties of Québec, Canada





Located in the eastern province of Canada, Québec is the second-largest Canadian province with its capital Québec City being the oldest city in the country and the province's major metropolis Montreal being the second-largest city in Canada.

The name Québec is derived from an Algonquian word that means “where the river narrows”, offering tourists and locals a splendid view of the majestic St. Lawrence River.

A vibrant charming city, rich in history has become a sought-after attraction, not only due to its historical sights but also for its many stunning landscapes, the friendliness it offers, and many activities that have made Québec a stand-out destination.

Historic Old Québec – World Heritage Site

Château Frontenac

Built in 1892, the Château Frontenac is the most photographed hotel in the world and Québec City's most notorious landmark. Located in the heart of the Old City the hotel stands high overlooking the St. Lawrence River and many other historical attractions offering a memorable stay. The Château Frontenac is one of Canada's most important establishments, the historical monument is a rich piece of French Canadian heritage.



Terrasse Dufferin

Stretching from the foot of the Citadelle to Château Frontenac, Terrasse Dufferin offers breathtaking views of Île d'Orléans, the St. Lawrence River, and Québec City's Lower Town, making it a perfect spot for a stroll to enjoy the viewings. The long wooden boardwalk is a year-round popular gathering place where street entertainers are out in full force in the summer, to the delight of passersby.



Petit-Champlain

A build of the 17th century, the street hosts many restaurants and shops for visitors to enjoy and explore. The Petit-Champlain is the oldest artery in North America granting a unique experience with the feel of going back in time. The magnificent buildings have an old-world charm portraying the significance of North American history.



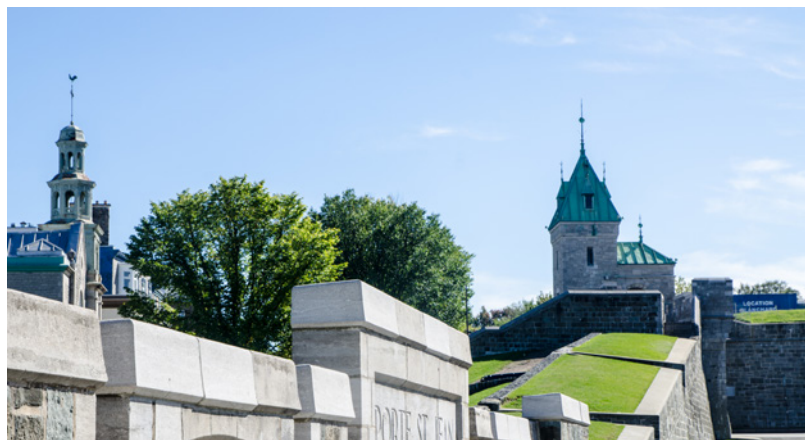
Place Royale

An important social center since the city's founding, the famous plaza is located in the heart of historic Lower Town. With a wide array of old buildings representing French style architecture, mostly over 300 years old, the square offers a refined, unique, and very enchanting experience to its many visitors.



Citadelle de Québec

A national historic site of Canada for decades, the Citadelle was the Largest British fortress in North America at its time. Its characteristic star shape is noticeable even from above. It hosts many locals and tourists, particularly in the summer, where all gather to watch the Changing of the Guard, a ceremony that takes place in only three places around the world, making this a very special opportunity.



Notre-Dame de Québec Basilica-Cathedral

A statement of the architecture, art, and history the basilica is a must-see attraction for anyone. The church offers a wonderful viewing with its neoclassical façade, stained glass windows, its Casavant organs, and its exquisite golden sculptures. Deemed a masterpiece by many, especially considering that it was built in 1647, burned down twice, and has been reconstructed to its original shape both times.



Plains of Abraham

An ideal place for a walk and sightseeing due to its beautiful greenery and its many museums. A rich park full of intriguing history since it is a major historic area within the battlefields park. The site makes this park one of outstanding value.



Parliament Building

The Parliament Building houses Québec's National Assembly. A magnificent tall building with an incredible architecture presents many quirky interesting details as well beautiful gardens for visitors to explore. In addition, the library, restaurant, and portrait art pieces are nowadays open to public.



Old Port

Another must-see part of the Old Town with its cobblestone roads, beautiful buildings, and many restaurants. Aside from the old-feel surroundings, visitors can take a cruise to watch the sunrise over the lovely port and picturesque architecture.



Top Québec Attractions

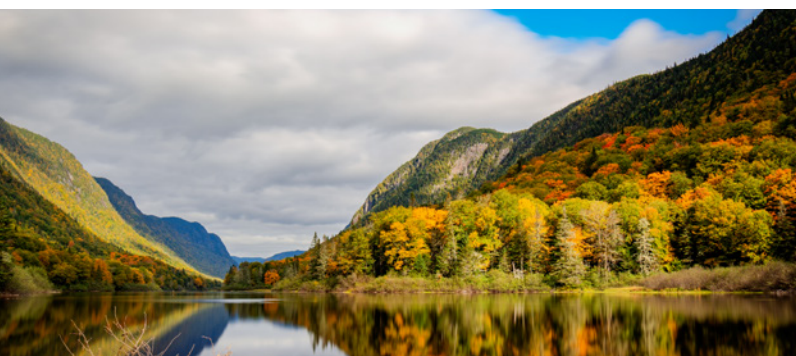
Montmorency Falls

The stunning waterfall is an ancient geological structure and is easily accessible since it is located merely a short drive away from Old Québec. The waterfalls offer a memorable time, not only due to the wonderful sights of the waterfalls themselves in any season, but also its many trails, picnic sites, and even activities such as rock climbing or zip lining.



Jacques-Cartier National Park

One of the most well-known attractions of Canada and one of the most popular national parks in the world, Jacques-Cartier National Park provides an unforgettable time depending on what you enjoy, aside from its lovely hiking trails, you can also partake in many activities, such as; fishing, surfing, mountain biking, and in the wintertime when the park is covered in snow it becomes a perfect attraction for winter sports, for example, skiing, snowshoeing, etc.



Île d'Orléans

The Island of Orleans provides a charming hands-on local experience with its opportunity to go berry picking at local farms. Needless to say, the island provides a lovely evening at its vineyards, chocolate factory, and country botanical garden, or if you are more interested in the historical sites you can explore the French-Canadian heritage, a restored 1700s manor house that is a historical landmark, or the historic church there.



Musée national des beaux-arts du Québec

For those with an interest in arts, the Musée national des beaux-arts du Québec is a must-see with pieces of well-known artists, antique sculptures and decorative arts and design, contemporary art, tributes, and the Pierre Lassonde Pavilion is worth mentioning being a piece of art in itself, made entirely of glass and steel it creates an inside-out illusion.



