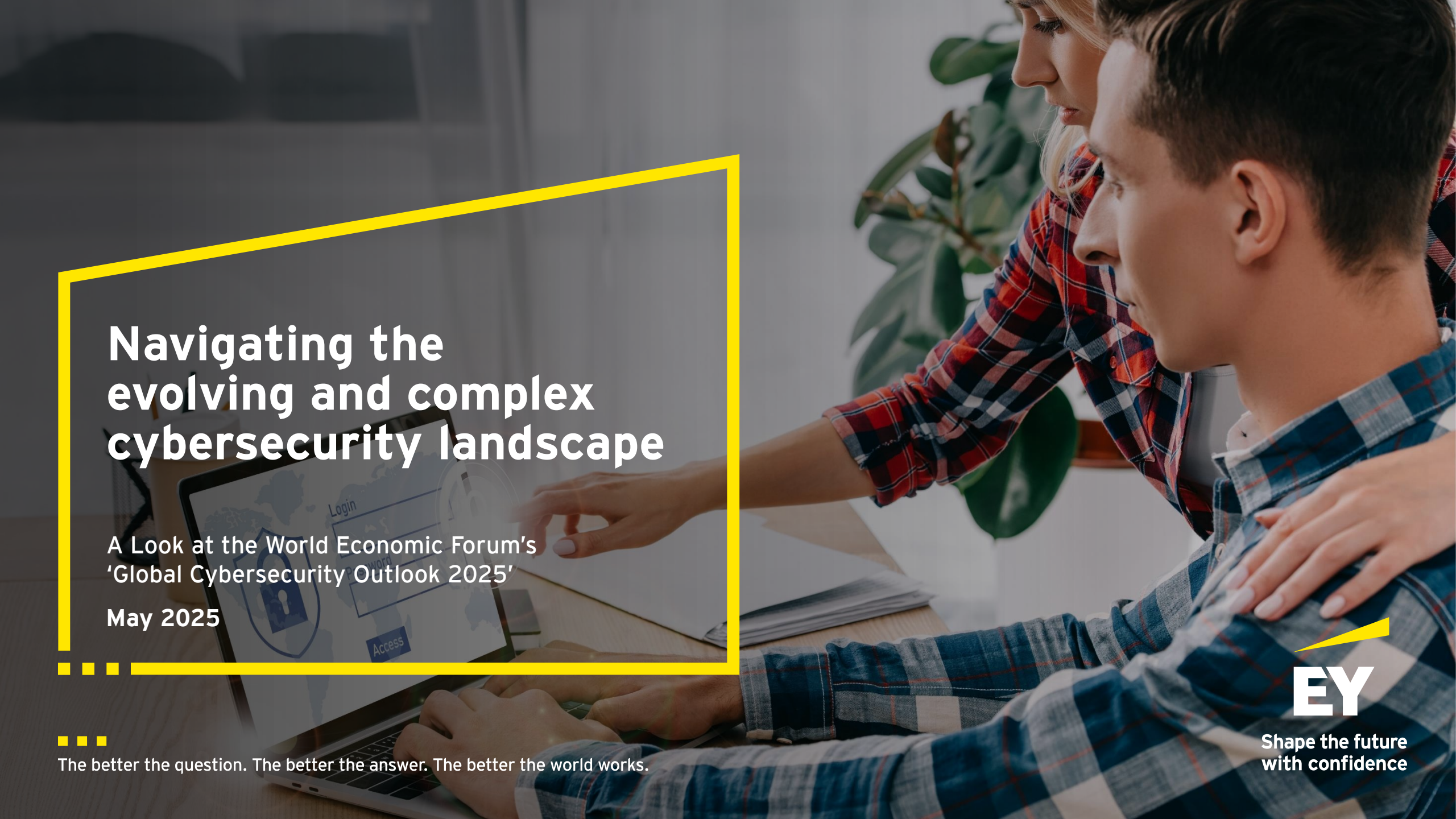


Navigating the evolving and complex cybersecurity landscape

A Look at the World Economic Forum's 'Global Cybersecurity Outlook 2025'

May 2025

The better the question. The better the answer. The better the world works.

