## PECB Magazine Year In Review

A Look Back at Our 2024 Journey



### **PECB Magazines 2024**

This year has been a journey of meaningful collaborations, groundbreaking insights, and innovative discussions spanning a diverse range of themes. From exploring the frontiers of Al and Emerging Technologies to delving into Cybersecurity and Ethical Hacking to Information Technology, Security, Privacy, and Business Continuity and Risk Management, we have tackled topics that reflect the evolving landscape of technology and governance.



## Al and Emerging **Technologies**

Dive into the dynamic world of artificial intelligence (AI) and explore the latest advancements shaping our future. From defense strategies and ethical considerations to the AI Act and emerging technologies' impact on organizations, this issue of the magazine probes into cutting-edge technologies revolutionizing industries and societies worldwide.





capable of addressing the wide array of ethical, legal, an

Consider taking online courses or tutorials to deepen your understanding of machine learning basics if needed.



> The Evolution of AI in Cybersecurity One of the key contributions of AI in cybersecurity it its ability to continuously monitor network traffic. By The use of AI in cybersecurity is not a recent phenomenon. It has been an evolutionary process, growing in analyzing vast amounts of data in real time, Al systems can

> Although the tech is now supercharged on larger datasets, Governanc many of the old issues remain. What is new is the speed The good news is, a whole governance toolbox exists and scale of these models - and where their data is coming already. This includes international and national legislatio

> > > Use case intelligence - Telco networks have been nurgose-built and deployed to deliver critical and distinctive services for decades. These networks are

the above challenges that can accele autonomous journey.

For narrow AI, compliance measures focus on specific Checking if personal data can be anonyn regulatory requirements relevant to the Al's application some of the simplest and most straightfe area, such as privacy and data protection laws for can take. personal data processing or industry-specific standards. Development teams can integrate compliance checkpoints

In contrast, developing GAI and ethical considerations directly related to the Ars consideration of compliance issues due to intended use, facilitating a more streamlined and focused potential applications. This may involve more dynamic and comprehensive govern compliance process. to anticipate and address a wide spectr

The data protection compliance steps are fairly easy to ethical considerations, even before specifi monitor: from incorporating data minimization principles the GAI are fully realized. to ensuring that only necessary data is collected and processed for the specific task.

Ensuring compliance with GDPR during processing, and dissemination of pe paramount. Developing frameworks to ider bias in Al algorithms becomes crucial fairness and transparency. Moreover, cybe like data poisoning pose serious risks to t models, necessitating robust security me data and maintain trust.

#### 2. Testing Phase

Testing involves evaluating the AI's p ensuring it meets the designated criteria any compliance requirements. For name closely tailored to the specific contexts in perate, allowing for focused assessm with relevant regulations and ethical stand At it is more probable to be able to repla with synthetic data to test Al functionalitik is clear and defined.

with GAJ, testing must encompass of scenarios to evaluate compliance : applications. This might include extensive hypothetical use cases to uncover any pote issues or ethical clifernmas that could contexts. For example, in this situation, strategies that can adapt to the various GAI, utilizing a mix of real, anonymized, ar to comprehensively assess privacy impact

#### 3. Deployment Phase

The final stage is deploying the Al

## Cybersecurity and Ethical Hacking

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, ensuring the integrity, confidentiality, and availability of information. Ethical hacking involves authorized attempts to breach these defenses to identify vulnerabilities and strengthen security measures. This edition provides invaluable insights into the evolving world of digital security, helping professionals enhance their skills and knowledge.



## Information Technology, Security, Privacy

The growing reliance on digital systems makes it imperative for organizations and individuals to stay informed on the latest security measures, privacy regulations, and IT innovations. With increasing awareness of the critical role privacy and security play, consumers are demanding greater assurance that their personal information is protected. Organizations are now tasked with implementing robust security frameworks and standards, this edition focuses on assisting you to meet these expectations and safeguard data in a complex environment.