Sainte-Anne-de-Beaupré Shrine

The shrine reveals its rich landscape alongside the St. Lawrence River and Montmorency Falls. Aside from its gorgeous surroundings, the cathedral itself stands tall with its beautiful architecture and colors. The interior is a sight to behold with its mosaic tiles, sanctuary basement, stained glass, paintings, and sculptures, to name a few.



Aquarium du Québec

For those seeking a day of fun and adventure, the Aquarium du Québec transports you to the heart of Canadian waters to observe the incredible amount of specimens, exotic fish, and even marine mammals such as polar bears and seals.



Wendake

An immersion in history. Wendake is a thoroughly unique and accessible First Nations community in Canada. A beautiful combination of nature, culture, and history this small town provides a once-in-a-lifetime experience with its traditional villages, museums, waterfalls, river, and if you are there in June you will get to experience the traditional Wendake pow wow.



What to Eat in Québec

The cuisine of the charming city is most certainly interesting. Home of maple syrup and poutine, Québec has a lovely combination of restaurants and street food to explore. The traditional cuisine is one to not miss with an array of different flavors. Tourtière is a traditional meat pie that comes in many different recipes depending on the area which makes this dish very versatile and exciting for its visitors. Other traditional dishes to not miss are; Montreal smoked meat, pea soup, maple baked beans, crepes, Montreal-style bagels, and multiple sweets such as maple taffies, pouding chômeur, tarte au sucre, and many more.



Partnership with PECB

CyberSerenIT Inc. provides auditing, consulting, and training services in cybersecurity, information security, business continuity, and privacy. We add value to our clients by deploying the best strategies that are tailored to their needs, size, and maturity.

Through this partnership with PECB, CyberSerenIT is now fully equipped to provide its customers with renowned high-quality training that will enable them to improve their readiness and operate more effectively and efficiently, and with greater assurance. This partnership is part of our strategy to increase our market footprint and establish ourselves as a key player in North America mainly due to our high level of expertise and field experience, and our ability to deliver courses in both, French and English.



Marc F. Etende

Cybersecurity Consultant at CyberSerenIT

Marc is an IT auditor and cybersecurity consultant with 10 years of experience, mainly in Internal Control and Audit, and Cybersecurity.

Visit www.cyberserenit.com for

further information about CyberSerenIT's principal objectives and activities.

The Principles of Building Cloud Security Solutions

 BY CHRISTINE GRASSI

Working as a consultant or CISO in the information security sector, I have witnessed several revolutions in technology and IT practices. Several business processes now rely on applications that automatically receive and transmit data from and to computer networks belonging to suppliers, customers, or partners. In order to have full control of our network, we must see who is connected to our organizational network and how they do it.

When Cloud Computing started, many had doubts and did not quite understand the importance of its implementation, rather choosing to observe the companies that did make that choice, needless to say Cloud now is a reality within organizations. It is no longer about whether a company uses it or not, but which one does it, to what extent, and for what purposes.

Does this mean that the cautious and even weak-willed speech by CISOs is totally out of touch? Or that they are naturally chilly conservatives and technophobes? That their vision is totally biased and that they always overrate the risks associated with technological changes?

Questioning something new is reasonable. Just like them, I have had my moments of fear and clear-cut positions when faced with certain practices. CISOs have had to contain their enthusiasm in the face of these revolutions. We live in a world where when “everything is going well”, organizations do not want to hear much about it, but when there is a crisis, we have to be prepared to answer, handle, and manage such circumstances! CISOs responsibilities are increasing at the same pace as IT revolutions, they must often work with small teams and find an unavailable time to constantly update their knowledge. In short, they are always expected to produce more within a short time and with much more limited financial, material, and organizational resources. In this context, it is quite easy to understand why some are not very excited about new technology, or even the desire for a little stability.



Hence, it is not really surprising that when cloud first came to the scene, it sometimes earned a dishonorable reputation in the security world. Especially since many people dramatized the slightest incident or wrongly accused faulty technologies for malfunctions rather than bad practices by their users. However, that stands incorrect! If confidential data has been stolen from a fully open SaaS storage space on the Internet, the technology is not to be blamed, but rather the end user who considers IAM as being accessory. It is of the same magnitude as blaming a car manufacturer for a stolen car left in a public place with the doors fully open and the key in the ignition.

However, I am sure that security operations are, in many ways, much easier to perform in cloud environments than on-premise. A CISO's toolbox has been enriched with an impressive number of solutions, which were previously only affordable at the price of significant material and human investments, and whose deployment relied on illusory organizational agility.

I am aware that the cloud has its vices and new risks have surfaced since it started, but my experience in the cloud security sector has permitted me to identify at least four strategic lines that greatly facilitate the appropriation of new stakes related to the cloud. I will go into further detail on this later in the article.

But first, let us start with the positives!

Cloud Security – An Improved Technical Tool

As a CISO, one of my greatest challenges has been to deploy security measures in a standard and global way. It is relatively easy to use encryption within a single application, to enable and collect logs from a homogeneous class of IT components, to ensure that a well-defined group of servers is updated. But the goal is to have encryption, monitoring, patch management, etc. mechanisms that present from one end of the IT chain to the other, which are resilient and constantly efficient even when the IT pack rapidly evolves, or when the applications or the number of users infinitely multiply.

That is where Cloud Security stands out.

For example, it has never been simple to provide a strong, natively auditable encryption architecture that is accessible to everyone and simultaneously managed through a granular access rights model, owing to managed services for encryption key creation and management (e.g. KMS for AWS, Key Vault for Azure or Cloud KMS for GCP), for the storage and automatic rotation of secrets (e.g. Secret

Manager for AWS, Key Vault for Azure, Secret Manager API for GCP), or for the management of internal and external certificates (e.g. ACM public & private, Key Vault for Azure, Secret Manager API for GCP).

Similarly, monitoring infrastructure and application spaces is made easier by the activation of monitoring and data centralization services (e.g. CloudWatch, AWS Config, CloudTrail, GuardDuty for AWS, Azur's Azure Monitor and Advisor, GCP's Cloud Monitoring, Cloud Asset Inventory, and Cloud Audit Logs). Instance creation, new service activation, resource deletion or modification, non-compliance with a security rule, sudden over-consumption of a resource, these are all events that were previously unidentifiable or difficult to identify, and even less likely to do so in real-time; except at the expense of heavy investment in third-party tools, not to mention operation, maintenance costs, and the additional risks inherent to the inclusion of new cross-functional components to the IT environment.