Shape the future with confidence

Overview

The World Economic Forum (WEF), established in 1971, is a not-for-profit foundation that engages political, business, academic, civil society and other leaders of society to shape global, regional and industry agendas. It creates a global platform to foster meaningful connections between stakeholders to establish trust, cooperation and progress.[1]

The WEF's 2025 global cybersecurity outlook report highlights the increasing complexity of the cyber landscape driven by geopolitical tensions, emerging technologies and widening cyber inequity. This complexity exacerbates vulnerabilities, particularly for smaller organizations and emerging economies, and demands a shift toward a "security-first mindset" with proactive and collaborative approaches. This document contains a summary of the information presented in the WEF's 2025 global cybersecurity outlook report.[2]

[1] "Our Mission," *World Economic Forum website*, https://www.weforum.org/about/world-economic-forum/.
[2] "Global Cybersecurity Outlook 2025," *World Economic Forum website*, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

WEF global cybersecurity outlook 2025 report highlights

1	Rising cyber inequity
2	Increasing cyber risks, accentuated using AI/GenAI
3	Concentration risk: i. Regulatory landscape ii. Third-party providers
4	Benefits of AI in cybersecurity
5	Importance of employee upskilling
6	Economics of cybersecurity

1

Small organizations lag in cyber resilience, increasing supply chain vulnerabilities, while larger organizations make steady progress.

2

Organizations face rising cyber risks, with many citing generative artificial intelligence (GenAI) advancements and deep-fake tool trade on dark web forums as key concerns.

3

Complex regulatory landscape with increasing dependency on a limited number of critical providers creating supply chain vulnerabilities.

4

Large language models (LLMs) can simulate human-like responses, making honeypots far more convincing to attackers while allowing organizations to adapt to adversarial behavior in real time.

5

The continued scarcity of cybersecurity talent exacerbates the risk landscape, leaving organizations vulnerable to sophisticated cyber attacks and breaches.

6

Leaders are struggling to assess investments in cyber-risk management, highlighting the need to articulate cyber risks in financial terms.

Rising cyber inequity

Small organizations lag in cyber resilience, increasing supply chain vulnerabilities, while larger ones make steady progress.

Statistics and data

- 35% of small organizations believe their cyber resilience is inadequate, a proportion that has increased sevenfold from 5% since 2022.
- By contrast, the share of large organizations reporting insufficient cyber resilience has nearly halved, from 13% to 7%.
- 71% of cyber leaders at the WEF's annual meeting on cybersecurity in 2024 believed that small organizations have already reached a critical tipping point where they can no longer adequately secure themselves against the growing complexity of cyber risks.
- Of large organizations, 54% identified supply chain challenges as the biggest barrier to achieving cyber resilience.
- By comparison, third-party risk management does not feature among the top five concerns for smaller organizations, which cite complex and evolving threat landscape as their top concern.

Increasing cyber risks, accentuated using AI/GenAI

Organizations face rising cyber risks, with many citing GenAI advancements and increased deep-fake tool trade on dark web forums as key concerns.

Statistics and data

- 72% of organizations state that their cyber risks have increased over the past 12 months, and 63% cited the complex and evolving threat landscape as their greatest challenge to becoming cyber resilient.
- Nearly 47% of organizations cite adversarial advances powered by GenAI as their primary cybersecurity concern, enabling more sophisticated and scalable attack.
- 42% of organizations experienced a successful social engineering attack in the past year, a number that can only increase with advances and the malicious adoption of AI.
- 55% of CISOs polled during the WEF's annual meeting on cybersecurity 2024 stated that deepfakes pose a moderate-to-significant cyber threat to their organization.

Concentration risk

A complex regulatory landscape with an increasing dependency on a limited number of critical providers

Statistics and data

- More than 76% of chief information security officers (CISOs) at WEF's annual meeting on cybersecurity in 2024 reported that fragmentation of regulations across jurisdictions greatly affects their organizations' ability to maintain compliance.
- The growing complexity of supply chains and limited organizational control is a primary concern.
  - 54% of large organizations highlight supply chain challenges as the greatest barrier to cyber resilience.
  - Concerns center on software vulnerabilities introduced by third parties and cyber attacks exploiting supply chain weaknesses, such as malware distribution.
- Compliance challenges: 48% of CISOs indicate that ensuring third-party compliance with security requirements is the main challenge to effectively implementing cyber regulations.
  - The risk, however, is that these providers become systemic points of failure, and that any vulnerability introduced through the providers will not only have knock-on effects throughout their extensive client base but also cause a ripple effect throughout the ecosystem. This was seen in 2024 when a faulty update to CrowdStrike's cloud-based security software resulted in a global IT outage, affecting businesses and governments around the world.

Benefits of AI in cybersecurity

By embedding LLMs into decoy environments, defenders can create sophisticated, dynamic interactions that adapt to adversarial behavior in real time. LLMs can simulate human-like responses, making honeypots far more convincing to attackers.