10	GRC Policies and the Data Sovereignty					MIO
THE EXPERT		Navigating Cyber Risks: Stratogies for Pusiness Continuity				
ľ					rading Auantum Encryption.	
	of th introx whicl speci progr polici	n ch nan cyber to be			Forging a Docitive	
	Europ	This a	STANDARD		The Lifestyle of an I	oformation
	(NA),	can a contir	ba se			
	Early	Unde	effect H chalk		Security Exp	ert
	In th	With	to re	some	🖉 BY ALAMEEN KARIM M	ERALI
	arour	conne	advar trans	advar 🛓		
	princ	of cyt	the fu	and v 💈		
	was t	organ		AL by	The second secon	
	as En		Unde	econx	performing malware analysis, or even attempting	
	by in	in to	Onor	focus	to gather information on a target for threat	
	disck	conse	Quan	trans	intelligence, the lifestyle of an information security expert is a very tedious task to take on in the world of cybersecurity,	- APR CAR
	Europ regul	from	Distri	use o	especially when helping to improve the security of a certain	A REELS
	risks.	legal	princ trans	We w	organization or project. To further understand this, let us	La reaction and the
	in 20	organ of the	math	on th	delve deeper into the subject.	Mar Star
	regul	OF UNC	quan	we n positi	During shifts, sometimes you may need to work at night	201
			of qu	and s	time as well, and this depends on the matter at hand, as	12.
	The I Unio	The I	that i	can u	analysis of logs is necessary for such a situation to identify anomalies within logs a system, as well as overtime checking of potential security vulnerabilities within a	
	As t	ranso	The	The I	system that is necessary to patch.	
	ubiqu	threat	To gri			
	critic	reput of int	a few	Imag	All this is done to prevent unauthorized access to the system, suspicious behavior within the system, and even	
6		organ		year	suspicious network traffic, and it is important to note	
		attaci	> Qu sta	accel	that all these are essential when operating within the	
		a busi	alk	Could	information security sector. From performing malware	
		inforn syster	Var	exper	analysis by using our eyes to scan every line of code and documenting them if any malicious code is found to even	
		syster	> Qu	like t	tracing the backend of an unexpected IP Address within	
		30	be	uneth	the system, it is a back-and-forth-and-forth task that	- AS
			oni	AL, IB	requires time and dedication.	- Maria
			uti	edge	Anat free shadding lass, and preserving subscription-	A State of the lot of the
			inf	early	Apart from checking logs, and assessing vulnerabilities within the system and such, penetration testing and	
		23	42	today	ethical hacking are also important factors in the life of an information security expert. Performing both Red	TR
				And )	an information security expert. Performing both Red Teaming and Blue Teaming tactics that are required	
				with	to secure the infestigation is essential within the life	

Global Impact and Case Studies of GDPR

Ransomware attacks, on the other hand, involve 4. Supply chain vulnerabilities: Organizations are cybercriminals encrypting a company's data and demanding a ransom for its release. These attacks can cause

increasingly reliant on third-party vendors, making them susceptible to cyber-attacks through the

> Heisenberg Uncertainty Principle: The principle states It involves generating and sharing a secret key between that it is impossible to simultaneously measure, both two parties using quantum states, such as photons. The the position and momentum of a particle, with absolute key features of QKD includ

Al for Good

A positive outcome for AI won't simply happen - we

within the Safcomms Network Environment to ensure that the customers of our Internet Service Provider do not have issues with their network access later or attackers attempting to infiltrate their devices through our network.