The same applies to access management. Security stakeholders have one well-known and much-loved mantra "Everything is forbidden, except what is explicitly authorized". But this usually remains wishful thinking or utopia in environments that are often open by default or based on very simple identity and access management mechanisms.

Cloud environments, on the other hand, more often use the principle of not assigning rights at creation and some offer the possibility, service by service and platform by platform, of setting up fine-tuned and controlled access management to various assets.

Another major advantage of the cloud is the automation of security services. This helps trigger immediate responses in case of feared events or non-compliance, adapt a filtering system to the design and modification of an IT resource, e.g.,: update access rights, isolate an instance, send an alert, delete a resource, activate a filtering rule, etc. With the cloud, defence security teams can easily create and distribute automatic monitoring and response rules that greatly reduce their operational load, as well as their response time.

This allows them to concentrate on activities that need human intervention, namely long-term analysis and improvement. Similarly, faced with an ever-increasing flow of logs, managed cloud services for data collection, cleaning, correlation, and Machine Learning, which are increasingly available and efficient in cloud environments, also help in facilitating and improving this investigation work.



For example, I remember a project carried out within security teams in a company that was implementing a system for detecting anomalies and malicious actions throughout its Information Security system based on statistical algorithms and Machine Learning. This project highly improved real-time monitoring and analysis of environments that were far too large to be supervised by humans alone, eased the identification of weak signals, and accelerated the identification of attack attempts and triggering of alerts. This allowed the Security Operations Center team to focus on the investigation and take quick action toward mitigation.

A final example, amongst others, of the benefits of using the cloud for security, although from a slightly different approach, is the cloud as a security laboratory. The cloud is not only used by business and IT teams to test and improve their practices. Security teams use it as well! How many security projects were stopped because the access time to test an environment was too long and the costs too high? Owing to the cloud, it is now possible to quickly create a sandbox environment to test new solutions, practice incidents or crisis management scenarios on a replica of your production environment, or gamify getting trained in best security practices. The security team should not only ensure that the cloud is safe for users; there is a lot to gain by its usage for the security team as well. This can help it to better master this environment, and therefore, it proposes more relevant security solutions to other entities!

As a matter of fact, all these tools and solutions do not help in handling all the challenges inherent to using cloud. For example, how to manage security in an optimized and centralized way in a multi-cloud environment? In this context, it is difficult to manage security in a centralized and uniform way by relying solely on the wide variety of managed security services offered by each cloud provider. What about the implementation of regulatory requirements, linked, for example, to industry standards or sovereign cloud requirements? How can we improve the exchange between IT and business teams, now that shadow IT practices are largely facilitated by the fact that an email address and a credit card are enough to create a cloud space that can be used immediately?

And incident management! How to absorb and integrate new logs specific to cloud environments into SIEM systems. Or how to design incident handling procedures adapted to environments where, in particular, access configuration is often decentralized and multi-layered? And I am not even talking about the need to adapt security control processes and perimeters, or the difficulties associated with contractual negotiations with often all-powerful suppliers.

There is no “one size fits all” solution to these different challenges and there probably will never be.

Although there is no magic formula, there are a number of key ingredients, methodologies, and operational models that make it much easier to develop an effective cloud security strategy tailored to the specific needs of each organization.

How to handle the new cloud security challenges

First of all, I believe that cloud security is a journey, and like any journey it takes time. The cloud philosophy is: “Start small and grow”. The same applies to cloud security. You could have state-of-the-art on-premise security, with the right processes, tools, and methods in place but that does not mean you can switch to cloud overnight and apply the same solutions to get the same results. In the same way, moving an application often requires an adaptation and refactoring phase, moving “on-premise” security processes and tools to the cloud imperatively requires a review of devices and ways of doing things to adapt them. All this takes time. The key is to start with a small technical or functional scope, or a pilot business project, to try, to fail, and sometimes to start again immediately (the fail fast principle!). Gradually, you will build your own convictions about the best way to proceed, and you will be better prepared to extend the cloud perimeter covered by security a little more each time.

Of course, all of these require resources. By this I mean building shared capabilities right after. Secondly, I believe that above all, you must be up to date! Many times have I seen security teams writing standards and policies or deploying tools without even logging into a cloud console once. It may sound surprising, but many times I have seen developer teams stamped “DevOps” overnight, ordered to use new tools and cloud services without having received any training in best cloud practices, let alone security practices. Training and practice are very important because you only master what you understand. Security colleagues, get trained in cloud concepts, CI/CD, DevOps, and Agile philosophies. And fellow developers, architects, SREs, DevOps, get trained in cloud and application security best practices. It is better to have a single well-trained security consultant on your team than an army of employees clumsily trying to fit a circle into a square, especially since it is possible to boost the impact of training programs by supplementing traditional methods with more dynamic, interactive training, and awareness modules adapted to the specifics of your organization: gamedays, HandsOnLab, communities of experts sharing cloud and security practices, project feedback sessions, etc.

Thirdly, I believe cloud and security training programs will facilitate the implementation of a security management system based on collaboration. Do your security teams lack resources? Let us go back to the main principles of the cloud one more time: “You build it, you run it!” Do infrastructure teams build the cloud foundation? So, they must also be responsible for thinking about security issues inherent to these platforms and how to handle them from the onset. Do application teams build CI/CD pipelines and cloud-first applications? They too have to think about security user stories from the start, which will enable them to create strong, protected, and controllable products.

There are many advantages in encouraging IT teams to stop “blandly”, asking security teams to provide turnkey solutions on the principle that “ensuring security is not part of their job”, and then complaining that they do not have the required autonomy to adapt these solutions when they are deemed too restrictive.

On the other hand, it is in the security teams' best interest to stop mistrusting development teams due to their perceived lack of responsibility and competence in security, and later be shocked by their reluctance to demonstrate autonomy in this area.

The key is healthy cooperation and ideal integration between the different teams. It is necessary to break down silos and build multi-disciplinary teams. Security teams must join ad hoc, or permanently, development and operations teams in order to understand “in situ” the difficulties they face, identify appropriate remedies, and train a few security players who will also empower their DevOps teams to internalize security skills. Little by little, by getting their hands on pilot projects with a limited and controllable scope, the security and DevOps managers must learn how to co-construct preventive rules, detective controls, and remediation measures adapted to both performance and risk management needs. In short, cloud has its own shared responsibility model, and cloud security must absolutely have its own version within organizations.

As each organization travels through the cloud security world, it will develop its own ways of doing things, adapted to its environment. Since the “one size fits all” approach does not exist, I believe, lastly, that there are some unavoidable principles in designing security solutions:

The first principle is to build security that aligns with the principle of immutable infrastructure. This is an IT service and software management system that favors the replacement rather than the modification of its components.