Statistics and data

- One notable project, SPHINX, supported by the European Union (EU)'s 2020 research and innovation program, aims to lure attackers, learn from their attacks and deploy security controls to address them. The AI honeypot uses advanced algorithms to process attack data for AI detection and management.
- AI offers defensive potential and opportunities to enhance threat detection, automate patching, improve vulnerability management, and augment human capabilities in cyber defense. Therefore, there can be benefit when embedding AI into cybersecurity.

Importance of employee upskilling

The scarcity of cybersecurity talent exacerbates the risk landscape, leaving more than two-thirds of organizations vulnerable to sophisticated cyber attacks and breaches due to a lack of critical skills.

Statistics and data

- 91% of participants in a focus group at the WEF's annual meeting on cybersecurity 2024 concurred that AI would generate novel roles in cybersecurity, enhancing areas such as incident response.
  - Yet 67% noted that they had a shortfall in investments in AI skills within their organizations, signalling a disconnect between current training and the evolving demands.
- Currently there is a significant workforce shortage in the cybersecurity sector.
  - It is estimated to be between 2.8 million and 4.8 million professionals globally.

Economics of cybersecurity

Many leaders struggle to assess investments in cyber-risk management, highlighting the need to articulate cyber risks in financial terms to balance them with business priorities.

Statistics and data

- 60% of CEOs and CISOs surveyed report that cyber-risk management is integrated into enterprise risk management in their organizations, and many still struggle to accurately assess the level of required investment.
- Therefore, being able to articulate cyber risk in financial terms is essential for organizations to allocate resources effectively and build resilience.
- One of the core tenets of cyber economics is the balancing act between investing in cybersecurity and managing competing business priorities.

Additional cybersecurity considerations

Increasing complexity of the cyber landscape

This complexity exacerbates cyber inequity between large and small organizations, developed and emerging economies, and across sectors.

Drivers

- Geopolitical tensions
- Sophisticated cyber threats
- Emerging technologies (AI, quantum computing, satellite technologies)
- Supply chains, increasing ecosystem interdependencies
- Regulatory requirements

Impact

- As the cyber landscape becomes increasingly complex, it has the potential to exacerbate cyber inequity for organizations that are unable to meet the growing challenges.
- Smaller organizations often lack resources and skills.
- Developed vs. emerging economies: cyber resilience tends to mirror global development indicators, with lower resilience in the global south.
- Sectors like education, government and health care are disproportionately affected by the cybersecurity skills gap.

~60% of organizations report that geopolitical tensions have affected their cybersecurity strategy.

33% of CEOs are concerned about cyber espionage and IP theft.

45% of CISOs are focused on disruption of operations.

The evolution of cyber crime

Top organizational cyber risks (2025)

Ransomware attacks, cyber-enabled fraud, supply chain disruption and identity theft are the top cyber risks.

Escalation

- Cyber crime is growing in both frequency and sophistication, including ransomware attacks and AI-enhanced tactics (phishing, vishing, deepfakes).

Convergence with organized crime

- Traditional organized crime groups are entering the cyber crime market, leading to increased violence and targeting of critical social services.

Ransomware continues to be the top organizational cyber risk, with 45% of respondents ranking it as a top concern. The adoption of Ransomware-as-a-Service (RaaS) has made it easier for criminals to launch attacks, further entrenching its prevalence.

- Significant innovations in ransomware attacks are expected, creating new challenges for organizations to defend against.
- Cybersecurity teams must stay vigilant in addressing the ever-evolving threat landscape, actively monitoring and defending against sophisticated ransomware attacks.

Cyber-enabled fraud is the second-highest organizational cyber risk, posing a significant threat alongside ransomware and supply chain disruptions.

- **Identity theft** has risen to the top of the agenda, becoming the primary personal cyber risk for both CISOs and CEOs.
- **AI-enhanced attacks** attackers are using AI tools to improve the effectiveness and scope of attacks, making it easier to launch large-scale phishing and social engineering campaigns.

According to the Global Anti-Scam Alliance, scammers have siphoned away more than $1 trillion globally in the past year, costing certain countries losses of more than 3% of their gross domestic product (GDP).

(Source: https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai)

The evolution of cyber crime (continued)

Evolving threat landscape: cybersecurity risks to critical infrastructure

- Escalating geopolitical tensions and sophisticated cyber threats pose substantial risks to critical infrastructure. The conflict in Ukraine highlights vulnerabilities in sectors like energy, telecommunications, water and heating, which are repeatedly targeted by cyber and physical attacks. These attacks disrupt control systems and compromise data, jeopardizing human safety.