Testing and applying new authentication mechanisms and even second-factor authentication is another necessary par to note. Even our Virtual Machines now have a Private Key to access the system via SSH which is established through strong encryption mechanisms apart from a password. therefore, implementing both the Something You Have (Private Key Encryption File) and the Something You Know (Password) Authentication Mechanisms. These vulnerability and risk assessments are done without disrupting the system nctions in an action of outsmarting the system itself and it. is all done to establish robust defenses against ovber threats

While we know that we are supposed to consult CISOs (Chief Information Security Officers) - in my personal case - it is quite different as only two of us are working in the company currently. It is pretty much like we are our own CISOs working on the entire infrastructure ourselves and securing the network in general on our own. Working on the system encryptions, hardware issues, hardware upgrades ystem hardening, as well as networking segr is all basically done by us. It is pretty much like a game and does not only involve firewalls but other tools, such as Intrusion Detection Systems and Hardware Assessment such as S.M.A.R.T, and a lot more when it comes to taking this into consideration

Hardening would be a factor to apply such as BitLocker Encryption, locking down some parts of our website to appropriate security by applying access controls and the principle of least privilege as well by putting a password and only allowing authorized individuals to access those sections. For example, as a U.S. Defense Contracting Business, we have restricted some access to certain level of our website to contractors and high-level business personnel only - that includes me and employer obviously (These are tools restricted from civilians). This is all done to create a holistic security posture, and by implement together an article of digital trust, protocols, policies, an selves together in preparation for anything even putting o and as h



## Business Continuity and Risk Management

This edition of the PECB Magazine delves into Business Continuity and Risk Management, offering insights into how organizations can navigate a world of increasing uncertainty. As businesses face disruptions from evolving threats, including cyber-attacks, disruptions, and regulatory changes, the need for comprehensive risk strategies and continuity planning has never been greater.



#### Top Issue of 2024

## Cybersecurity and Ethical Hacking

Delivering a rich collection of knowledge and equipping you with the tools to stay at the forefront of cybersecurity, this edition features captivating articles, expert perspectives, and detailed case studies, on an array of topics, including:

- → Building a Culture of Cybersecurity: Strategies for Organizational Resilience
- → The Boardroom: Digital Liabilities
- → What You Need to Know About Implementing ISO/IEC 27032 in Organizations
- → Cloud Environments: Penetration Testing from Scratch
- → Demystifying LLM Evaluation Frameworks: A Closer Look at Metrics and Oversight
- → And many more



# Top Three Articles of 2024



#### Securing the AI Ecosystem: Harnessing Enterprise-Grade Platforms for ML Model Security and Privacy

→ By embracing enterprise-grade AI platforms, organizations can refine their AI ventures, implement standardized controls, and fortify security and privacy measures, and unlock the full potential of AI. This article delves into the protocols for ML models, AI lifecycle development, governance procedures, AI implementation organization-wide, and much more.

## Legal Considerations in Implementing the EU AI Act

→ As AI permeates various facets of our lives, the need for ethical, legal, and societal considerations has become paramount. The AI Act represents a significant milestone in global AI regulation, demonstrating the EU's commitment to pioneering a comprehensive legislative approach that fosters the trustworthy and responsible utilization of AI systems. This article serves as an introductory guide to the AI Act, offering professionals insights into its key provisions, implications, and potential impacts on their respective domains.

#### The Emerging Risk: Artificial Intelligence

→ As artificial intelligence continues to advance, its impact on business operations, risk management, and decisionmaking is becoming increasingly profound. While Al offers enormous potential for innovation and efficiency, it also presents emerging risks that organizations must understand and address. Learn more through this article on Al-related risks, Al governance, and best practices for integrating Al into risk management frameworks.

## What Is Coming in 2025?

In 2025, you can look forward to a dynamic year filled with cutting-edge topics, insightful articles, and forward-thinking discussions. From advancements in AI and cybersecurity to emerging trends in governance and innovation, we remain committed to equipping you with the knowledge and strategies needed to navigate this rapidly evolving landscape. Expect a deeper dive into the integration of technology with business resilience, practical solutions for digital trust, and explorations of how industries are adapting to global challenges. The year promises a wealth of content designed to inspire, inform, and empower.

We are thrilled to kick off the year with a special milestone: the 50th edition of the magazine. This landmark issue will feature an extraordinary collection of content, celebrating the journey so far while setting the stage for even more impactful themes and innovations throughout the year. Stay tuned for a year of inspiration and empowerment as we navigate the everevolving landscape together.