This philosophy is based on the fact that it is better to manage components, each time renewed “as new”, than solutions that become unstable over time as a result of piling on patches, updates, add-ons, and deploying a cumbersome change monitoring process. This approach reduces incidents, improves security, and greatly simplifies the underlying infrastructure. The cloud, which derives its power from its automation and Infrastructure as Code abilities, is the perfect playground for deploying an immutable infrastructure. That is why it is increasingly found in organizations that have taken the step of cloud and digital transformation. Security solutions should, therefore, be designed to accommodate this flexible deployment approach: storage space independence, on-the-fly environment mapping, automated policy adaptation, etc. It does not make sense to think of security as an immovable cemented block in an environment whose very strength lies in its capacity for perpetual evolution and re-creation.

The second powerful principle is to start building your cloud security by using primarily the managed security services made available by cloud providers. Not necessarily because they are always the best, but because they are often cheaper, easier, and faster to deploy than third-party products. Moreover, they are fully automatable and very often 100% interoperable with each other. These qualities make it easy to practice a “trial and error” logic learning. Trying different action scenarios will help you quickly discover exactly what your needs are and how to implement these services with regard to the specificities and constraints of your organization. Once you have matured your security model, you will be better equipped to identify third-party or multi-cloud solutions you need to complement or replace, to conduct much more relevant and complete POCs, and challenge your third-party providers on the right topics.

By the end of this article, you may be thinking: but where do I start? Your organization has probably already conducted its first cloud experiments or is even a regular user of these services. Some security measures are already in place, and others are being deployed. How can you verify that the direction taken is the right one, and if necessary, change the course?

My advice is to start by performing a cloud security maturity audit. Not just a technical audit, but a 360° evaluation of practices, knowledge levels, process evolution, and relevance/coverage of security tools in place. To do this, you can use the maturity standards already available, such as [Cloud Security Maturity Model](#) of Cloud Security Alliance or AWS's [Security Maturity Model](#).

Once this assessment has been completed, the second step will be to take the opinions and principles set out in this article and study how you can appropriate, adapt, and implement them in your organization through a progressive and collaborative program, involving at least one representative of all the stakeholders in your organization, well beyond the IT department.

“Rome wasn't built in a day”, and neither is a successful cloud security framework. Cloud security is a journey, if not an odyssey. And the strength of a trained and united team, an iterative approach, and the use of tools and services designed for the cloud, are the fundamentals that will keep you on course without going from bad to worse.



Christine Grassi
Cloud Security Consultant
and Practice Leader

Christine Grassi is a security consultant and AWS security practice leader at Devoteam Revolve. Christine is passionate about IT security issues and relies on her extensive experience in France and Canada as a CISO and security consultant to help her clients manage their digital transformation projects, structure, and optimize their governance and security architecture for their cloud environment.

Digital Transformation Essential Reads

In the face of the increase in threats, many organizations have initiated the implementation of digital transformations in an effort of a long-term fix and as a competitive advantage. Using AI, automation of processes, cloud technologies, intelligent data flows, to name a few, creates higher expectations for customers and creates new business opportunities.

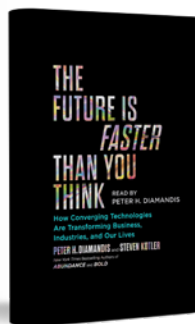
The benefit of digital transformation is becoming evident to organizations for the improvement of operations, creating greater value for employees, partners, and customers. These benefits include deeper analysis, more efficient processes, improved safety, quality, and productivity, reduced costs, as well as increased capacity. Here are some book recommendations to deepen your knowledge of digital transformations.

Digital Transformation: Survive and Thrive in an Era of Mass Extinction by Thomas M. Siebel



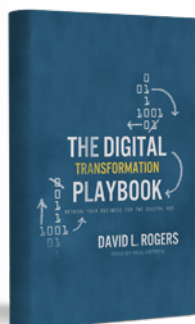
A suitable read for those interested in the evolution of technology, the author provides useful advice in an educative and generally informative manner to its readers on the complexities of digital transformation. Digital transformation goes to the very core of how organizations operate and what they do. The book takes on multiple technical tools offering details to adopt a hands-on approach to digital matters. This requires business leaders to study digital transformation carefully and get a better understanding of how the digital undertaking may induce changes in the way we do business, our organization's culture, and its business model. Artificial intelligence, big data, cloud computing, and the Internet of Things, as disjunctive terms, frequently permeate discussions of commerce, technology, and even the operations of governments. The author explains the impact of AI software innovations on organizational growth through illustrated cases. Written by a highly esteemed author the book is highly recommended to all business owners and anyone seeking to enhance their knowledge.

The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives by Peter H. Diamandis and Steven Kotler



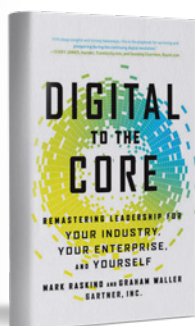
The book is a must-read for anyone wanting to know and understand the ever-evolving and augmented world we now live in. Technology is accelerating far more quickly than anyone could have imagined. During the next decade, we will experience more disturbance and the authors offer a good overview of what is happening in cutting-edge technology. The book gives a solid overview of how wave after wave technology is impacting, both our day-to-day lives and society in general, such as shopping, advertising, entertainment, healthcare, finance, food, life expectancy, and other aspects of our lives in a time of exponential growth in computing power. There is a strong sense in the book that the law of rushing returns will compound the effects of the convergence of a number of exponential technologies, such as 5G, ultrafast fixed broadband, AI, AR/VR, etc. It is very well-researched material and has the added bonus of an extensive web-based resource and notes section which serves as a foundation for further exploration of the many topics covered throughout the book.

The Digital Transformation Playbook: Rethink Your Business for the Digital Age by David L. Rogers



With businesses being transformed, changed, adapted, or disrupted by digitalization, the author proposes to view digital transformation in organizations as a strategy over the technology process. A useful source of information for those seeking knowledge, evaluating their business models, and for organizations interested in reinventing themselves digitally. Transitioning into the digital age necessitates an organization to upgrade its strategies by developing a clear vision and enforcing its capabilities to put data to work in the service of innovation, not simply its IT infrastructure. This adaptation to the digital age requires the organization to view customers differently and understand the networked and dynamic ways of their interaction. Creating a framework for digital transformation that suits most organizations, the author breaks the book down to five components of digital transformation; customers, competition, data, value, and innovation, to proceed through the chapters on harnessing customer networks, building platforms, turning data into assets, innovating by experimentation, adapting your value proposition, and mastering disruptive business models.