Climate crisis and energy systems

- Modern technology's heavy energy consumption makes power grids prime targets for cyber criminals, highlighting the need for security in emerging renewable energy systems to increase reliability.

Water facilities under cyber attack

- Cyber attacks on water facilities threaten public safety, infrastructure and national security, with vulnerabilities in OT systems like remote access points and outdated software. The October 2024 attack on the largest US water utility disrupted operations and raised concerns about the security of critical infrastructure.

Biosecurity at risk

- Cyber threats pose substantial risks to biosecurity by compromising sensitive data, disrupting laboratory security systems and sabotaging critical information. The targeting of two laboratories in South Africa and the UK in 2024 highlights the urgent need for advanced cybersecurity measures in biosecurity strategies.

Attacks on communications infrastructure

- After the 2022 attack on ViaSat, 124 additional cyber operations against the space sector were recorded amid the Ukraine conflict.
- Vital for global data flow, undersea cables are vulnerable to monitoring and disruption due to limited defenses and rising geopolitical tensions.

Genomic data vulnerabilities

- Genomic data's ability to identify individuals and reveal familial ties poses substantial risks, including threats of reidentification, unauthorized access and misuse. A late 2023 breach of a genetic-testing company exposed data of nearly 7 million people, highlighting these vulnerabilities.

The rise of cybersecurity regulations

Motivations for compliance

- Organizations are increasingly recognizing the importance of regulations as a driver for improving cybersecurity posture and mitigating risks.
- According to surveys, a majority of CISOs and CEOs cite strengthening security and reducing cyber threats as primary motivations for implementing new regulations. This reflects a growing awareness of the critical role that regulations play in fostering a more secure digital environment.

Regional and global compliance

- The global landscape of cybersecurity regulations is becoming increasingly fragmented, with different regions and countries implementing distinctive frameworks. This creates challenges for organizations operating in multiple jurisdictions, requiring them to navigate a complex web of compliance requirements.
- Requirements overlap and often are conflicting. This can lead to confusion, increased compliance costs, and potential inconsistencies in security practices.
- Varied enforcement timelines, constant vigilance and adaptation need.

NIS2 directive (EU)

Enhanced incident reporting, stricter supply chain oversight, and increased accountability for boards of directors.

CIRCIA (US)

Act mandates the prompt disclosure of cyber incidents, strengthening cybersecurity for critical infrastructure in the US.

DORA, GDPR, NDPR, LGPD (Global)

These initiatives extend regulatory scrutiny across sectors and borders, highlighting the growing global consensus on the need for strong data protection and cybersecurity practices.

Call to action

Call to action

The global cybersecurity outlook 2025 emphasizes that escalating complexities in cyberspace challenge ecosystem cyber resilience and expose gaps in preparedness. Addressing this complexity requires proactive and collaborative efforts.

This includes fostering a security-first mindset, investing in skills development, harmonizing regulations, and exploring economic incentives to improve overall cyber resilience across organizations and nations.

Organizations should proactively discuss the changing cyber landscape and determine the best preventive and detective measures for their organizations. This includes:

- Re-evaluating the organization's cyber risk posture
- Understanding their organization's supply chain dependencies
- Assessing the organization's cyber incident response plans and conducting incident simulations
- Support compliance with cybersecurity regulations
- Determining the impact of AI on the company's cybersecurity program

Contact

Jaime Kipnes

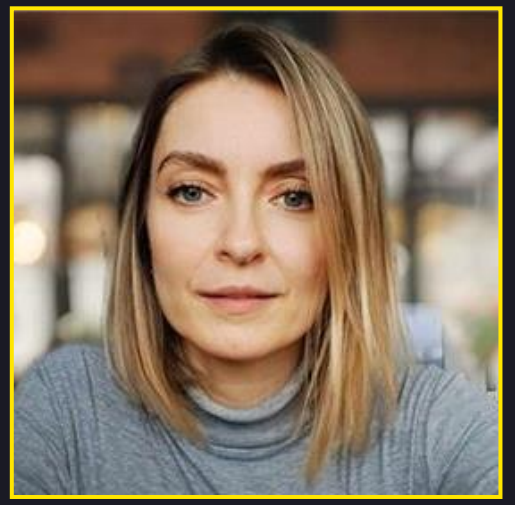
Principal

EY Global and Americas

Cyber Assurance Leader

jaime.kahan@ey.com

+1 212 773 7755



Mariola Łuka

Assistant Director

EY Global Center for

Cyber Assurance

mariola.luka@gds.ey.com

+4 871 714 3746

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EYG No. 003390-25Gbl
ED None

ey.com