Digital to the Core: Remastering Leadership for Your Industry, Your Enterprise, and Yourself by Mark Raskino and Graham Waller



The book is sectioned in three parts, as the title suggests, with the first part being about the remapping of your industry, the second part covering the remodeling of your enterprise, and the third focusing on remaking yourself. Through real-life examples that are used throughout the book, from governments to the private sector, the reader gets to gain a better understating of how digital business is about integrating technology and blurring the lines between the digital and physical world. Digital transformation is disrupting the way businesses are delivering value to their customers, therefore, organizations are more and more interested by the day in taking their businesses to the next level in this digital age or by integrating technology. Each chapter ends with actionable takeaways that will help leaders and business owners think through what it means to be digital to the core in their company and industry. The main purpose of the book is to help leaders gain clarity on the existing digital businesses and develop a better understating of what lies ahead while orienting the reader on staying up to date with their organizations for the digital age.

International Anti-Corruption Day

Corruption is a continuous factor in many countries' instability. In an attempt to raise awareness, International Anti-Corruption Day is commenced annually on the 9th of December to largely advocate the fight against corruption.

ISO 37001 Anti-Bribery training courses specify the requirements and provide guidance for the establishment, implementation, monitoring, maintenance, and continual improvement of an Anti-Bribery Management Systems.

FIND OUT MORE





START YOUR JOURNEY TO SUCCESS!

Enhance your career by investing in knowledge. PECB University offers a variety of different programs that are set to enrich your expertise, in your chosen field.

The academic year, Fall 2022/2023, at PECB University has begun.

We would like to greatly wish our students the best of luck in their studies.

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.



PECB UNIVERSITY
EXISTIMATIO PER VERITATEM





PECB UNIVERSITY
EXISTIMATIO PER VERITATEM

A Personal Experience of Studying at PECB University

Nthabiseng Mdhlozini who is studying EMBA in the Business Continuity Management program at the PECB University shares her experience through this interview.

How has the studying experience at PECB University helped you in your work settings?

Studying for my EMBA through PECB University courses has provided the opportunity for me to apply some of the learned concepts in the class setting to the world of work and business. It allowed me to obtain broader knowledge outside of my core competence and domain. The value of networking with people outside of my key contacts has been highly beneficial.

What is one thing that you like about your studying experience at PECB University?

Thy hybrid learning methodology. We have experienced both instructor-led as well as eLearning modules, which do not disenfranchise students, such as myself, who are studying abroad or who have to balance work and school and are sometimes plagued with time constraints due to work commitments. You have access to the same quality tuition.

What message would you give to future PECB University candidates and students?

It is imperative that you set aside sufficient time for school as the program is rather demanding but also students must adopt an open mind in order to benefit from the worldview that the program provides.

Top Five High-Paying Job Positions You Can Pursue with a Cloud Security Certification

Nowadays, cloud computing has emerged as one of the most important aspects of modern technology as it offers countless benefits to businesses. Its advantages are seen on many levels as this virtual way of collecting and managing data is more cost-effective, facilitates data recovery and backups, and improves agility and accessibility.

Considering its benefits, cloud computing has become a vital part of the vast majority of organizations globally. In fact, according to [Cloudwards](#), 94% of all organizations use cloud computing.

Cloud computing is often chosen for its security, however, this does not mean that clouds are entirely secure.

Cloud computing can be threatened by many malicious activities like cloud breaches. Based on a [Thales Cloud Security Report](#), 45% of organizations have faced a cloud breach or failed audit during the past 12 months, representing an increase of 5% over the previous year.

[Cloud security training](#) would help you expand your professional knowledge and expertise in the complex field of cloud security. I would also provide the necessary guidance in selecting information security controls applicable to cloud services based on risk assessment and other cloud-specific information security requirements.

1. Cloud Security Architect

According to Salarycom, PayScale, and ZipRecruiter, the average annual salary for a Cloud Security Architect is **US \$156,831**.

2. Cloud Security Engineer

According to PayScale, Salarycom, and ZipRecruiter, the average annual salary for a Cloud Security Engineer is **US \$125,276**.





3. Cloud Security Consultant

According to Glassdoor, Salarycom, and ZipRecruiter, the average annual salary for a Cloud Security Consultant is **US \$116,529**.

4. Cloud Automation Engineer

According to ZipRecruiter, Payscale, and Salarycom, the average annual salary for a Cloud Automation Engineer is **US \$114,017**.

5. Cloud Security Manager

According to ZipRecruiter, Salarycom, and Glassdoor, the average annual salary for a Cloud Security Manager is **US \$95,006**.

Organizations that adopt cloud security should ensure that the level of security of their cloud systems meets

their requirements and complies with the applicable laws and regulations.

Implementing the guidelines of ISO/IEC 27017 and ISO/IEC 27018 helps maintain information security controls related to cloud services. This would also guide organizations in selecting information security controls applicable to cloud services based on risk assessment and other cloud-specific information security requirements. A cloud security certificate would demonstrate your ability and competencies to manage a cloud security program based on best practices.

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

FIND OUT MORE



The Influence of Blockchain on Digital Transformation

 BY JOSINA RODRIGUES

THE EXPERT

The recovery of the world economy after almost 2 years of pandemic effects has made the business and corporate world eager to find answers and seize opportunities that were created by the challenges in a new ecosystem.

The aim of this article is to encourage a reflection regarding the new ecosystem that is immersed in Web 3.0, and present new solutions that can create exponential results. Blockchain can be considered the architecture behind it, or the starting point for a technological evolution, which is associated with the digital transformation that will enable and enhance businesses in unprecedented ways. The maturing of blockchain was due to the numerous applications of this instrument in different activity sectors across the world and the success of all the use cases. During my presentations, I recurrently referred to blockchain as the logical structure that enabled the emergence of smart contracts and tokenization of physical asset commerce transactions, cryptocurrencies, DEFI (decentralized finance), non-fungible tokens (NFTs), and the metaverse.

Blockchain: A Game Changer

Blockchain is a key part of this new stage, especially as it is a data storage structure and a distributed digital ledger of transactions or records, which is immutable. Based on P2P (Peer to Pler), blockchain increases the transparency of transactions for all or only part of the partners. It also accelerates the performance of international transactions, consequently reducing their cost.

The creation of new business models and the restructuring of many permeated structures are used to add value. And, in this sense, digital transformation was a strategic consequence, where blockchain was an instrument for accelerating and catalyzing this transformation. Blockchain became popularly known as the backbone of the world's first cryptocurrency – Bitcoin.



Many authors compare blockchain with the effect that the internet had on society – since it most clearly is a “re” structure of relationships, actions, and businesses. This logical structure drives digital transformation. Blockchain, by providing a decentralized, secure, authenticated information infrastructure, leads to the transformation of value chains at a higher level of efficiency and true digital integration. In my collaboration with [PECB Insights Magazine](#) in an article published in June 2021, I speak further on several blockchain applications in different sectors and activities, and the framework linked to digital transformation, as an accelerator.

Without a doubt, blockchain business models are drivers of digital transformation. Thus, the very adoption of Blockchain in new ecosystems can be considered a digital transformation. The global ecosystem of central bank exchanges has adopted the creation of CBDCs (Central Bank Digital Currency). During the 2022 Davos Conference that took place earlier this year in May, world leaders gathered to discuss global issues and solutions. The opening panel revolved around the fact that 90% of central banks worldwide are creating their own digital currency, CBDC which speaks to the importance and relevance of this topic.



According to [The World Economic Forum](#), there is an estimate “that 70% of the value created over the coming decade will be based on digitally enabled platform business models, due to the rapid digitalization of economies around the world. Collaboration can also unlock value – research shows that digital “ecosystems” are expected to account for more than 30% of global corporate revenue by 2025.”

Metaverse as a New “Universe”

In a simple way, the metaverse is defined as an online space where users interact through a recreated reality – the so-called virtual and augmented reality. In this space of immersion, true experimentation and interaction allow brands, businesses, and exchanges to take on new dimensions.

Metaverse encapsulates solutions and applications in smart manufacturing, healthcare, and telemedicine in support of post-operative recovery, therapies, and physiotherapies. In education, users can count on tutorial support through avatars, developer, and creator economies with dimensions of experimentation, virtual advertising, virtual spaces and communities, social commerce, digital events and concerts and tourism, and virtual cities and public services. Undoubtedly, blockchain is a successful and inclusive factor in the scenario that includes new ways to sell, buy, interrelate, and boost.

The metaverse is built based on a universe of competition, dissemination, and business that, as strategists, requires immersion in this new reality. As such, profiles will require individuals to be skillful strategists (functionally and digitally) in order to lead businesses in exciting new directions. Some unavoidable ways to sharpen the profiles of this new era are education, integrating study and research groups, and even market analysis with the help of professionals and experts.

According to the [Citi Report: Metaverse and Money](#), it is estimated that “the target addressable market (TAM) for the Metaverse economy could be in the range of US \$8 trillion to US \$13 trillion. Expert contributors to our Citi GPS report also indicate a potential range of users of up to five billion, depending on whether we take a broad definition (i.e., unique internet users) or just a billion based on a narrower definition (i.e., Virtual Reality/Augmented Reality-device user base).”

The metaverse presents real solutions for activity sectors that can benefit from new payment relationships, purchase decisions, and user experimentation from the first contact with the innovative product or service to the creation of new business models.

As such, blockchain can be considered an articulator of this new system that converges user experience, data, and the value generated as a differential.

Web 3.0: A Natural Evolution of Interaction

On another hand, if doing a macro-level analysis, it can be said that we are already immersed in the so-called Web 3.0, the new phase of the internet that has followed Web 1.0 and Web 2.0.

Web 3 technologies are expected to revolutionize the world of commerce. In the “17 ways technology could change the world by 2027” report shared during the Davos Conference, several sectors directly related to the introduction of Blockchain were mentioned, as well as others that are reflections of this adoption in society and in business.

This new level of connectivity allows greater decentralization, more privacy for users, and transparency in the handling of their data. In this new space, users begin to exercise active participation, both in the production of content and software, as well as in the data infrastructure and in the exchange of information. Web 3.0 presents itself as more horizontal and less hierarchical with greater decision-making power for users.

As such, the new connectivity that both web 3.0 and the IoT (Internet of Things) offer should be highlighted. With the interconnection of all existing devices in businesses, access to the ubiquitous cloud is allowed, which speeds up industrial production, access to information, availability of services, and problem-solving almost in real-time. Thus, there is an opportunity to redesign the production processes in each business.

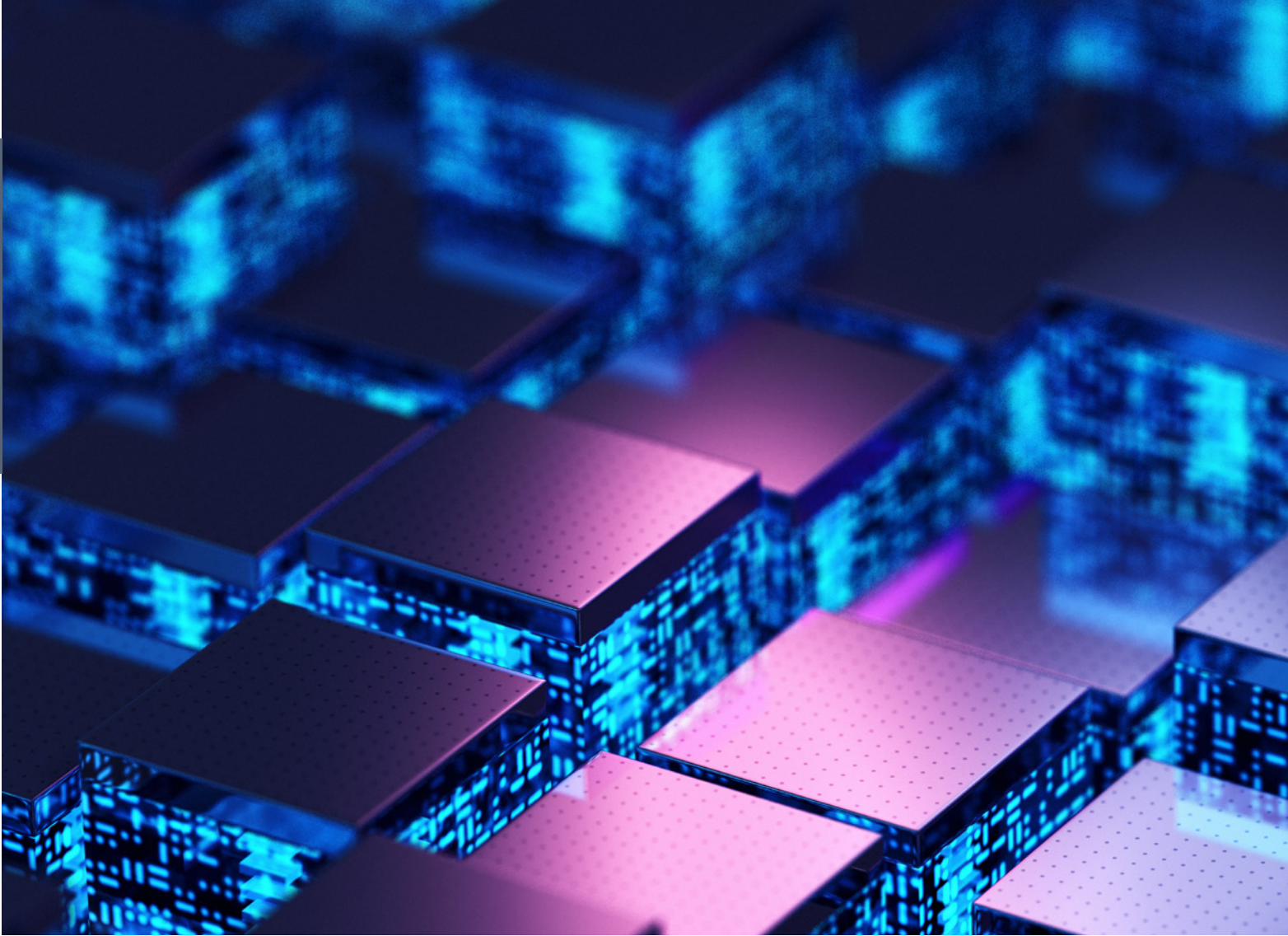
Blockchain as an accelerator of Digital Transformation immersed in the Metaverse

Time and space are part of a new paradigm in this scenario of multidimensional interaction. Companies are faced with new possibilities and challenges for their business in a blockchain-based universe which include sharing information, creating communities, and identifying cases of experimentation.

From distinct perspectives, we find different arguments that prove blockchain can be an accelerator of digital transformation.

Each of the blockchain's characteristics are a decisive factor for individuals and companies to consider Blockchain as an accelerator of digital transformation.





There is an increase in time saved when performing transactions, as they are not repetitive, transparent, and do not require intermediaries, which, once again, makes blockchain an accelerator of business processes. It should be noted that the decentralized nature of blockchain with transparency in each transaction allows it to be called a “game changer”, particularly in processes involving the supply chain. Thus, digital transformation now relies on blockchain as an essential instrument in its implementation.

Another argument that supports blockchain as not just a mere influencer, but as a new ally for digital transformation is smart contracts. As well as allowing the secure storage of information, it allows entire business processes in a transparent and inviolable way. In the near future, all our productive professional relationships will be based on smart contracts. From a financial perspective that has already been adopted by international organizations including Central Banks, blockchain helped enable the creation of a new ecosystem of exchanges based on cryptocurrencies. Today monetization and exchange systems can be sustained in a decentralized economy with a design that has never been imagined.

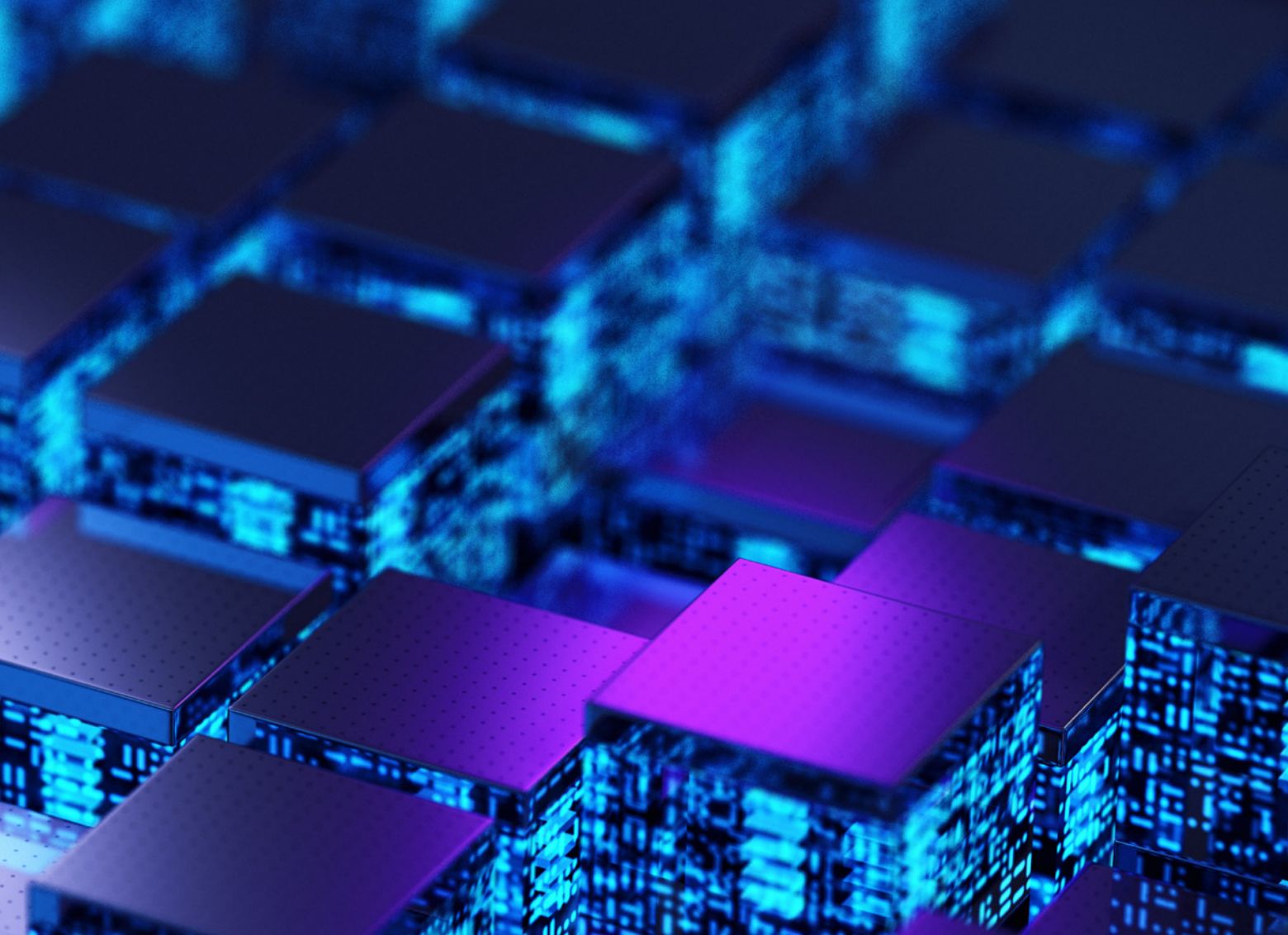
Companies can envisage financing, payment processes, and remuneration in this new ecosystem based on protocols and applications.

Even though the adoption of metaverse technologies is considered nascent and fragmented, Gartner predicts that 25% of people will spend at least one hour per day in the metaverse by 2026.

Final Considerations

Nevertheless, before making any decisions or changing current processes and structures, it is essential that businesses determine how blockchain, as a technology, can inspire value-generating digital transformation and new business models in an organizational and corporate context.

Previously, digital transformation could be postponed, as it was seen as a major challenge for many companies. And yet, today, companies question the timing and the combination of digital and physical components, as well as the reflexes in the value creation of their businesses.



Undeniably, there is no stagnating this evolutionary process. The game began with the challenge of remote work, hybrid or in-person, associated with new local and global legislation.

These devices are increasingly capable of sharing information and conducting business, which breaks the physical and structural limitations associated with traditional commerce.

The identification of a technical team that supports this journey is essential. Experimentation and practice with formal knowledge are great allies in this process. For digital transformation to occur in alignment with the challenges and expected results, a clear definition of a strategy is crucial.

Therefore, companies and businesses should surround themselves with complementary professionals, experts, and consultants who can be added value in this important moment of immersion. Thus, the new context of business multidimensionality drives competitiveness to levels never imagined.



Josina Rodrigues, PhD
Academic Advisory Board
Member at INATBA

Josina is the first holder of a Ph.D. specializing in blockchain in Portugal. In her thesis, she focused on blockchain as a new social and financial model and analyzed the impacts this technology would have on business models and the ecosystem.

Before starting as an investigator, she worked for over 20 years in the corporate world as a marketing and finance director and as a consultant and advisor.

Josina is currently a blockchain trainer, a digital business transformation and blockchain specialist for companies and start-ups, as well as a lecturer and advisor at various institutions and venture capitalists.

Furthermore, Josina is an international speaker and member of the Academic Advisory Body at INATBA (International Association of Trusted Blockchain Applications).

BUILD YOUR FOUNDATION TO THE PATH OF SUCCESS

Advance 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	
Certified Data Transformation Officer (CDTO)	English	New!	→
Lead Crisis Manager (LCM)	English	New!	→
ISO/IEC 27001 Transition	English	New!	→
ISO/IEC 27001 Foundation	English	New!	→
Lead Disaster Recovery Manager (LDRM)	English	Updated	→
ISO/IEC 27001 Lead Implementer	English	Updated	→
ISO/IEC 27001 Lead Auditor	English	Updated	→
ISO 21502 Foundation	English	Updated	→

ENHANCE YOUR PROFESSIONAL GROWTH WITH ISO/IEC 27701

ISO/IEC 27701 assists organizations in establishing, maintaining, and continually improving their Privacy Information Management System based on the requirements of ISO/IEC 27001 and guidance of ISO/IEC 27002.

The ISO/IEC 27701 Toolkit provides the necessary tools and documents that are needed in implementing and auditing the management system.

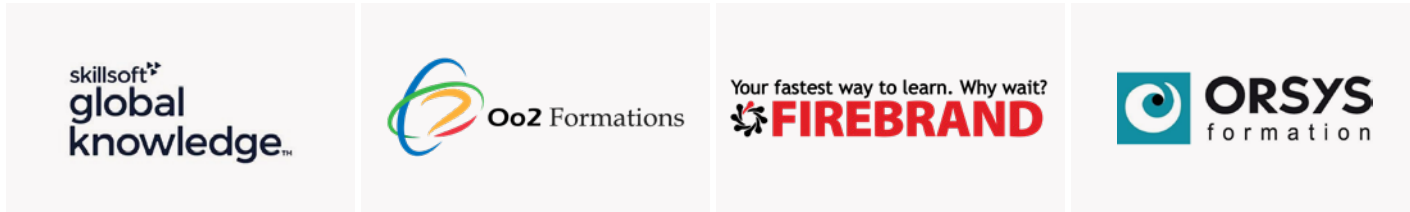
SHOP NOW ! ►

ISO/IEC 27701 Toolkit

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

SPECIAL T

TITANIUM



PLATINUM



GOLD PA



Note that PECB Partners are listed as per the credits

HANKS TO

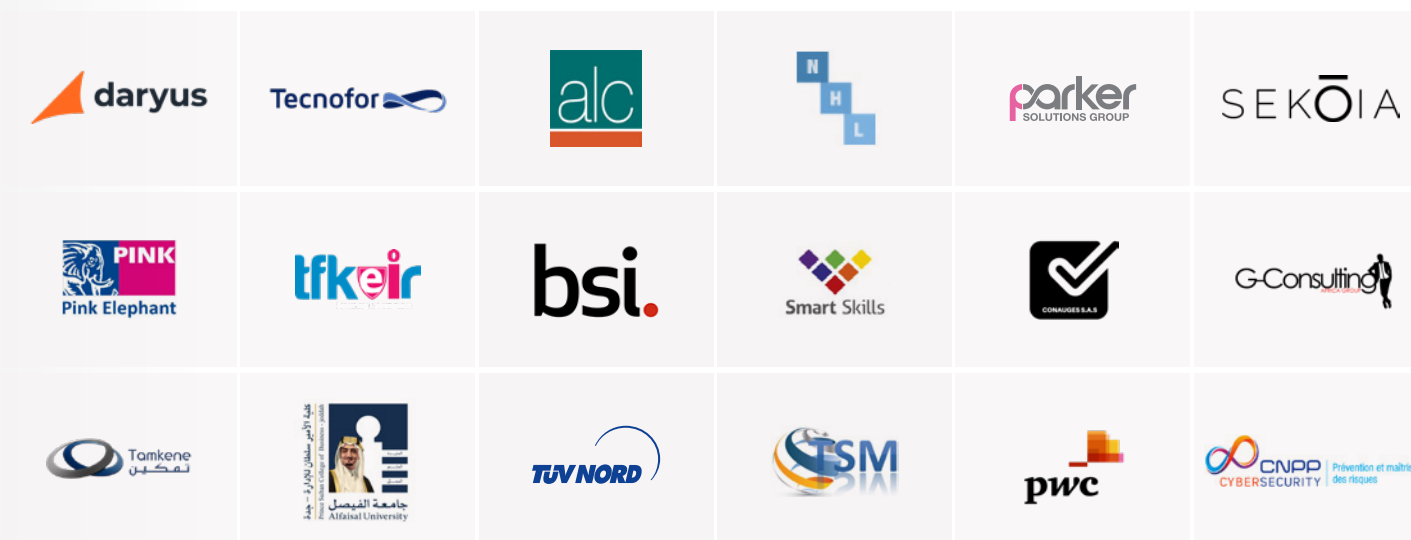
PARTNERS



PARTNERS



PARTNERS



USE DIGITAL TOOLS TO YOUR ORGANIZATIONS ADVANTAGE

